



Universidad Popular Autónoma del Estado de Puebla
Centro Interdisciplinario de Posgrados.

Diseño y Planeación Estratégica de un Modelo de Seguridad
Para Implementar Votaciones Electrónicas Presenciales en el
Estado de Colima.

Tesis

Que para obtener el grado de Doctor en:
Planeación Estratégica y Dirección de Tecnología

Presenta

Juan Alfredo Lino Gamiño

Puebla, México, 03 de Febrero de 2012



UPAEP – Secretaría General

Dirección General de Apoyos Académicos

Dirección del Centro de Recursos para el Aprendizaje y la Investigación.

Biblioteca Central - **Karol Wojtyła**

Tesis Digitales Restricciones de uso:

DERECHOS RESERVADOS ©

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis está protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de textos, imágenes, gráficas, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente de donde la obtuvo mencionando el autor o autores involucrados en el documento.

Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



Universidad Popular Autónoma del Estado de Puebla
Centro Interdisciplinario de Posgrados
Investigación y Consultoría

Doctorado en
Planeación Estratégica y Dirección de Tecnología.

SE LIBERA LA TESIS DEL ALUMNO:

Juan Alfredo Lino Gamiño

CUYO TEMA ES:

Diseño y Planeación Estratégica de un Modelo de Seguridad Para
Implementar Votaciones Electrónicas Presenciales en el Estado de
Colima.

Comité Doctoral

Dra. Mayrén Polanco Gaytán

Director de Tesis

Dr. Carlos Arturo Vega Lebrún.

Asesor

Puebla, México.

Dr. Luis Alejandro Fabre Bandini

Asesor

03 de febrero de 2012

Agradecimientos:

A Dios:

Quien en los momentos más crudos siempre confié en Él y por más negro que fuera el panorama su manto siempre me cobijó y su luz nunca dejo de iluminar mi camino.

A Doña María Eugenia Gamiño Valtierra (F):

Madre tu hijo no te fallo y sé que desde el cielo siempre me cuidaste y alentaste para que no claudicara, mamá te extraño.

A Don Juan Lino Sánchez:

Por ser mí ejemplo, mis cimientos, mi coraje y mi valor, padre con amor tu hijo.

A mi esposa Alejandra Robles Salazar:

Gracias por apoyarme y ser mi complice en todo, te amo robu.

A mis hijas Itzel, Eugenia:

Por su amor y comprensión, por sus lágrimas, por todo lo que me han dado, son mi todo.

A mis hermanos con amor.

A mis profesores:

Dra. Mayrén Polanco Gaytán, Dr. Alejandro Fabre y Dr. Carlos Vega L.
Su sabiduría, paciencia, apoyo, pero por sobre todo su calidez, Dios los bendiga.

A Sergio Felipe López Jiménez:

Por qué me acompañaste en esta aventura que soñamos durante mucho tiempo y que al final se hizo realidad, un golla para ti.

Al Dr. Pablo Nuño:

Por su confianza, por marcarme una nueva manera de ser en Cristo y en el Espíritu Santo, Dios lo bendiga.

A todos mis amigos que siempre estuve en sus oraciones:

Juan Carlos Moreno, Juan Ángel Frías, Antonio Águila Reyes y familia, Juan Carlos Gutiérrez Ayala, Luis García y todos aquellos que han sido, son parte de mi vida y que siempre me dieron palabras de aliento, bendiciones para todos.

A la Universidad de Colima y UPAEP por darme esta gran oportunidad, ¡gracias!

Índice

| | |
|---|-----------|
| Introducción..... | i |
| Capítulo I.- Planteamiento del Problema..... | 1 |
| 1.1 Antecedentes de la investigación. | 1 |
| 1.2 Justificación de la investigación..... | 6 |
| 1.3 Objetivos de investigación. | 9 |
| 1.3.1 Objetivo general. | 9 |
| 1.3.2 Objetivos específicos. | 10 |
| 1.3 Preguntas de Investigación. | 10 |
| 1.4 Alcances y limitaciones del proyecto..... | 11 |
| 1.5 Viabilidad de la Investigación..... | 12 |
| 1.7 Esbozo del Marco Teórico. | 13 |
| 1.7.1 Principios básicos de estrategia. | 13 |
| 1.7.2 Administración estratégica. | 15 |
| 1.7.3 Planeación estratégica. | 18 |
| 1.7.4 Estrategia Electrónica (<i>E-Strategy</i>). | 20 |
| 1.7.5 Alineación estratégica. | 26 |
| 1.7.6 Transformación de las empresas mediante la innovación operacional. | 28 |
| 1.7.7 Perspectiva estratégica de la democracia electrónica..... | 29 |
| 1.7.8 Dimensiones del voto electrónico..... | 29 |
| 1.7.9 Votaciones electrónicas..... | 30 |
| 1.7.10 Redes privadas virtuales (RPV)..... | 52 |
| 1.8 Metodología de investigación. | 53 |
| 1.9 Resultados (a priori) esperados..... | 55 |
| 1.10 Contribuciones originales esperadas. | 56 |
| 1.11 Impacto Social Esperado. | 56 |
| 1.12 Estructura de la tesis..... | 56 |
| | |
| Capítulo II.- Marco de referencia..... | 59 |
| 2.1. Las votaciones electrónicas a nivel mundial. | 59 |
| 2.2 Estonia..... | 60 |
| 2.2.1 Partidos políticos..... | 63 |

| | |
|--|-----|
| 2.2.2 Evolución del voto electrónico. | 64 |
| 2.2.3 Participación ciudadana. | 66 |
| 2.3 Japón. | 70 |
| 2.3.1 Partidos políticos. | 73 |
| 2.3.2 Evolución del voto electrónico. | 74 |
| 2.4 España. | 81 |
| 2.4.1 Partidos políticos. | 84 |
| 2.4.2 Evolución del voto electrónico. | 87 |
| 2.4.3 Participación Ciudadana. | 91 |
| 2.5 Dinamarca. | 102 |
| 2.5.1 Partidos políticos. | 105 |
| 2.6 Polonia. | 106 |
| 2.6.1 Partidos políticos. | 108 |
| 2.7 Estados Unidos de Norteamérica. | 110 |
| 2.7.1 Partidos políticos. | 113 |
| 2.8 Canadá. | 115 |
| 2.8.1 Partidos políticos. | 117 |
| 2.8.2 Evolución del voto electrónico. | 119 |
| 2.9 Argentina. | 126 |
| 2.9.1 Partidos políticos. | 129 |
| 2.10 Brasil. | 131 |
| 2.10.1 Partidos políticos. | 134 |
| 2.11 Venezuela. | 135 |
| 2.11.1 Partidos políticos. | 138 |
| 2.12 México. | 139 |
| 2.12.1 Partidos políticos. | 142 |
| 2.12.2 Evolución del voto electrónico. | 143 |
| 2.12.3 Participación ciudadana. | 146 |
| 2.13 Entorno del voto electrónico seguro. | 150 |
| 2.13.1 Seguridad. | 150 |
| 2.13.2 Confiabilidad. | 151 |
| 2.13.3 Auditoría de las votaciones. | 152 |
| 2.13.4 Validez. | 154 |

| | |
|------------------------|-----|
| 2.14 Conclusiones..... | 157 |
|------------------------|-----|

Capítulo III.- Antecedentes del Instituto Federal Electoral, Alineación del Proceso de Planeación Estratégica y la Tecnología.....164

| | |
|--|-----|
| 3.1 Estructura..... | 166 |
| 3.2 Consejo General..... | 167 |
| 3.3 Proceso Electoral..... | 167 |
| 3.4 Actividades previas..... | 168 |
| 3.5 Instalación y apertura de casillas..... | 169 |
| 3.6 Votación..... | 170 |
| 3.7 Escrutinio..... | 170 |
| 3.8 Cierre de casillas..... | 171 |
| 3.9 Credencial para votar..... | 172 |
| 3.9.1 Parte frontal..... | 172 |
| 3.9.2 Parte posterior..... | 176 |
| 3.10 Instituto Electoral del Estado de Colima..... | 178 |
| 3.10.1 Fines..... | 181 |
| 3.10.2 Consejo General..... | 181 |
| 3.10.3 Consejos Municipales Electorales..... | 182 |
| 3.11 Seguridad del voto electrónico..... | 190 |
| 3.11.1 Planeación de la Seguridad Informática..... | 190 |
| 3.11.2 Niveles del Plan Operacional..... | 192 |
| 3.11.3 Planeación Previa de los Sistemas de Seguridad..... | 194 |
| 3.11.4 Ciclo de Vida al Desarrollo de Sistemas..... | 196 |
| 3.11.5 El Ciclo de Vida del desarrollo de los Sistemas de Seguridad (SecSDLC)..... | 200 |
| 3.11.6 Elementos que integran una Urna Electrónica Segura..... | 210 |
| 3.11.7 Entorno de seguridad..... | 219 |
| 3.12 “Fallas” en el voto electrónico..... | 248 |
| 3.12.1 Elementos de seguridad para el voto electrónico..... | 251 |
| 3.13 Cuadro de Mando Integral (<i>Balanced Score Card, BSC</i>)..... | 252 |
| 3.14 Conclusiones..... | 255 |

| | |
|--|------------|
| Capítulo IV.- Metodología de la Investigación..... | 259 |
| 4.1 Introducción..... | 259 |
| 4.2 Alcance y enfoque de la investigación. | 260 |
| 4.3 Preguntas de investigación. | 261 |
| 4.4 Diseño de la investigación. | 263 |
| 4.5 Selección de la muestra. | 264 |
| 4.6 Recolección de datos..... | 266 |
| 4.6.1 Selección del instrumento..... | 267 |
| 4.6.2 Aplicación del instrumento. | 283 |
| 4.7 Interpretación de los resultados..... | 285 |
| 4.8 Video entrevista. | 297 |
| 4.9. Conclusiones. | 300 |
| | |
| Capítulo V.- Modelo de Seguridad para Elecciones Presenciales en el Estado de Colima..... | 303 |
| 5.1 Modelo general de seguridad. | 303 |
| 5.2 Planeación Estratégica de la Seguridad. | 304 |
| 5.2.1. Gobierno del Estado de Colima y Congreso del Estado de Colima. | 305 |
| 5.2.3 Órgano ejecutivo. | 307 |
| 5.2.4 Director de Tecnologías de Información (<i>IT Director o CIO</i>). | 308 |
| 5.3 Seguridad física de los servidores. | 309 |
| 5.3.1 Instalaciones del Instituto Electoral del Estado de Colima (IEE). | 309 |
| 5.4 Seguridad lógica. | 313 |
| 5.4.1 Seguridad del servidor..... | 314 |
| 5.4.2 Servicios de red. | 317 |
| 5.5 Urna electrónica. | 320 |
| 5.5.1 Logística de traslado de la urna..... | 321 |
| 5.5.2 Seguridad de la urna en sitio. | 322 |
| 5.5.3 Suministro de energía. | 323 |
| 5.5.4 Protocolos de autorecuperación. | 323 |
| 5.6 Bitácoras de servicio..... | 324 |
| 5.7 Auditorías..... | 325 |
| 5.7.1 Auditorías de software..... | 326 |

| | |
|---|-----|
| 5.7.2 Auditorías de seguridad. | 327 |
| 5.7.3 Auditorías generales. | 327 |
| 5.8 Evaluación y desempeño del modelo, usando Cuadro de Mando Integral (<i>Balanced Score Card</i>). | 328 |
| 5.9 Conclusiones. | 334 |

Resumen.

En la actualidad en el mundo los sistemas de información han penetrado la actividad diaria de todas las personas, actividades bancarias, hacendarias, gubernamentales, comercio electrónico, negocios electrónicos, en fin, todas las actividades cotidianas prácticamente están vinculadas al uso de tecnología de la cual la sociedad en su mayoría es dependiente.

La integración de una planeación estratégica con el uso de la tecnología, los sistemas de información, aunado al uso de estándares de los sistemas de información y comunicación han generado en el mundo tecnológico una nueva forma de que los sistemas cumplan con las exigencias de la dinámica social, la cual requiere de velocidad, certeza, integridad y facilidad de uso.

Además de considerar la integración de las Tecnologías de Información y Comunicación junto a la Planeación Estratégica se debe tomar en cuenta los elementos potenciadores como son: educación, familiaridad con el uso de tecnología, entorno social, gobernabilidad y confianza en las autoridades, lo anterior para que exista de manera natural una inercia que permita que la dinámica de todos los elementos se conjugue para que el uso de la tecnología se dé por sí sola y de manera natural, sin forzar su uso, implementación y confiabilidad.

Actualmente los sistemas de votación electrónico han generado mucha expectativa al momento de su implementación, ya que en la mayoría de las ocasiones solo se han desarrollado usando técnicas de Ingeniería de Software y cubriendo el uso de protocolos de comunicación que mejor se adapte al modelo en turno, sin el uso de un estándar como tal o la integración de una planeación estratégica bien estructurada y a la altura de las circunstancias.

Por otro lado se debe tener en cuenta un esquema como el Cuadro de Mando Integral (Balanced Score Card) que evalúe de manera eficiente el uso y desempeño de la tecnología, ya que con un monitoreo constante se garantiza que los sistemas funcionen adecuadamente y en caso de alguna anomalía poder solucionarlo al momento antes que ocurran daños mayores.

Con los elementos anteriores se pueden integrar un modelo de seguridad para implementar votaciones electrónicas presenciales, en el Estado de Colima. que soportado en una Planeación Estrategia, Estándares Internacionales de Desarrollo e Implementación así como su correspondiente evaluación pueda estar a la altura de las exigencias de la sociedad, partidos políticos, gobierno y en general a todos los involucrados con la democracia en la entidad.

Abstract.

Nowdays in the current world of information systems have penetrated the daily activity of all people, banking, treasury, government, electronic commerce, electronic business, in short, almost all daily activities are linked to the use of technology which society is largely dependent.

The integration of strategic planning with the use of technology, information systems, coupled with the use of standards for information and communicationsystems in the world have created a new form of technological systems to meet the demands of the dynamic social, which requires speed, accuracy, completeness and ease of use.

In addition to considering the integration of Information and CommunicationTechnologies by the Strategic Planning should take account of enhancer elementssuch as: education, familiarity with the use of technology, social, governance and trust in the authorities, previous naturally there is an inertia that allows the dynamics of allthe elements come together to make the use of technology is given by itself and naturally, without forcing the use, implementation and reliability.

Currently, electronic voting systems have generated much expectation at the time ofimplementation, since in most cases have only been developed using software engineering techniques and covering the use of communication protocols that best fits the model in turn

without the use of a standard as such or the integration of a well structured strategic planning and rise to the occasion.

On the other hand should consider a scheme like the Balanced Scorecard (BalancedScorecard) to evaluate efficiently the use and performance of the technology, because with a constant monitoring ensures that the systems function properly and if an error to occur can be resolved as soon as possible.

With the above elements can be integrated security model to implement electronic voting in person, in the State of Colima. That supported by a Planning Strategy, International Standards Development and Implementation and the corresponding evaluation can be up to the demands of society, political parties, general government and all concerned with democracy in the state.

Introducción.

A nivel internacional todas las actividades del ser humano se han estado soportando en Tecnologías de la Información y Comunicación (TIC's), actividades bancarias, hacendarias, comercio electrónico, gobierno electrónico, medicina, en fin, todas las actividades cotidianas prácticamente están vinculadas al uso de tecnología de la cual la sociedad en su mayoría es dependiente.

En el caso de la democracia a nivel internacional ha sufrido giros importantes dependiendo del tipo de gobierno, sociedad, educación, economía y otros potenciadores que hace de ella un interés por demás importante, ya que se juega por sí mismo el futuro de millones de personas.

Los últimos procesos electorales en nuestro país se han caracterizado por la falta de planeación estratégica, organización, transparencia, seguridad y confianza de los participantes. Es evidente la disminución del interés de los votantes para participar en futuros procesos. Sobre todo por las anomalías que cometen los partidos políticos antes, durante y después de los comicios.

Diferentes grupos parlamentarios aseguran que el actual sistema electoral es fácilmente vulnerable. Se necesita construir una nueva democracia, incorporando urnas electrónicas al sistema electoral vigente. Enfatizan sobre la creación de mecanismos que permitan ejercer el voto electrónicamente, en tiempo real y de manera transparente. Para lo cual han presentado diferentes iniciativas de reformas al Código Federal de Instituciones y Procedimientos Electorales (González, 2007).

Dada la expansión de los cambios tecnológicos que están transformando las diferentes áreas de la actividad humana, más su capacidad para hacer eficiente la manera en que un gobierno promueve la participación ciudadana, se busca aprovechar el potencial que ofrecen las Tecnologías de la Información y Comunicación (TIC's), como herramienta estratégica en el

diseño de un modelo de seguridad, para implementar votaciones electrónicas presenciales en el Estado de Colima.

Países con tradición democrática como Estados Unidos y la Unión Europea, han adoptado el sistema de votación electrónica, con relativa facilidad en algunos estados y comunidades que fueron elegidos como prueba piloto para observar su desarrollo y evolución. Posteriormente, en base a las experiencias obtenidas, el proceso se ha ido mejorando para extenderlo en más lugares, que paulatinamente lo han implementado en sus respectivas democracias (Téllez, 2009).

Un país como el nuestro que se caracteriza por elegir a sus gobernantes en forma democrática, requiere de mecanismos alternos más eficientes que los actuales. Por lo que el voto electrónico reúne también las características de; universal, libre, equitativo, directo y secreto, para enfrentar ese desafío. Además, ayuda a disminuir la brecha política y tecnológica entre la población. Ofreciéndole igualdad de oportunidades en las decisiones que tienen derecho a participar. Incluyendo a personas con alguna discapacidad física o intelectual.

El voto electrónico ofrece ventajas a mediano y largo plazo. Principalmente en; el ahorro de insumos, el recuento de los votos, evita o disminuye los fraudes, brinda transparencia al proceso, mejora la logística, entre otros.

Algunos países de Europa, Asia y Latinoamérica, en vías de desarrollo (por ejemplo; Eslovenia, India, Brasil, Venezuela, Paraguay y Argentina), con atributos socio-económicos similares o inferiores a los de nuestro país, también han adoptado esta nueva forma de hacer democracia. Han obtenido resultados satisfactorios, a pesar de su geografía, elevado nivel de analfabetismo y diversidad étnica. Por ejemplo, la India celebró en 2004 las que, hasta la fecha, han sido las mayores elecciones generales con un sistema de voto electrónico. Con casi 388 millones de votantes sobre un censo de 671 millones de electores y con un 39 por ciento de analfabetismo (Presno, 2006).

El objetivo de este trabajo es desarrollar un modelo de planeación estratégica de seguridad en las votaciones presenciales en el Estado de Colima, lo anterior para establecer un nuevo esquema democrático-electoral que asuma los desafíos estratégicos y tecnológicos que predominan a nivel mundial, estableciendo un protocolo a seguir, que sea garante de los derechos políticos-electorales de los ciudadanos.

Dicho esquema ha de ser implementado sobre normas y estándares con altos niveles de exigencia que cubran las necesidades de una sociedad necesitada de transparencia y veracidad, aunado a una vigilancia y monitoreo que permita ver su evolución antes, durante y después de los comicios.

Capítulo I.- Planteamiento del Problema.

1.1 Antecedentes de la investigación.

Haciendo una retrospectiva sobre los antecedentes del voto electrónico, en Europa, los primeros prototipos se empezaron a usar en los años noventa. Por ejemplo, en Suecia y Holanda (1990) y en Francia (1992), durante la ratificación del Tratado de Maastricht, instituido por la Unión Europea.

Estos países, de acuerdo con el Índice de Competitividad Global (ICG 2009-2010) que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se ubican en cuarto, décimo y décimo sexto lugar, respectivamente. En lo que corresponde a requerimientos básicos, que incluye; instituciones, infraestructura, estabilidad macroeconómica, salud y educación primaria, se encuentran en el quinto, décimo segundo y décimo quinto lugar. Finalmente, con respecto a los potenciadores de la eficacia, los cuales abarcan; educación superior, capacitación, eficacia del mercado de bienes, eficacia del mercado de trabajo, sofisticación del mercado financiero, disponibilidad tecnológica y el tamaño del mercado, se posicionan en el séptimo, décimo y décimo sexto lugar (FEM, 2009).

Otro de los países europeos que sobresale por la experiencia acumulada, a través del tiempo en la implantación de sistemas de votación electrónica, es Bélgica. Con respecto al ICG 2009-2010 se ubica en el décimo octavo sitio. En requerimientos básicos está en el vigésimo lugar y en potenciadores de la eficacia, ocupa también la décimo octava posición (FEM, 2009).

Inició con las elecciones legislativas y municipales de 1991, haciendo una prueba piloto en el cantón de Verlaine. En junio de 1994, en las elecciones para el Parlamento Europeo (PE), donde aproximadamente 14 millones de ciudadanos votaron. Uno de cada 5 lo hicieron mediante las urnas electrónicas (Barrientos, 2007).

España se ubica en el trigésimo tercero del ICG, trigésimo octavo en requerimientos básicos y vigésimo noveno en potenciadores de la eficacia (FEM, 2009). Allí, en 1991, se tuvo una de las primeras experiencias de voto electrónico, a través de un programa piloto en Alicante. De

igual forma, en 1995 en Cataluña. En 1997 en Galicia, durante las elecciones parlamentarias (Barrientos, 2007).

Recientemente, la empresa de origen español, Indra, ha realizado pruebas piloto de voto electrónico en Francia y Portugal, sin validez legal. Éste último país ocupa el cuadragésimo tercer lugar del ICG. Trigésimo noveno en requerimientos básicos y cuadragésimo tercero en potenciadores de la eficacia (FEM, 2009). De los seis proyectos experimentales, el efectuado en la localidad francesa de Vandoeuvre-les-Nancy, se realizó conjuntamente con el Ministerio Interior de ese país. Tuvo un carácter vinculante, en el que participaron 15,000 personas que eligieron a sus representantes en el PE, a través de urnas electrónicas (Barrientos, 2007).

El voto electrónico en Estados Unidos, con un segundo lugar en el ICG, un vigésimo octavo en requerimientos básicos y primer lugar en potenciadores de la eficacia (FEM, 2009), tiene sus orígenes a partir de 1975. Cuando la Oficina General de Estadística de las Elecciones Federales, firmó un acuerdo con la Oficina Nacional de Estándares, para desarrollar las guías de consulta operacionales, que los administradores de la elección utilizarían, para garantizar la confiabilidad y seguridad del proceso de voto por correspondencia, basado en computadora.

Tomando como base las recomendaciones, incluidas en el informe del estudio de viabilidad para desarrollar ingeniería voluntaria y estándares para el desempeño en los procedimientos de los sistemas de votación estadounidense, realizado en 1984, el Congreso Norteamericano destinó fondos apropiados para iniciar el proyecto: “Desarrollo voluntario de estándares nacionales, para sistemas de votación basados en computadora”.

La Comisión Federal Electoral inició el proceso en julio de ese año. Concluyó con su aprobación, en enero de 1990, de los primeros estándares nacionales de funcionamiento, incluyendo; prueba para tarjeta perforada, marca sensible y sistemas electorales electrónicos de grabación directa.

En América Latina se han realizado esfuerzos para implementar el voto electrónico, sin lograr que se consolide en todo el continente. Esto se debe a la serie de obstáculos que han frenado su desarrollo. Principalmente en los países más pobres, que tienen una legislación inadecuada, una brecha digital profunda, actores políticos con poca visión y compromiso social, más gobiernos que actúan conforme a intereses personales.

No obstante, el padrón electoral de Brasil, ubicado en la quincuagésima sexta posición en el ICG, nonagésima primera en requerimientos básicos y cuadragésima segunda en potenciadores de la eficacia (FEM, 2009), se automatizó en 1985, extendiéndose el voto por computadora en todo el país. En 1996 se dio el último paso para automatizar las elecciones, con la introducción de las máquinas electrónicas para votar, conocidas como urnas electrónicas (e-urnas), que se implementaron gradualmente, abarcando, en 1996, una tercera parte de los electores; dos tercios en 1998 y el cien por ciento en 2000 (Brunazo, 2005).

En Venezuela, ubicada en el centésimo décimo tercero en el ICG, centésimo cuarto en requerimientos básicos y centésimo octavo en potenciadores de la eficacia (FEM, 2009), se implementó el voto electrónico en 2004. Tuvo la participación del 97 por ciento de los electores, que es el resultado de las adecuaciones hechas a la Carta Magna de la República Bolivariana de Venezuela, en 1999. Dicho esquema para votar se usó en el referéndum y las elecciones de Gobernador, en 2004 (Morelis, s. f.).

México se encuentra en el sexagésimo sitio del ICG, es quincuagésimo noveno en requerimientos básicos y quincuagésimo quinto en potenciadores de la eficacia (FEM, 2009). Respecto a la situación actual del voto electrónico, tanto en el Distrito Federal, así como en los estados de Coahuila y Jalisco, se han utilizado, a la par de los procesos electorales tradicionales, prototipos para que el ciudadano vote electrónicamente a través de máquinas de Registro Electrónico Directo (DRE). Con el propósito de recoger experiencias que servirán de base para configurar, a mediano y largo plazo, un sistema totalmente automatizado, a través del cual los electores ejerzan su derecho al voto.

De acuerdo con los indicadores publicados en el informe 2006 del Instituto Mexicano de la Competitividad (IMCO, 2008), los territorios antes mencionados se ubican, a nivel nacional, de la siguiente manera:

Tabla 1.1. Indicadores de competitividad en estados que han implementado voto electrónico.

| Indicador | Coahuila | Distrito Federal | Jalisco |
|--|-----------------|-------------------------|----------------|
| Sociedad incluyente, preparada y sana (ingreso promedio de la mujer, penetración informática, analfabetismo, eficiencia terminal en secundaria, grado promedio de escolaridad y población ocupada con estudios superiores o de posgrado). | 8 | 1 | 16 |
| Sistema político estable y funcional (Participación en elecciones locales, concentración política en su congreso local, acuerdos entre el ejecutivo y el legislativo). | 10 | 8 | 5 |
| Sectores precursores de clase mundial (líneas telefónicas fijas y penetración móvil, usuarios de Internet, productividad de las telecomunicaciones). | 9 | 1 | 10 |
| Gobiernos eficaces y eficientes (efectividad del gobierno, transparencia informativa de los estados, gasto en soluciones tecnológicas del gobierno e índice de calidad de e-government). | 11 | 4 | 23 |

Fuente: IMCO, 2008.

En las elecciones de julio de 2009, el estado de Jalisco se distinguió por ser el primero en realizar un proceso electrónico para elegir Presidente Municipal. Específicamente en el municipio de Tuxcueca, a través del Sistema de Información de la Jornada Electoral (SIJE). Con esto, pasó a la historia como el primer municipio que elige a sus representantes en forma automatizada, sin utilizar el sistema tradicional de boletas de papel vigente en nuestro país. Al final, los resultados fueron válidos y respetados por el Instituto Electoral y Participación Ciudadana de esa demarcación.

A nivel local, no se han desarrollado ejercicios que promuevan la adopción en el mediano y largo plazo del voto electrónico. Sólo existe un prototipo apoyado por el Instituto Tecnológico de Colima denominado: “Casilla Inteligente de Votación Electoral” (CIVE). Sirvió para acreditar la materia Seminario de Desarrollo de Proyectos de Investigación. Obtuvo el primer lugar en la fase local del XX Evento Nacional de Creatividad.

Dicho prototipo fue presentado ante las autoridades gubernamentales y electorales del estado. Desafortunadamente no le dieron el seguimiento, ni el apoyo requerido para su mejoramiento y posible implementación.

1.2 Justificación de la investigación.

Los últimos procesos electorales en nuestro país se han caracterizado por la falta de planeación estratégica, organización, transparencia, seguridad y confianza de los participantes. Es evidente la disminución del interés de los votantes para participar en futuros procesos. Sobre todo por las anomalías que cometen los partidos políticos antes, durante y después de los comicios.

Diferentes grupos parlamentarios aseguran que el actual sistema electoral es fácilmente vulnerable. Se necesita construir una nueva democracia, incorporando urnas electrónicas al sistema electoral vigente. Enfatizan sobre la creación de mecanismos que permitan ejercer el voto electrónicamente, en tiempo real y de manera transparente. Para lo cual han presentado diferentes iniciativas de reformas al Código Federal de Instituciones y Procedimientos Electorales (González, 2007).

Dada la expansión de los cambios tecnológicos que están transformando las diferentes áreas de la actividad humana, más su capacidad para hacer eficiente la manera en que un gobierno promueve la participación ciudadana, se busca aprovechar el potencial que ofrecen las Tecnologías de la Información y Comunicación (TIC's), como herramienta estratégica en el

diseño de un modelo de seguridad, para implementar votaciones electrónicas presenciales en el Estado de Colima.

Similar a lo sucedido cuando apareció la televisión, que para algunas personas sólo era un “radio más imágenes”, sin gran futuro, porque los contenidos que ahí se ofrecían eran los mismos que se presentaban en los cines y teatros de aquella época. Algunos sectores de la población desconfían aún del voto electrónico, se resisten a adoptarlo, principalmente por desconocimiento y analfabetismo tecnológico.

Países con tradición democrática como Estados Unidos y la Unión Europea, han adoptado el sistema de votación electrónica, con relativa facilidad en algunos estados y comunidades que fueron elegidos como prueba piloto para observar su desarrollo y evolución. Posteriormente, en base a las experiencias obtenidas, el proceso se ha ido mejorando para extenderlo en más lugares, que paulatinamente lo han implementado en sus respectivas democracias (Téllez, 2009).

Un país como el nuestro que se caracteriza por elegir a sus gobernantes en forma democrática, requiere de mecanismos alternos más eficientes que los actuales. Por lo que el voto electrónico reúne también las características de; universal, libre, equitativo, directo y secreto, para enfrentar ese desafío. Además, ayuda a disminuir la brecha política y tecnológica entre la población. Ofreciéndole igualdad de oportunidades en las decisiones que tienen derecho a participar. Incluyendo a personas con alguna discapacidad física o intelectual.

El voto electrónico ofrece ventajas a mediano y largo plazo. Principalmente en; el ahorro de insumos, el recuento de los votos, evita o disminuye los fraudes, brinda transparencia al proceso, mejora la logística, entre otros.

Algunos países de Europa, Asia y Latinoamérica, en vías de desarrollo (por ejemplo; Eslovenia, India, Brasil, Venezuela, Paraguay y Argentina), con atributos socio-económicos similares o inferiores a los de nuestro país, también han adoptado esta nueva forma de hacer

democracia. Han obtenido resultados satisfactorios, a pesar de su geografía, elevado nivel de analfabetismo y diversidad étnica. Por ejemplo, la India celebró en 2004 las que, hasta la fecha, han sido las mayores elecciones generales con un sistema de voto electrónico. Con casi 388 millones de votantes sobre un censo de 671 millones de electores y con un 39 por ciento de analfabetismo (Presno, 2006).

En el Estado de Colima, se tiene como antecedente un prototipo básico, desarrollado por alumnos del Instituto Tecnológico de Colima en 2005, denominado: “Casilla Inteligente de Votación Electoral (CIVE)”. Sus características son limitadas, principalmente en su funcionamiento, alcance, la seguridad física y lógica. Pero no existe un proyecto formal que responda a la demanda ciudadana, para disponer de mecanismos alternos confiables, con el fin de elegir a sus gobernantes. A pesar de tener las condiciones y fortalezas estratégicas necesarias para llevarlo a la práctica:

- a) Espacio geográfico pequeño (a nivel nacional es el tercer estado más pequeño, sólo superado por Tlaxcala y Aguascalientes).
- b) Cobertura tecnológica en los diez municipios, por parte de la Universidad de Colima.
- c) La población de 15 años y más tiene un promedio de escolaridad de 8.4 grados, cuando a nivel nacional es de 8.1 grados (INEGI, 2005).
- d) Sólo el 6.4 por ciento de la población es analfabeta, cuando a nivel nacional es de 8.4 por ciento (INEGI, 2005).
- e) Sociedad incluyente, preparada y sana. Economía estable y dinámica: ocupa el lugar 12 y está 13 por ciento y 11 por ciento arriba de la media nacional, respectivamente (IMCO, 2008).
- f) Es el estado con mejor percepción sobre seguridad (IMCO, 2008).
- g) Ocupa el quinto lugar a nivel nacional en número de líneas telefónicas fijas y móviles, así como en el número de usuarios de Internet: 281 por cada 1,000 habitantes (IMCO, 2008).
- h) Aumento de 2 por ciento en la eficiencia terminal en secundaria, 114 por ciento de más computadoras por habitante, incremento en 5.6 por ciento el grado promedio de

escolaridad y se disminuyó en 37 por ciento el coeficiente de desigualdad de ingresos (IMCO, 2008).

El modelo propuesto ayudará a establecer las bases de un nuevo esquema democrático en Colima. Ofrecerá mejores canales de comunicación entre las autoridades regulatorias del proceso electoral, gobernantes, legisladores, partidos políticos y sociedad en general. De igual forma, se ofrecerá una mayor transparencia en la jornada electoral. Lo que permitirá establecer métricas de su confiabilidad. También se busca contribuir al establecimiento de un marco jurídico innovador que sustente y valide el voto electrónico en la región.

El proyecto también contempla el análisis, revisión y propuesta de mejora para los entornos; político, jurídico, tecnológico y social. Por lo que se realizará una investigación documental y de campo, en las áreas antes mencionadas. Esto servirá para desarrollar un modelo que cubra las necesidades de votaciones electrónicas en el territorio colimense.

En el aspecto tecnológico, se revisarán los límites de rubros como; seguridad física y lógica, redes privadas virtuales, protocolos de comunicación, algoritmos criptográficos, interfaces hombre-máquina, ergonomía computacional, visual y física. Estos últimos tópicos serán desarrollados en la tesis: **“Diseño Estratégico de una interfaz para voto electrónico presencial en el Estado de Colima”**.

Asimismo, se pretende compartir con los diferentes actores políticos esta propuesta, para su análisis, mejora, y en su caso: adopción.

1.3 Objetivos de investigación.

1.3.1 Objetivo general.

Desarrollar un modelo de planeación estratégica de seguridad en las votaciones electrónicas presenciales en el Estado de Colima, para el establecimiento de un nuevo esquema

democrático-electoral, que asuma los desafíos estratégicos y tecnológicos que predominan a nivel mundial, estableciendo un protocolo a seguir, que sea garante de los derechos políticos-electorales de los ciudadanos.

1.3.2 Objetivos específicos.

Obtener una perspectiva estratégica de los ámbitos; políticos, legales y tecnológicos en el Estado de Colima, para recabar los datos necesarios que servirán de base para construir el modelo de seguridad del voto electrónico presencial.

1. Conocer la opinión de los colimenses con respecto a la implantación de un modelo presencial para votar electrónicamente.
2. Diseñar la planeación estratégica para la implementación de la seguridad de la información electoral, sus contingencias y políticas de seguridad.
3. El diseño de la presente investigación servirá como soporte de seguridad para el trabajo desarrollado por el C. Sergio Felipe López Jiménez, denominado: **“Diseño Estratégico de una interfaz para voto electrónico presencial en el Estado de Colima”**.

1.3 Preguntas de Investigación.

- ¿Cuál es el impacto estratégico de las acciones que realizan el IEEC, Gobierno del Estado de Colima, legisladores y partidos políticos, para motivar el uso de las TIC's en los diferentes escenarios, a través de los cuales se vinculan con la sociedad colimense?
- ¿El Estado de Colima cuenta con la infraestructura tecnológica, logística, legal y política necesaria, para desarrollar un modelo estratégico de votaciones electrónicas presenciales seguras, e implantarlo a mediano plazo?
- ¿Qué tan informada está la sociedad colimense con respecto a las votaciones electrónicas seguras?

- ¿Qué tecnologías de hardware y software se requieren para desarrollar un modelo estratégico de seguridad, para votaciones electrónicas presenciales, que apoyen al proceso democrático en el que participa la sociedad?
- ¿Cuáles son los algoritmos de seguridad más confiables, para soportar transmisión y encriptación de los datos, en una red de computadoras?
- ¿Cuáles son las políticas de seguridad informática más adecuadas para resguardar los sufragios, de acuerdo al entorno actual, que cumplan con los estándares internacionales?

1.4 Alcances y limitaciones del proyecto.

El alcance del proyecto es desarrollar un modelo estratégico de seguridad para las votaciones electrónicas presenciales en el Estado de Colima, a partir del análisis de la situación que prevalece en los ámbitos; gubernamentales, legislativos, políticos, sociales y tecnológicos.

El impacto geográfico se dará específicamente en el Estado de Colima.

Se dispone de dos años para la realización del proyecto, esperando concluirlo en agosto de 2011.

Se requiere traslado a la Ciudad de Colima para iniciar la investigación y aplicar encuestas que servirán de base para hacer el diagnóstico de la situación actual, en lo correspondiente a; gobierno del Estado, ayuntamientos, partidos políticos, legisladores, sociedad y desarrollo tecnológico.

Conforme se avance en la investigación, se necesitará mayor infraestructura computacional, por lo que en caso de no recibir apoyo del IIEC, la Universidad de Colima o la Universidad Popular Autónoma del Estado de Puebla (UPAEP), habría dificultades para culminar con éxito el proyecto.

1.5 Viabilidad de la Investigación.

Actualmente se tiene la autorización del Consejo General del IIEEC, encabezado por el Lic. Mario Hernández Briceño, para realizar esta investigación.

Por el momento se dispone de los recursos financieros y materiales para iniciar la investigación. Sin embargo, conforme se avance en el proyecto, será necesario trasladarnos a la ciudad de Colima para estar en contacto permanente con el gobierno del Estado, IIEEC, legisladores, partidos políticos y sociedad. Igualmente, realizar trabajo de campo, así como el análisis correspondiente de la información recopilada. De requerirse más equipo, se solicitará apoyo al IIEEC, Universidad de Colima y la UPAEP, esperando contar con una respuesta satisfactoria de dichas instituciones.

Así mismo, se buscará obtener apoyo económico a través de los diferentes fondos sectoriales del Consejo Nacional de Ciencia y Tecnología (Conacyt), del Consejo Estatal de Ciencia y Tecnología del Estado de Colima y de la Universidad de Colima.

La investigación se dividirá en las siguientes fases:

Fase 1 Marco teórico.

- Antecedentes del voto electrónico y su estado del arte.
- Conformación del Instituto Federal Electoral.
- Seguridad en los sistemas informáticos.

Fase 2 Investigación documental del voto electrónico en el mundo.

- Investigación documental en países del primer mundo y relación de indicadores de competitividad.
- Investigación documental en países en vías de desarrollo y relación de indicadores de competitividad.

- Impacto del uso del voto electrónico en las democracias donde se ha implementado esta tecnología.

Fase 3 Investigación documental de la administración de sistemas de información.

- Alienación de los sistemas informáticos y la planeación estratégica.
- Interpretación de la estrategia electrónica.
- Investigación documental de la cadena de valor virtual y las nuevas estrategias centradas en la tecnología.
- Planteamiento de las estrategias, partiendo del Diamante de Leavitt.

Fase 4 Planteamiento del modelo.

- Desarrollo del modelo teórico.
- Estrategias para implementar el modelo.

1.7 Esbozo del Marco Teórico.

1.7.1 Principios básicos de estrategia.

Una estrategia se puede definir como el conjunto de actividades encaminadas a lograr un objetivo. Porter (1985) define la estrategia como “una manera de competir que entrega valor único en un particular conjunto de usos o para un particular conjunto de clientes”. Mientras que Thompson y Strickland (2003) se refieren a la estrategia como “la dirección del plan de juego utilizada para establecer hacia fuera una posición del mercado, para conducir su operación, para atraer y satisfacer a clientes, competir con éxito, y para alcanzar los objetivos de la organización”.

Para establecer y mantener un distintivo posicionamiento estratégico, Porter (2001) estipula que “una compañía necesita seguir los siguientes seis principios fundamentales”:

- Debe iniciar con la *meta correcta*: rendimiento superior a la inversión a largo plazo. Sólo fundamentando la estrategia, en una rentabilidad sostenida, podrá generarse el valor económico real. El valor económico se crea cuando los clientes están dispuestos a pagar un precio por un producto o servicio que exceda el costo de producirlo.

- La estrategia de la compañía debe permitir entregar una *propuesta de valor*, o un conjunto de beneficios, diferente a lo que ofrecen los competidores.
- La estrategia necesita reflejarse en una *configuración diferente de valor*. Para establecer una ventaja competitiva sostenida, una compañía debe realizar diferentes actividades que sus rivales, o desempeñar actividades similares en formas diferentes.
- Estrategias robustas involucran *acuerdos*. Una compañía debe renunciar o ir delante de algunas características del producto, servicios, o actividades, para ser única que otros.
- La estrategia se define como todos los elementos que una compañía realiza *conjuntamente*. Una estrategia implica tomar decisiones a través de la configuración del valor que son independientes. Todas las actividades de la compañía se deben reforzar mutuamente.
- La estrategia implica la *continuidad* de la dirección. Una compañía debe definir una propuesta de valor que estará disponible, aún cuando eso significa prever ciertas oportunidades.

Según Chew y Gottschalk (Estrategia de la Tecnología de la Información y Administración, 2009), los elementos necesarios que una estrategia debe incluir son; “misión, visión, objetivos, estrategia de conocimiento, sistemas de información y tecnología de la información”.

- La **misión** describe la razón de existir de la compañía. Es un enunciado inequívoco de lo que hace la compañía y su propósito a largo plazo.
- La **visión** describe lo que la empresa quiere lograr. La visión representa el punto de vista a futuro que los altos ejecutivos tienen de la organización. Es en lo que se quieren convertir.
- Los **objetivos** describen dónde está encabezando el negocio. Los objetivos son el conjunto de logros mayores que servirán para alcanzar la visión. Son normalmente pequeños en número, pero incluyen los aspectos más importantes de la visión como; ganancias, servicio al cliente, excelencia en la fabricación, moral del personal, obligaciones sociales y ambientales.

- La **estrategia de conocimiento** se refiere a la capacidad que tienen las empresas para generar valor agregado, a partir de una serie de conocimientos, lo cual representa su ventaja competitiva.
- Los **sistemas de información** son un conjunto organizado de elementos que se comunican entre sí, ya sea en forma manual o automatizada para procesar datos, generar información y distribuirla oportunamente conforme a los objetivos de la organización.
- La **tecnología de la información** se refiere al estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados. Específicamente, del software de aplicación y equipos sofisticados (hardware) que ofrecen la capacidad de almacenar, procesar y transmitir datos.



Figura 1.1. Ejemplo de un modelo estratégico de negocios.

Fuente: http://www.bicecorp.com/portal_bicecorp/img/area_negocios.jpg

1.7.2 Administración estratégica.

La estrategia sin acciones no tiene valor en cualquier entidad. Para que se refleje a futuro, el efecto hacia dónde apunta la estrategia, la organización debe “administrar” la estrategia desde la formulación hasta la implementación y la realización de beneficios.

Esta disciplina es llamada *administración estratégica*. Incluye comprender la posición estratégica de una organización, las opciones estratégicas para el futuro y *moldear la estrategia dentro de la acción*.

Comprender la posición estratégica incluye; el impacto de la estrategia en el ambiente externo, recursos internos, competencias, expectativas e influencia de los partidos políticos, Organizaciones No Gubernamentales (ONG's) y sociedad en general. Las decisiones estratégicas contemplan comprender las bases subyacentes, para el futuro estratégico, tanto del gobierno y de los diferentes niveles jerárquicos que lo integran, así como las opciones para desarrollar la estrategia en términos de ambas direcciones, sobre las cuales debe moverse, más los métodos para desarrollarla.

Traducir la estrategia en acciones se lleva a cabo con el aseguramiento de que las estrategias están trabajando en la práctica. Una estrategia no es sólo una buena idea, una declaración o un plan. Es solamente significativa cuando actualmente se está poniendo en práctica (Johnson y Scholes, 2002).

La disciplina que se encarga de desarrollar la estrategia, en una serie de planes de acción, se llama *planeación estratégica*. La planeación estratégica es un subconjunto de la administración estratégica. Se enfoca en priorizar recursos para seleccionar planes de acción, coordinar y controlar las actividades para asegurar que el futuro visionario sea creado.

Thompson y Strickland (2003, p. 6) estipulan que “la administración estratégica es una combinación de procesos para la fabricación de la estrategia e implementación de la misma, lo cual compromete cinco tareas administrativas interrelacionadas”:

1. Desarrollar una visión estratégica y misión del negocio.
2. Establecer un conjunto de objetivos.
3. Diseñar una estrategia para alcanzar los objetivos.

4. Implementar y ejecutar la estrategia seleccionada eficientemente y eficazmente, para obtener los resultados deseados en las empresas.
5. Evaluar el desempeño y monitorear las políticas e implementación de los programas estratégicos, en los diferentes niveles de gobierno y oficinas descentralizadas. Iniciar ajustes correctivos en la visión, objetivos estratégicos, estrategia, o ejecución, según se necesite.

Como estas tareas están interrelacionadas, se necesita que no se realicen secuencialmente. La administración estratégica es un proceso en curso –no un evento de arranque (Thompson y Strickland, 2003). La estrategia y su implementación se adaptarán con la experiencia del desempeño, más los cambios en el entorno interno y externo de la administración pública.

Generalmente, hay algunas características de las decisiones estratégicas que son usualmente asociadas con la palabra estrategia (Johnson y Scholes, 2002):

- La estrategia es referida como la dirección a largo plazo de una organización.
- Las decisiones estratégicas están normalmente alrededor de intentar alcanzar los mejores indicadores de desempeño en el servicio público.
- Las decisiones estratégicas están referidas con el ámbito de las actividades del gobierno.
- La estrategia puede ser vista como el acoplamiento de los recursos y actividades del gobierno al servicio de la sociedad.
- La estrategia se puede considerar también como la construcción o expansión de los recursos y competencias de una organización, para crear oportunidades o para capitalizarlas.
- Las estrategias pueden requerir mayores cambios en los recursos para una organización.
- Las decisiones estratégicas probablemente afectan las decisiones operacionales.

- La estrategia de una organización es afectada no solamente por las fuerzas del entorno y la disponibilidad de los recursos, sino también por los valores y expectativas de quienes tienen el poder alrededor de una organización.

1.7.3 Planeación estratégica.

Traducir estrategias en acciones no es una tarea simple. *Primero*, es importante organizar para el éxito; la introducción de una estructura apropiada, procesos, relaciones y límites. *Segundo*, es importante para permitir el éxito en el manejo del personal; administrar información, administrar finanzas, administrar tecnología, y la integración de recursos. *Finalmente*, el cambio estratégico debe ser utilizado para; diagnosticar la situación del cambio, aplicar estilos y roles relevantes. Igualmente, implementar controles para administrar el cambio estratégico, tales como rutinas organizacionales y procesos simbólicos (Johnson y Scholes, 2002).

Los procedimientos de planeación estratégica representan diseñar el enfoque para administrar la estrategia. Tales procedimientos pueden tomar una forma altamente sistematizada, paso por paso, involucrando procedimientos cronológicos de algunas partes diferentes de la organización.

Algunos de los principales conceptos en planeación estratégica son; pensar a futuro, controlar el futuro, tomar decisiones, tomar decisiones integradas, más un procedimiento formalizado para generar un resultado, articulado en forma de un proceso integrado de decisiones.

Chew y Gottschalk (Estrategia de la Tecnología de la Información y Administración, 2009) definen a la planeación estratégica como “*el proceso de decisión sobre los proyectos que la organización emprenderá y la cantidad aproximada de recursos que serán necesarios para cada programa en los próximos años*”.

La planeación representa la extensión en la cual los tomadores de decisiones miran a futuro y usan metodologías formales de planeación. Planear es algo que hacemos antes de realizar alguna acción. Es tomar una decisión en forma anticipada. Tomamos decisiones antes de que se requiera la acción. El foco de la planeación gira alrededor de los objetivos, los cuales son el corazón del plan estratégico (Mintzberg, 1994).

En el caso de la administración pública, se deben considerar algunos factores externos, que pueden influir en el éxito y cumplimiento de las metas planeadas, en los tiempos esperados. Tal es el caso de:

- a) **Sindicatos.** Son parte inherente de la administración pública. Lo integran gran parte de la fuerza laboral, principalmente empleados de base. Las negociaciones realizadas en torno al salario, prestaciones y diversos problemas que los aquejan, pueden coadyuvar al desempeño armónico de las acciones, o por el contrario, entorpecer la actividad con huelgas o desempeño ineficaz en las actividades encomendadas.
- b) **Partidos políticos.** Las diversas organizaciones políticas ejercen presión en las decisiones que toma el gobierno. Así como en las políticas para el establecimiento de una correcta planeación. En ocasiones, influyen en el criterio de la sociedad para obstaculizar el desempeño del servicio público, a través de manifestaciones y cargas impositivas que sólo buscan favorecer sus intereses.

De acuerdo con Rossana Schiaffini (2006, pp. 98-99), los principales ordenamientos para la planeación en los estados son:

- **Elementos normativos de mediano plazo.**
 - Plan Estatal de Desarrollo.
 - Programas Regionales y Especiales.
 - Programas Institucionales.
- **Instrumentos operativos.**
 - Programas Anuales, Sectoriales, Institucionales y Municipales.
 - Leyes de Ingresos Estatal y Municipal.

- Presupuestos Anuales de Egreso Estatal y Municipal.
- Convenio de Desarrollo Social.
- Convenio de Desarrollo Estado-Municipio.
- Convenios de coordinación.
- **Elementos de control.**
 - Informes de las condiciones económica y social.
 - Informes de auditorías gubernamentales.
- **Instrumentos para la evaluación.**
 - Informes anuales.
 - Del Gobernador.
 - Presidentes Municipales.
 - Informes.
 - De los foros de consulta popular.
 - Sectoriales e institucionales.

1.7.4 Estrategia Electrónica (*E-Strategy*).

El Internet es una nueva tecnología extremadamente importante. No es sorprendente que haya recibido demasiada atención de los empresarios, ejecutivos, inversionistas y observadores de negocios.

Alcanzados por el fervor general, muchos han asumido que el Internet cambia todo, barriendo todas las viejas reglas acerca de las compañías y la competencia obsoleta. De acuerdo con Porter (2001), eso puede ser una reacción natural, pero es peligroso. Ha llevado a muchas compañías punto-com, y apoyado igualmente, a tomar malas decisiones que han erosionado el atractivo de sus industrias y minado su propia ventaja competitiva. El tiempo ha venido a cambiar el punto de vista de Internet.

El Internet proporciona una infraestructura global que permite; la compresión de tiempo y espacio, integrar cadenas de suministro, uniformar y customizar masas, más la habilidad para navegar. El impacto de Internet puede ser descrito como el rompimiento de los tradicionales acuerdos, entre la riqueza de la posible interacción con un cliente y el número de clientes que pueden acceder a un negocio o productos que pueden ofrecer.

Los negocios basados en Internet pueden competir en selecciones enormes de productos, que no tienen restricciones como las tiendas físicas. También una rica interacción, por ejemplo; checar el estado de la orden, buscar recomendaciones en línea, entre otros. Igualmente, customizar las relaciones con una gran cantidad de clientes, para que los costos incrementales sean cada vez más factibles con la economía de la información (Grover y Saeed, 2004).

La tecnología de Internet proporciona mejores oportunidades para que las compañías establezcan posicionamiento estratégico, diferente al de previas generaciones de tecnología de la información. El gran impacto de Internet ha permitido la reconfiguración de industrias existentes, que han sido condicionadas por los altos costos para; comunicarse, reunir información o realizar transacciones.

Kim et al. (2004) argumentan que:

una estrategia electrónica (*e-strategy*) permitirá un aseguramiento superior, un desempeño sustentable por una disciplina de “estrategia integrada” (cuando se compara cualquier diferenciación o liderazgo en costo). El cual se esfuerza para alcanzar tanto el liderazgo en costo y el posicionamiento de la diferenciación estratégica.

También sugieren que:

las empresas que se basan en la cantidad de “clics” que da un usuario en su sitio Web, disfrutarán de un desempeño superior, en relación con aquellas que solamente tienen un

contador de visitas, *sólo* cuando sus operaciones en línea y fuera de línea están alineadas y firmemente integradas.

Las características más sobresalientes de Internet, según Afuah y Tucci (2003) son:

- **Tecnología mediática.** El internet es una tecnología mediática que interconecta partes que son independientes o que quieren ser. La interconexión puede ser; negocio a negocio (B2B), negocio a cliente (B2C), cliente a cliente (C2C) o cliente a negocio (C2B). Esto puede ser también con una empresa o cualquier otra organización, en un proceso denominado intranet.
- **Universalidad.** La universalidad de Internet se refiere a la capacidad de Internet, tanto para ampliar y reducir el tamaño del mundo. Se agranda el mundo, porque cualquiera en cualquier parte del mundo puede, potencialmente, hacer sus productos disponibles para cualquier persona del orbe. Se encoge el mundo porque se reducen las distancias en las autopistas electrónicas.
- **Externaliza redes.** Una tecnología o producto presenta externalidades de red cuando se vuelve más valiosa a los usuarios, a medida que más gente se aprovecha de ella. Un ejemplo clásico es el teléfono, donde el valor de cada abonado aumenta con el número de suscriptores. Cuanta más gente esté conectada a una red en la Internet, el valor de la red se incrementa.
- **Canal de distribución.** Internet actúa como un canal de distribución para los productos que son en gran parte pedacitos de la información, tales como; software, música, vídeo, noticias, y boletos. No hay efecto de reemplazo si la Internet se utiliza para servir a los mismos clientes, atendidos por el viejo canal de distribución, sin traer nuevos clientes. Hay un efecto de extensión si el Internet es utilizado por más personas y para los nuevos servicios.
- **Moderador de tiempo.** La quinta propiedad de la Internet es la moderación del tiempo, o su capacidad para reducir y ampliar el tiempo. Se reduce el tiempo para los clientes que desean información sobre los productos que, en las tiendas regulares, no tienen la difusión necesaria. Se amplía el tiempo cuando el trabajo relacionado se puede hacer en diferentes momentos.

- **Encoge la asimetría de la información.** Una asimetría de la información existe cuando una de las partes, en una transacción, tiene información que la otra no maneja. Información que es importante para la transacción. La web reduce las asimetrías de información, tal como la otra parte pueda encontrar la misma información en la web.
- **Capacidad virtual infinita.** El acceso a Internet se percibe como ilimitado. No tiene que esperar en una larga fila. Por ejemplo, las comunidades virtuales como el chat-casas, tienen una capacidad infinita para los miembros que se pueden comunicar, en cualquier momento del día, durante todo el tiempo que quieran.
- **Bajo costo estándar.** Las empresas no pueden aprovechar las propiedades de Internet si no lo adoptaron. Por dos razones, la adopción ha sido fácil. Lo primero y más importante, el Internet y la Web son estándares abiertos a todos, en todas partes. Son de uso muy fácil de usar. En segundo lugar, el costo de la Internet es mucho más bajo que el de los medios anteriores, es decir, las comunicaciones electrónicas.
- **Destructor de la creatividad.** Estas propiedades de la Internet han permitido el comienzo de una ola de destrucción creativa en muchas industrias. La prensa, por ejemplo, que tiene dificultades para ofrecer a sus lectores materiales en sus sitios Web. El Internet es un tipo de estándar de imprenta de bajo costo, con una red de distribución en capacidad ilimitada, que llega a más personas que cualquier periódico podría esperar alcanzar. Esto destruye una gran parte de las barreras de entrada que existen en el negocio de los periódicos.
- **Disminuye los costos de las transacciones.** El Internet también reduce costos de transacciones para algunas industrias. Gracias en parte a la universalidad, por los canales de distribución, el bajo costo estándar y propiedades de reducción de asimetría de la información. El costo de las transacciones son los costos en la búsqueda de vendedores y compradores. Implica recolectar información en productos. Permite la negociación, escribir, monitorear y la aplicación de contratos. Facilita el costo, asociado con la transportación entre compradores y vendedores.

En un amplio estudio de organizaciones en Norte América y Europa (Andal et al, 2003) identificaron los diferentes controladores, que determinan la ventaja competitiva para

desarrollar nueva tecnología de la información. Cada uno de los controladores es muy específico sobre cómo las nuevas TIC's pueden aplicarse en una entidad particular.

No son factores generales como el costo excesivo de una tecnología. Son diferentes de los factores críticos de éxito, que afectan la implementación de la tecnología de la información. Los que son bastante específicos para una organización, en comparación con lo que distingue a una industria.

Hay 10 controladores que ayudan a determinar una apropiada estrategia electrónica:

- **Entrega electrónica.** Algunos productos tienen componentes grandes que se pueden entregar por vía electrónica. Las compañías aéreas, por ejemplo, permiten a los clientes de reservaciones en línea, después de lo cual puede ser la confirmación y los boletos entregados de manera eficiente, a través del correo electrónico.
- **Intensidad de la información.** Casi todos los productos y servicios tienen un cierto contenido de la información, pero la cantidad varía dramáticamente. Hay coches que vienen con un volumen de instrucciones de operación, por ejemplo.
- **Customización.** La nueva tecnología de información permite, a muchas empresas, adaptar una oferta global a las necesidades específicas y preferencias de los clientes individuales. En el pasado, los periódicos eran de un solo tamaño para todos los productos. Hoy en día, las ediciones en línea se pueden personalizar para incluir sólo las noticias y la información de un suscriptor en particular, que es probable que desee.
- **Efectos de agregación.** Los productos y servicios difieren en la forma en que se pueden agregar o combinar. Gracias a la tecnología de la información, las instituciones pueden ofrecer a sus clientes paquetes de servicios.
- **Búsqueda de costos.** Antes de la llegada de empresas de Internet, como amazon.com, encontrar una salida de datos de impresión podía requerir mucho tiempo y esfuerzo. Ahora, la web ofrece a las personas con grandes cantidades de información, independientemente de su ubicación o zona horaria, la reducción de los costos de búsqueda para encontrar exactamente el producto o servicio que desea.

- **Interfaz en tiempo real.** Una interfaz en tiempo real es necesario para las empresas y los clientes que ocupan de la información importante que cambia de repente y de manera impredecible. Un buen ejemplo es el comercio en línea, en los que cambios rápidos en el mercado de valores puede ser devastador para aquellos que no tienen acceso instantáneo a la información.
- **Contracción del riesgo.** Comprar libros en línea tiene poco riesgo de contratación para los clientes. Los precios son relativamente bajos, y especificar el título exacto es sencillo. Comprar en línea los coches es completamente diferente. Los precios son sustancialmente más altos
- **Efectos de red.** En muchas industrias, la utilidad de un bien o servicio aumenta con el número de personas que lo utilizan, o uno que sea compatible. Un beneficio clave de la utilización de Microsoft Office, por instancias, es que el conjunto de programas es ubicua en el mundo de negocios, permitiendo a la gente compartir documentos con facilidad, en programas de; Word, PowerPoint, Excel, entre otros.
- **Beneficios de la estandarización.** Las nuevas tecnologías de la información permitieron a las empresas sincronizar y estandarizar los procesos determinados. Lo que resulta en una mayor eficiencia para la transacción de negocio a negocio, así como una mayor comodidad para los clientes.
- **Debilita a la competencia.** Las nuevas tecnologías de la información pueden facilitar a la compañía alianzas, en las cuales los socios usan uno del otro para llenar sus deficiencias.

Estos 10 controladores se pueden clasificar en tres tipos. Los primeros cuatro controladores son características inherentes al producto o servicio. Los controladores 5-7 se refieren a las interacciones entre la organización y sus clientes. Mientras que los últimos tres se refieren a las interacciones entre la empresa, sus socios y competidores.

1.7.5 Alineación estratégica.

La alineación entre la estrategia de la organización y la estrategia de TIC's es ampliamente creíble para mejorar el desempeño de la entidad (Sabherwal y Chan, 2001). Por lo tanto, la alineación estratégica es una preocupación, tanto de los altos ejecutivos, como una importante característica de los atributos de efectividad en los niveles gerenciales. Mientras que la estrategia de la organización es el modelo más amplio de las decisiones, para asignar recursos, las decisiones más específicas están relacionadas con sistemas de información y plataformas tecnológicas.

Los sistemas de información deben ser vistos tanto en un contexto organizacional, como tecnológico. Los sistemas de información están a la mitad, porque soportan las organizaciones, mientras utilizan plataformas tecnológicas.

La estrategia de la organización está relacionada con el aseguramiento de la misión, visión y objetivos de una entidad. Mientras que la estrategia de SI se refiere al uso de aplicaciones de sistemas de información. Donde la estrategia tecnológica está relacionada con la infraestructura técnica. Ambas alineadas, desde luego, con la estrategia de la organización.

Una estrategia de SI/TI es una estrategia combinada, incluyendo; el contexto de la organización, los sistemas de información en un sentido estrecho, y la plataforma tecnológica. Los elementos necesarios de una estrategia de SI/TI incluyen; la dirección de la empresa y la estrategia (misión, visión, objetivos, estrategia del conocimiento), aplicaciones (sistemas de administración del conocimiento), gente (la competencia futura de recursos humanos), organización (futuro de la organización y control de la función de TI), más plataforma tecnológica (futuro de la infraestructura técnica). Por lo tanto, SI/TI es un término absolutamente amplio, por lo que se debe tener cuidado de todas las conexiones e interdependencias en una estrategia, así como en los cambios de un elemento que podrían tener efecto en otros elementos, como se muestra en la Figura 1.2.



Figura 1.2. Elementos de la estrategia de SI/TI y sus interdependencias.

Fuente: Chew y Gottschalk. Estrategia de la Tecnología de la Información y Administración (p. 76).

Actualmente, las organizaciones que alinean sus estrategias de negocio, con las estrategias de SI/TI, deben considerar un espectro más amplio, para tener éxito en todas las aristas incluidas en su plan estratégico. Ya que se deben involucrar completamente en un entorno cooperativo, como se muestra en la Figura 1.3 en el diamante de Leavitt .

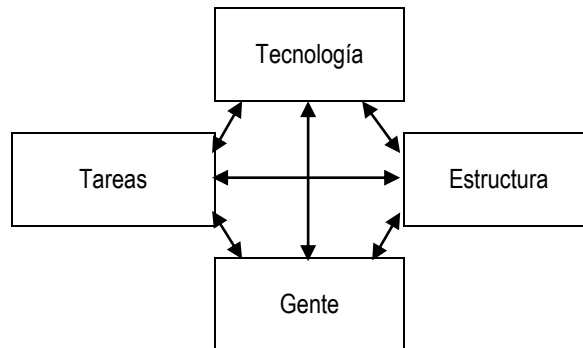


Figura 1.3. Elementos del diamante de Leavitt y sus interrelaciones.

Fuente: Chew y Gottschalk. Estrategia de la Tecnología de la Información y Administración (p. 76).

1.7.6 Transformación de las empresas mediante la innovación operacional.

La innovación operacional implica apartarse de las normas conocidas. Requiere de grandes cambios en la forma como los departamentos ejecutan su trabajo y se relacionan entre sí. Es un cambio verdaderamente profundo, que afecta la esencia misma de una empresa y su manera de trabajar. Los efectos de la innovación operacional se propagan hacia todos los aspectos de la organización. Desde los sistemas de medición y compensación, hasta los perfiles de cargos, la estructura organizacional y el rol jerárquico.

Por lo tanto, nunca despegará sin el liderazgo de los ejecutivos. Pero los altos niveles jerárquicos, rara vez consideran la innovación operacional como una tarea importante. Ni la reciben con entusiasmo cuando otros les presentan la idea. ¿Por qué no? Las respuestas están en algunas de las características desagradables del liderazgo empresarial contemporáneo:

- Las actividades rutinarias subestiman a las operaciones.
- Las operaciones están fuera del radar visual (y mental).
- Nadie es dueño de la innovación operacional.

En las iniciativas de innovación operacional, lo más común es que partan como un movimiento, desde las bases, fomentado por personas dispersas a lo largo de la organización. Profundamente comprometidas en descubrir y explotar oportunidades de innovación operacional. Estos catalizadores asumen la tarea de encontrar un líder capaz de captar lo que tiene en mente y de encabezar la iniciativa de innovación.

El funcionario debe tener la imaginación y el carisma necesario para impulsar grandes cambios operacionales. Luego, los catalizadores hacen campaña incesante a favor de su causa, exponiendo al funcionario las falencias de las operaciones existentes. Organizan reuniones con colegas de otras empresas, que han implementado con éxito innovaciones operacionales, para lo cual se deben realizar las siguientes actividades:

- Buscar modelos fuera de su sector.
- Identificar y desafiar las premisas limitantes.
- Convertir un caso especial en regla general.
- Repensar las dimensiones críticas del trabajo.

1.7.7 Perspectiva estratégica de la democracia electrónica.

La democracia electrónica es un nuevo fenómeno. Invita a los ciudadanos para que aprendan cómo utilizarlo. Una jerarquía de habilidades desarrolladas (conocer qué, conocer cómo, conocer por qué, por qué cuidarlo) provee una base de trabajo, para guiar el proceso de aprendizaje.

Una estrategia para la realización del voto electrónico es sugerida por Watson y Mundy (*Communications of the ACM*, 2001). Involucra cuatro fases:

- Iniciación (conocer qué).
- Infusión (conocer cómo y conocer por qué).
- Customización (por qué cuidarlo).

1.7.8 Dimensiones del voto electrónico.

Prosser y Krimmer (2003) proponen un modelo para el voto electrónico, que contempla los siguientes aspectos:

- **Políticas.** En este campo es importante conocer el tipo de sistema político encontrado, como; monarquía constitucional, democracia parlamentaria, entre otros. Asimismo, el método, frecuencia de las elecciones, así como estadísticas generales sobre elecciones, por ejemplo; votantes elegibles, distritos electorales y número de colegios electorales.

- **Leyes.** Tiene que ver con la Ley Electoral, específicamente con las bases para la solución electrónica. En el caso de México, se debe revisar también la legislación electoral y hacer las modificaciones necesarias para que ésta tenga sustento. Para la existencia del voto electrónico, los principios legales para las elecciones son importantes. Lo mismo, la manera en que el voto electrónico es y debe ser implementado. Además, en qué nivel está el voto electrónico en el proceso de elaboración de la legislación.
- **Tecnología.** Es importante conocer el estado de los registros en general. En especial, un registro de ciudadanos y como subgrupo, aquellos que son elegibles para votar. Además de la importancia de las preguntas sobre infraestructura tecnológica, están; la implementación de una tarjeta digital de identificación nacional, de la firma digital, y verificar si la adopción de estándares internacionales para el voto electrónico están planeados. También es interesante conocer el nivel de gobierno electrónico ofrecido en general.
- **Sociedad.** Se debe concentrar básicamente en el nivel de participación política, los votos por correo postal, la actitud pública hacia las nuevas tecnologías y el voto electrónico en particular. Es también necesario conocer el radio de penetración de teléfonos, teléfonos celulares, computadoras personales, el Internet, incluyendo su acceso a banda ancha. Finalmente, las transacciones que realiza la sociedad a través de Internet.

1.7.9 Votaciones electrónicas.

Desde 1960 se han venido utilizando los sistemas de votación electrónica para elecciones, cuando se empezaron a utilizar las tarjetas perforadas (Bellis, n. d.). A través de los sistemas de escaneo óptico, una computadora puede contabilizar los votos que han marcado los electores en las boletas.

Por ejemplo, durante las elecciones en Brasil, se utilizan máquinas para votar de Registro Electrónico Directo (DRE) para almacenar y contabilizar los votos en un solo dispositivo. Algo similar se presenta en la India, Venezuela y Estados Unidos.

Introducción.

Con el desarrollo de las TIC's, el sector público se ha beneficiado con la implementación de diferentes sistemas automatizados, que permiten ofrecer servicios eficientes y confiables a los ciudadanos.

En algunos estados de la República Mexicana como; Coahuila, Estado de México y Jalisco, se han empezado a utilizar prototipos a la par del sistema tradicional durante los procesos electorales. Lo anterior, para que el ciudadano vote electrónicamente, con el propósito de recoger experiencias que servirán de base para configurar, en el mediano plazo, un sistema totalmente automatizado, a través del cual los electores puedan ejercer su derecho a votar. Esto contribuirá significativamente para que la sociedad conozca, en menos tiempo y con altos niveles de confiabilidad, quiénes han sido los ganadores de la contienda.

Además del esquema de seguridad, bajo el cual deberá operar el sistema, se requiere de un mecanismo alternativo para verificar la consistencia de los datos almacenados, en la base de datos, al finalizar las votaciones, con el número de boletas que físicamente se encuentran en las urnas. Las boletas deberán ser expedidas por el mismo sistema. Para introducirlas en las urnas, deberán cumplir con diferentes parámetros para aceptarse como válidas.

Voto electrónico.

Al voto electrónico se le conoce también como e-voto (*e-vote*). Es un concepto amplio que abarca varios tipos de votación, ya sea tanto las maneras electrónicas de emitir los votos, como los medios electrónicos para contar los votos.

De acuerdo con Arévalo, Garzón y Roa (2003, p. 354), se deben tomar en cuenta dos aspectos para definir al voto electrónico. Por un lado, viéndolo desde el punto de vista amplio, implica la referencia a todos los actos electorales, factibles de ser llevados a cabo apelando a la tecnología de la información. Incluyen; el registro de los electores, la gerencia, administración y logística electoral, el ejercicio del voto, finalizando con los escrutinios, transmisión de los resultados, más la certificación oficial. Desde una perspectiva restringida, se refiere exclusivamente al acto de votar a través de máquinas electrónicas.

Análisis del voto electrónico.

Con respecto a otras técnicas de votación, los sistemas de voto electrónico pueden ofrecer ventajas importantes. Por lo general, estos métodos incluyen; las etapas de instrumentación, distribución, ejercicio del voto, recolección y escrutinio de las boletas. En cada una de las etapas, se pueden incorporar las TIC's para que el proceso sea más rápido, eficaz y seguro.

Sin embargo, a pesar de los beneficios que se obtienen al utilizar la tecnología en los procesos electorales, hay desventajas potenciales, como las fallas o debilidades de algún componente electrónico en algún momento. Al volverse más complejos e incluir software, los sistemas de votación siguen siendo vulnerables al fraude electoral, a la alteración física de las máquinas o dispositivos utilizados durante los sufragios.

Desde el punto de vista teórico, hay gente que cuestiona el uso del voto electrónico. Afirman que la sociedad no tiene la infraestructura suficiente para verificar el funcionamiento de las máquinas electrónicas, por lo tanto, no se puede confiar en ellas.

El especialista en criptografía, Bruce Schneier (2004, p. 84), afirma que “para asegurar que los electores puedan votar honestamente, ellos necesitan anonimidad, para lo cual se requiere una boleta secreta para votar”. Sugiere el uso de una máquina computadora de votos, que cuando el ciudadano vote, imprima una boleta de papel, porque los votos “oficiales”, como él les

llama, pueden utilizarse en los recuentos, ya que la computadora solamente proporciona una cuenta inicial rápida.

No se sabe en qué momento una computadora puede fallar. Por lo tanto, deben considerar un esquema manual alternativo, que permita verificar la confiabilidad de los resultados proporcionados por la máquina.

Requerimientos para el voto electrónico.

Un sistema para el voto electrónico debe considerar los siguientes requerimientos, como mínimo (Aceproject, 2008):

- Asegurarse de que solamente las personas con derecho a votar puedan emitir un voto.
- Asegurarse de que cada voto lanzado se contabilice y que cada voto se cuente solamente una vez.
- Mantener los derechos del votante para formar y expresar su opinión en forma libre, sin cualquier coerción o influencia indebida.
- Proteger el secreto del voto en todas las etapas del proceso de votación.
- Garantizar la accesibilidad a tantos votantes como sea posible, especialmente con respecto a las personas con discapacidades.
- Aumentar la confianza del votante, maximizando la transparencia de la información en el funcionamiento de cada sistema.

Implicaciones.

Llevar a la práctica un sistema para votar electrónicamente no es una labor sencilla. Requiere de una planeación exhaustiva por sus características particulares, para aspirar a obtener resultados satisfactorios.

De acuerdo con Schneier (2004), un sistema de votación debe cumplir con las siguientes características:

1. **Exactitud.** La meta de cualquier sistema para votar es establecer el intento para que cada individuo pueda votar, traduciendo esos intentos en una boleta final. Esta característica también incluye la seguridad. Debe ser imposible cambiar alguno de los votos, materiales de las papeletas para votar, destruir votos o de lo contrario afectará la precisión del conteo final.
2. **Anonimato.** Las votaciones secretas son fundamentales para la democracia. Los sistemas para votar deben ser diseñados para facilitar el voto anónimo.
3. **Escalabilidad.** Los sistemas para votar deben ser capaces de soportar elecciones muy largas. Específicamente, aquellas donde la participación de los ciudadanos es bastante considerable. El sistema debe seguir funcionando sin ningún problema, a pesar del crecimiento exponencial de su base de datos.
4. **Velocidad.** Los sistemas automatizados para votar deben producir los resultados rápidamente. Eso es particularmente importante en los Estados Unidos, donde la gente espera conocer los resultados el día de las elecciones, antes de irse a dormir.

Países con proyectos de votaciones electrónicas.

A continuación indicamos algunos países donde se están trabajando diferentes proyectos de votaciones electrónicas (Aceproject, 2008). Ver Tabla 1.2:

Tabla 1.2. Clasificación de países y tecnología que usa para voto electrónico.

| País | Tipo de tecnología. |
|--|--|
| Alemania, Australia, Canadá, España, Estados Unidos, Estonia, Francia, Reino Unido, Suiza, Unión Europea (Proyecto CyberVote). | Voto electrónico remoto. |
| Australia, Bélgica, Brasil, Estados Unidos, Francia, India, Irlanda, Noruega, Portugal, Reino Unido, Unión Europea (Proyecto CyberVote). | Recipiente para el registro de votos electrónicos. |

Fuente: Elaboración propia, a partir del reporte de Aceproject (2008).

Seguridad en las urnas electrónicas.

Actualmente, uno de los grandes problemas que hay en el mundo informático es la seguridad de los datos, su transmisión y protección. Así como evitar el ingreso de intrusos a los sistemas de información.

En general, para las empresas de gobierno o privadas, lo máspreciado es la información, porque les permite tomar decisiones eficaces de manera oportuna, ya sea para manejo de personal, mercancías, flujo de efectivo, inversiones, entre otros. La seguridad informática incluye la parte física que abarca; los edificios, instalaciones eléctricas, protección del equipo, software adecuadamente configurado y protegido con las herramientas pertinentes, como; antivirus, paredes de fuego y filtros. En el caso de los servidores y equipos principales; el empleo de zonas de seguridad, paredes de fuego empresariales, detección de intrusos e informática forense, en algunos casos. La Figura 1.4 ilustra un esquema de seguridad informático.

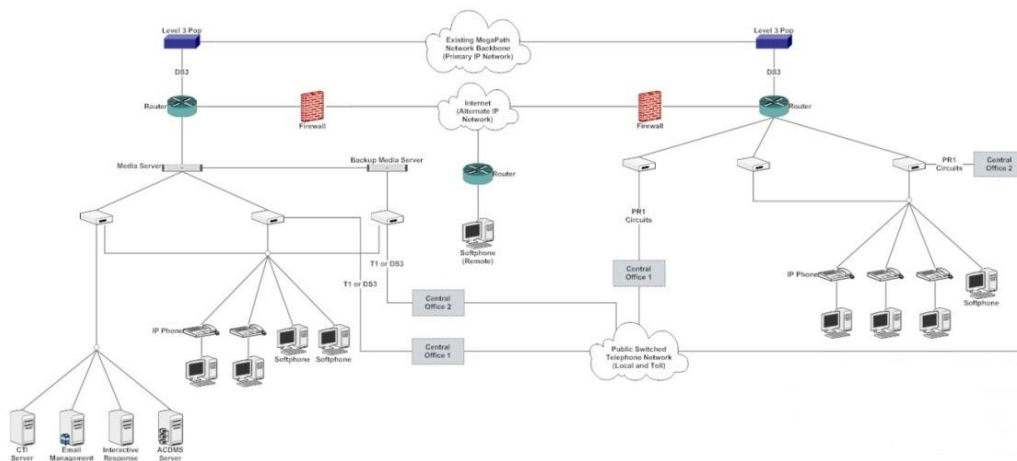


Figura 1.4. Elementos de seguridad del entorno informático.

Fuente: Propia.

Slykey Bélanger (2003) definen amenaza informática como: “*Las circunstancias, condición o evento con el cual se causa un daño económico a los datos o recursos de red, en forma de*

destrucción, modificación de datos, denegación de servicio y/o fraude, pérdida y abuso”. Así pues, se habla de condiciones que permiten la realización de dichos ilícitos, como por ejemplo;

- a) Configuración inadecuada de los equipos, red, software o algún otro componente informático.
- b) Funcionamiento inadecuado de los principales sistemas de defensa como: *routers*, servidores, paredes de fuego y detección de intrusos, comúnmente llamados “agujeros” de seguridad. Por donde personas no autorizadas se filtran para modificar áreas de envío de paquetes de red (correos, paquetes web, paquetes no maliciosos que buscan saturar el ancho de banda, entre otros).
- c) Poca o nula capacitación de los usuarios al aceptar o abrir archivos que contengan código malicioso que puede mover archivos, destruirlos, o en el peor de los casos, dañar por completo el equipo. Por esta razón, dejan de operar correctamente áreas completas en donde los usuarios comparten impresoras, directorios o carpetas y archivos, que al abrirse, provocan daño en efecto dominó.
- d) Fraudes por correo apócrifo, páginas web fantasma (estafa mediante *phishing*), malware, códigos ocultos empotrados en páginas web.
- e) Falta de actualización del software, ya sean parches del sistema, antivirus, paredes de fuego, anti-spy, entre otros, que son la principal causa de caídas de los sistemas personales.

Slykey Bélanger (2003) definen privacidad como: “*La capacidad para gestionar la información sobre sí mismo*”. En una economía global, basada en el flujo transaccional e intercambio de la información, la privacidad constituye un elemento fundamental en la atención a los clientes.

Las políticas usadas por los diferentes entornos informáticos, para el manejo de la información, deben ser claras y precisas. Esto como una condición estrictamente empresarial.

En este sentido, el Departamento de Seguridad de Cómputo de la Universidad Nacional Autónoma de México establece lo siguiente (UNAM-CERT, 2008):

- **Política de Privacidad.** Antes de enviar su nombre, dirección de correo electrónico, u otra información a un sitio web, verifique la existencia de la política de privacidad. Esta política debe indicar cómo la información será usada, y si la información será o no distribuida a otras organizaciones. Las organizaciones, algunas veces comparten información con socios que ofrecen productos relacionados u ofrecen opciones de suscripción a listas de correo en particular. Busque las indicaciones que en efecto le estén agregando a las listas de manera automática. La imposibilidad para no seleccionar estas opciones, pueden conducir a recibir correo SPAM. Si no encuentra una política de privacidad en el sitio, considere el contactar a la compañía para solicitarle información acerca de la política, antes de enviar información personal, o busque un sitio alternativo. Las políticas de privacidad en ocasiones cambian, por lo que debe revisarlas periódicamente.
- **Evidencia de que su información está siendo cifrada.** Para protegerse contra el robo de información, por parte de atacantes, cualquier tipo de información personal que envíe por la red debe estar cifrada. De forma tal que sólo pueda ser leída por el recipiente apropiado. Muchos sitios utilizan SSL (*Secure Sockets Layer*), para cifrar la información. Un indicativo de que la información será cifrada, es que el URL inicie con *https:* en lugar de *http*. Además, que un ícono en forma de candado cerrado aparezca en la esquina inferior derecha del navegador. Algunos sitios indican también si los datos están cifrados cuando se almacenan. Si los datos se cifran en tránsito, pero se almacenan de manera insegura, un atacante puede comprometer el sistema del vendedor y podría tener acceso a su información personal.

Así mismo, los usuarios deben estar al pendiente de su “propia seguridad”. Las empresas en general deben habilitar a sus empleados para que manejen adecuadamente los diferentes esquemas informáticos. Esto es, que el compromiso sea bilateral y no solamente de la entidad

que brinda el servicio. De esta manera se fomenta la alfabetización informática y las empresas podrán estar seguras de que la información es manejada correctamente.

En lo que respecta a controles empresariales, se debe iniciar con la protección de la frontera con el mundo informático exterior. Asegurándose que esté blindada ante ataques o ingresos no autorizados. Para ello, es necesario invertir en la seguridad de equipos, como; servidores de alto rendimiento, sistemas operativos con elevados esquemas de seguridad integrados, software y hardware para la detección de intrusos. Igualmente, equipos que soporten la configuración de redes privadas virtuales, accesos remotos protegidos, así como el intercambio de llaves para garantizar la protección.

Software y hardware que lo integran.

Los elementos de software y hardware que se requieren para desarrollar un modelo de votaciones electrónicas son:

- Una interfaz para votar, la cual se puede elaborar utilizando el lenguaje de programación XML.
- Elementos Web de uso común.
- Un sistema de gestión de base de datos, como; MySQL, SQLServer u Oracle.
- Software de seguridad.
- Encriptación e implementación de candados al vuelo.
- Una PC habilitada para votar electrónicamente.
- Un sistema de transmisión alámbrico o inalámbrico.
- Una fuente de alimentación ininterrumpida (*no-break*), para evitar las caídas de sistema.
- Habilitar una zona segura para votar, donde sólo tenga acceso el votante. Aquí se puede incluir alguna mampara blindada contra reflejos o accesos visuales, para protección del interesado.

Niveles y tipo de seguridad.

El primer nivel que se debe cuidar, es la seguridad física de los equipos y las instalaciones. Iniciando con las especificaciones de las instalaciones físicas y ubicación de los módulos informáticos. Por otro lado, el suministro de energía debe cumplir con normas estrictas como son (Zacker, 2004):

- a) Líneas de suministro reguladas.
- b) Líneas de suministro alternativas y auxiliares.
- c) Cableado estructurado, tanto en señalizaciones como en red, que no se confundan.
- d) Tierras físicas de acuerdo a las normas y uso que se le dará al suministro.

Al mismo tiempo, no hay que olvidar las amenazas naturales, como por ejemplo:

- a) Incendios accidentales, tormentas e inundaciones.
- b) Amenazas ocasionadas por el hombre.
- c) Disturbios y sabotajes (internos y externos) deliberados.

En el segundo nivel, se encuentra la seguridad lógica. La integran los controles y políticas, bajo las cuales se debe desarrollar el proceso de votación electrónica, el flujo de la información, control de cuentas de usuario, así como el mapeo de los servicios.

De esta manera, se podrá:

- a) Restringir el acceso a programas y archivos.
- b) Asegurar que los operadores trabajen bajo una supervisión minuciosa y no puedan modificar los programas o archivos que no correspondan.
- c) Asegurar la utilización de datos, archivos y programas correctos en el procedimiento que corresponda.
- d) Recibir la información transmitida sólo por el destinatario al que se envió y no a otro.
- e) Asegurar la consistencia entre la información recibida y la que se envió.

- f) Disponer de sistemas alternos de transmisión entre diferentes puntos.
- g) Disponer de un programa de contingencias para la transmisión de datos.

Tener control de los usuarios que ingresan al sistema principal y módulos secundarios, son funciones básicas de los administradores de red. Es necesario definir la jerarquía de los usuarios, para que no puedan vulnerar la seguridad del mismo. Algunas de las políticas que debe establecer el responsable de la red son (Raya & Raya, 2001):

- a) Definir roles de los usuarios.
- b) Tipo de transacciones que realizará.
- c) Limitación de servicios.
- d) Modalidad de los accesos.
- e) Ubicación y horario.
- f) Control de acceso y seguimiento de acciones.
- g) Administración.

El estándar de seguridad más utilizado a nivel mundial es el TCSEC (*Trusted Computer System Evaluation Criteria*), llamado comúnmente *Orange Book* o libro naranja. Fue desarrollado en 1983, de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos. Los niveles describen diferentes tipos de seguridad del sistema operativo y se enumeran desde el mínimo hasta el máximo. Esto ha servido de base para desarrollar los estándares europeos ITSEC/ITSEM (*Information Technology Security Evaluation Criteria/Information Technology Security Evaluation Manual*). Así como los mundialmente conocidos ISO (*International Organization for Standardization*) e IEC (*International Electro technical Commission*).

Identificación de los principales tipos de ataques.

Para que el diseño e implementación de la urna electrónica sea posible, es necesario documentarse lo suficiente. También, adquirir experiencia sobre los diferentes tipos de ataques cibernéticos que pueden poner en riesgo la seguridad y confiabilidad del proceso. Saber cómo prevenirlos o cómo bloquearlos, cuando el equipo está operando. A continuación, se mencionan algunos de los ataques más populares sobre una red de computadoras.

Sniffer (Programa de monitoreo).

Una PC, o estación de trabajo en modo regular, envía y recibe paquetes, siempre y cuando correspondan a su interfaz de red. En caso contrario, el ruteador los deja pasar hacia otro segmento de la red, provocando que nunca lleguen a su destino y se destruyan. Sin embargo, es posible configurar un software que envía datos de la tarjeta de red, en modo promiscuo, para estar capturando información de otras estaciones, sin importar su destino. En caso de que las demás computadoras no tengan alguna protección de envío-recepción, existen altas posibilidades para que dicha información sea vista por el *sniffer*.

Scanners.

Un scanner generalmente analiza un segmento de red, o una estación de trabajo, para buscar protocolos o puertos abiertos que sean vulnerables. Estos descuidos ocasionan muchos problemas a corto y mediano plazo, por ejemplo;

- Permisos laxos o erróneos para archivos.
- Cuentas predeterminadas.
- Entradas de UID (identificador de usuario) erróneas o duplicadas.

***Spoofing* (Engañando).**

Este ataque es muy común y se produce cuando se autentifica una computadora, utilizando paquetes falsos de un host confiable. Las técnicas de engaño se basan en:

- **Spoofing de IP.** Se sustituye la dirección IP, origen de un paquete TCP/IP, por otra dirección con la cual se quiere enmascarar. Esto se puede realizar mediante programas como; mendax, spoofit o ipsnoop. Este tipo de spoofing, junto con el uso de peticiones de broadcast, a diferentes redes, se utiliza para hacer lo que se conoce como flood (ataque Smurf).
- **Spoofing de ARP.** Se suplanta la identidad usando las tablas ARP. Se construye por tramas de solicitud y respuesta ARP, modificadas. Con el objetivo de falsear la tabla ARP de una víctima y forzarla a que envíe los paquetes a un host atacante, en lugar de hacerlo a uno legítimo. Lo anterior se realiza cuando el host que recibe el ataque, confía en la petición hecha por el host atacante, pues está confundido. No hay manera de validarlo, a menos que exista alguna forma de defensa.
- **Spoofing de DNS.** El intruso pone en peligro el servidor de DNS y modifica explícitamente las tablas IP del nombre de Host. Estos cambios se graban en las bases de datos de las tablas de traducción del servidor DNS. Así, cuando el cliente solicita una búsqueda, recibe una dirección falsa. Esta dirección sería la dirección IP de una máquina que estuviera bajo el control total del intruso.

Algoritmos criptográficos.

Como cualquier esquema de seguridad, este método utilizado para cifrar y descifrar datos, también es susceptible de ataques. Existen tres formas de atacar un algoritmo criptográfico:

- **Ataques contra el protocolo.** Un sistema es tan sólido como sus algoritmos de cifrado y las funciones de transformación del código en los que está basado. Al violar

cualquiera de ellos, se viola el sistema entero. Es posible diseñar un sistema con esquemas de cifrado débiles, lo que propicia que sea demasiado fácil desdoblarlo. Por lo tanto, de vulnerar el sistema.

- **Ataques contra el algoritmo.** El algoritmo o las operaciones matemáticas que se ejecutan en los datos podrían debilitar todo el sistema. Los algoritmos de cifrado propietarios no hacen que un sistema sea más seguro. La mayoría han demostrado ser débiles. El uso de claves débiles y de una cantidad pequeña de datos, además de la alteración de funciones de transformación de código, contribuye al debilitamiento del sistema.
- **Ataques contra la implementación.** Algunas implementaciones dejan rastro, como pequeños archivos en memoria, que son las migajas que cualquier *hacker* necesita para vulnerar la seguridad. Otro punto débil, es la inadecuada combinación de claves. Aunque no necesariamente sea más seguro usar muchas combinaciones. Se debe revisar el tipo de combinación, temporalidad y espectro que tiene la implementación.

De número aleatorios.

Este tipo de ataque se da cuando el generador de números aleatorios repite la semilla. Ocurre en sistemas limitados que tienen poco espacio en su manejo de RGN, por lo que el agresor puede obtener la función inversa de números en ciclos cortos. Actualmente, se puede decir que este problema ya se superó, porque técnicamente la computadora es un generador infinito de números, a partir del nuevo espacio de procesamiento.

Pretty Good Privacy (PGP).

Esta implementación es de las más confiables. Los ataques PGP han sido a la implementación y no al protocolo, lo que da un espectro de alta seguridad. Se realiza mediante ventanas que husmean, pero sin llegar al origen de los datos, como se ilustra en la Figura 1.5.

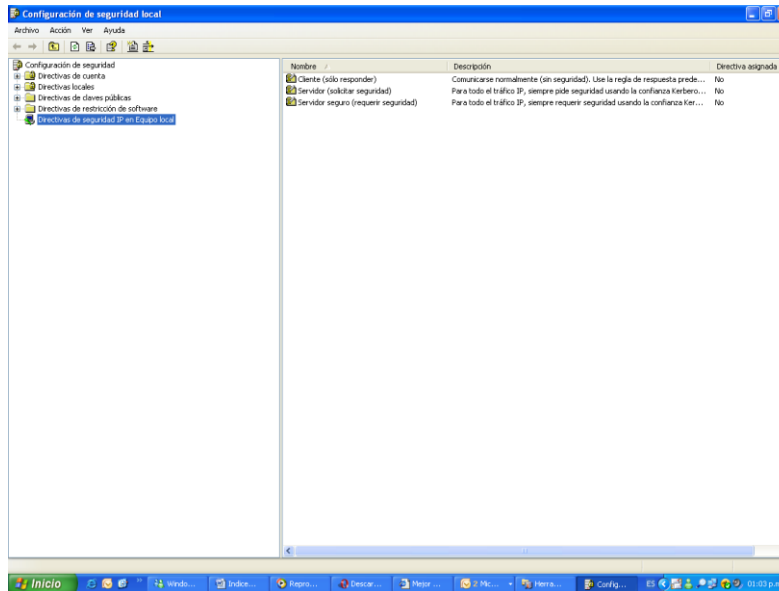


Figura 1.6. Políticas de Windows.

Fuente: Microsoft Windows Vista Consola de Administración (MMC).

De acuerdo con la compañía Cisco Networks (Cisco Networks, 2008), existen tres niveles de riesgo, donde se deben establecer las políticas restrictivas más severas:

- **Sistemas de bajo riesgo** o datos que, en caso de peligro (ver datos por personal no autorizado, los datos dañados o la pérdida de datos) no perturban el negocio, ni ramificaciones de causa jurídica o financiera. El sistema dirigido o datos pueden ser fácilmente restaurados y no permitir más el acceso de otros sistemas.
- **Sistemas de riesgo medio** o datos que, en caso de peligro (ver datos por personal no autorizado, los datos dañados, o la pérdida de datos) podrían causar una perturbación moderada en la empresa, sus ramificaciones menores, jurídicas o financieras, y facilitar más el acceso a otros sistemas. El sistema dirigido o datos requiere un esfuerzo moderado, para restaurar, o mejorar el proceso de restauración que podría ser perjudicial para el sistema.
- **Sistemas de alto riesgo** o datos que, en caso de peligro (ver datos por personal no autorizado, los datos dañados, o la pérdida de datos) podrían causar una perturbación

extrema en el negocio. Podrían ser la causa principal de daño en las ramificaciones financieras legales, o poner en peligro la salud y la seguridad de una persona. El sistema dirigido o datos, requiere un esfuerzo significativo para restaurar el proceso de restauración, o mejorarlo, sino sería perjudicial para la empresa u otros sistemas.

Así pues, se debe considerar el impacto de la información estratégica, más el tiempo y dinero que implica la caída o robo del sistema en cuestión.

Encriptación y cifrado.

Básicamente, la criptografía es esconder algo para que pase desapercibido. Por ejemplo, un texto sencillo lo convierte a un texto cifrado, por medio de un proceso especial. El texto cifrado se puede restablecer a su forma original mediante un proceso llamado descifrado. El uso de la clave facilita este proceso, ya que los procesos de descifrado sólo pueden ocurrir con el uso de la clave. Todos los algoritmos de cifrado dependen de las funciones criptográficas. Las preocupaciones más comunes de este método son: si el algoritmo criptográfico se puede violar, si los datos están protegidos y si la persona que envió algo es realmente quien dice ser.

Códigos de autenticación de mensajes.

Los códigos de autenticación de mensajes (MAC) son similares a los resúmenes, ya que también se utilizan en esquemas de cifrado con una llave secreta. Se aplican a un mensaje específico. Al igual que en los sistemas de clave pública, sólo los puede verificar la persona que los recibe. Los MAC se clasifican en diferentes categorías. Pueden estar basados en transformación del código, en cifras o incondicionalmente en la seguridad. Además, se pueden utilizar para revisar la manipulación de datos. El emisor y el receptor comparten una llave secreta, que está incrustada en el mensaje. El receptor puede verificar el mensaje, para asegurarse de que no fue manipulado durante la transmisión. Los MAC también pueden usar una llave, con una función basada en la transformación de código. Esto produce un resumen adjunto al final del mensaje que se denomina encabezado MAC, basado en llaves.

Generador de números aleatorios.

Algo que dificulta mantener los algoritmos criptográficos en secreto y los datos a salvo, es la generación de números aleatorios utilizados como claves. Se ha trabajado bastante con los números aleatorios, pero siguen siendo inseguros. Los mejores números aleatorios se presentan en la naturaleza. El ruido eléctrico y la estática son las formas más eficientes para generarlos, pero por diferentes circunstancias no se usan. Se han construido dispositivos generadores, sin embargo, son predecibles y no verdaderamente aleatorios.

Además de lo anterior, existen generadores de números pseudo aleatorios, que utilizan algoritmos criptográficos diseñados para simular un ambiente del mundo real, generalmente a través de funciones matemáticas.

Cifrado de clave pública y privada.

Se basa en la generación de números aleatorios o pseudo aleatorios. En el sistema de cifrado de clave privada (simétrico), se emplea la misma clave para cifrar y descifrar. Se debe tener cuidado de que esa clave llegue al receptor en forma segura. En un sistema de clave privada la integridad es muy importante. Por lo tanto, es necesario cambiar periódicamente esa clave.

El concepto denominado “secreto perfecto”, donde las claves son renovadas frecuentemente, ayuda a limitar el daño, debido a que sólo proporcionan una pequeña oportunidad para los ataques. En el cifrado de clave pública, se utiliza una clave privada que el ente mantiene en secreto y una clave pública que está disponible. La clave privada sirve para descifrar los mensajes que fueron cifrados con la clave pública asociada.

La seguridad de una clave viene determinada por:

- **Longitud.** Cuanto mayor sea el número de bits de información en la clave, mayor es el número de combinaciones que debe probar un atacante. Por ejemplo, una clave compuesta de dos cifras necesita de 100 intentos como máximo para ser descubierta. Mientras que una clave de cinco dígitos requiere 100,000 intentos como máximo.
- **Aleatoriedad.** Si una clave es elegida, basándose en palabras que existen en una lengua natural, es susceptible de ser rota mediante un ataque de diccionario. Por ello, una clave segura debe ser generada en forma aleatoria, usando letras y números, así como símbolos ortográficos si es posible. Desde un punto de vista matemático, una clave es más segura cuanto más entropía contenga. Algunos sistemas informáticos contienen herramientas para "obtener entropía" de procesos impredecibles, como los movimientos de la cabeza lectora del disco duro. Sin embargo, la verdadera aleatoriedad sólo puede conseguirse mediante procesos físicos, como el ruido producido por el viento captado por un micrófono o simplemente un dado.
- **Periodo de uso.** Una clave se vuelve más insegura cuanto mayor sea el tiempo que ha estado en uso. Por eso es importante renovarlas periódicamente, no obstante haber sido generadas con la mayor aleatoriedad posible.

Claves secretas compartidas.

Esta clave tiene muchos inconvenientes, ya que previamente se deben haber puesto de acuerdo, un emisor y un receptor, para que se lleve a cabo dicha transferencia. Para fortalecerla se han creado algunos mecanismos que la hacen más segura.

La permuta de claves se debe realizar antes de intercambiar la información que se quiere proteger (clave IKE, *Internet Key Exchange*). Es necesario acordar un nivel de negociación entre los equipos involucrados, para proteger la información durante el intercambio. A esta asociación se le denomina Asociación de Seguridad (SA).

Una asociación de seguridad es la combinación de una clave negociada, un protocolo de seguridad y el índice de parámetros de seguridad (SPI), que se definen entre todos para proteger la comunicación desde los dos puntos de conexión. A continuación se describe ampliamente dicho proceso.

Primera Fase.

Para garantizar una comunicación segura y exitosa, IKE trabaja en dos fases. La confidencialidad y la autenticación se aseguran durante cada una de las fases, mediante el uso de algoritmos de cifrado y algoritmos de autenticación, acordados entre los dos equipos durante las negociaciones de seguridad. Al dividirse las tareas en dos fases se agiliza la creación de claves.

En la primera fase o SA de modo principal, los equipos involucrados establecen un canal seguro y autenticado. IKE proporciona automáticamente la protección de identidad necesaria para que se realice el intercambio.

Fase I:

- a) Negociación de directivas.
- b) Intercambio Diffie-Helman (de valores públicos).
- c) Autenticación.

El intercambio realiza una oferta para establecer una asociación de seguridad con el receptor. El interlocutor no puede modificar la oferta. En caso de que se modifique la oferta, el interlocutor inicial rechazará el mensaje del interlocutor que responde. El interlocutor que responde envía una respuesta, para aceptar la oferta o bien una respuesta con alternativas.

Los mensajes enviados durante esta fase tienen un ciclo de reintento automático, que se repite cinco veces. No hay ningún límite preestablecido en cuanto al número de intercambios que se

puedan realizar. El número de asociaciones de seguridad solamente están limitadas por los recursos del sistema.

Fase II o SA de modo rápido:

- a) Se negocia la directiva.
- b) El material de clave de sesión se actualiza o se intercambia.
- c) La SA y las claves, junto con el SPI intercambian el controlador de IPsec (en el caso de IPsec).

La segunda negociación (configuración de seguridad y material de claves) está protegida por la SA de modo principal. Mientras que la primera fase protege la identidad, la segunda fase brinda protección mediante la actualización del material de claves, antes de enviar los datos.

Duración de la SA.

La SA de modo principal se almacena en caché, para permitir varias negociaciones en forma rápida. Cuando la clave principal o de sesión acumula cierto tiempo, se vuelve a negociar la asociación de seguridad. Además, la clave se actualiza o se vuelve a generar.

Cuando transcurre el periodo de espera predeterminado de la SA, de modo principal o cuando se alcanza la duración de la clave principal o de sesión, se envía un mensaje de eliminación al interlocutor que responde. Este mensaje determina que su duración caducó. De este modo se impide la creación de nuevas SA de modo rápido.

Firmas digitales.

Cuando alguien recibe un documento, es importante asegurarse de dos cosas: la firma digital que certifica al emisor original, más el sello que muestra la fecha y la hora en que se creó o se modificó el documento. Juntos, las firmas digitales y los sellos, pueden actuar como notaría pública en un documento electrónico. Los documentos electrónicos, almacenados en el disco duro de un servidor, necesitan otra forma de documentar la fecha y la hora. Al cambiar la fecha en la máquina, no se afecta la fecha del documento. Enseguida, se necesita un modo de asignar sellos al texto electrónico y no al medio en que está almacenado.

Una solución para el problema de los sellos, es una autoridad emisora de sellos confiable, similar a una autoridad emisora de certificados.

Integración en formato digital de los elementos de seguridad de la credencial para votar.

La integración de los elementos de seguridad de la credencial para votar del IFE, es un aspecto central de este trabajo de investigación, ya que generan confianza a todos los involucrados en el proceso electoral. Tal es el caso de:

- a) Firma digital.
- b) Folio.
- c) Clave de elector.
- d) Banda magnética.

Dichos elementos se pueden integrar para generar llaves compartidas, independientemente de los que se generan a la hora de crear el túnel de comunicación y del intercambio de claves de entidades.

Esto permitirá tener un nivel de encriptamiento alto, así como un entorno seguro al momento de crear el túnel. Otro nivel de seguridad es el que brinda el protocolo de comunicación, por lo que sería muy difícil vulnerar la seguridad de esta implementación.

1.7.10 Redes privadas virtuales (RPV).

Las redes privadas virtuales son implementaciones de una red virtual, soportada por una infraestructura física instalada, regularmente una LAN (*Local Area Network*), más equipo de comunicación, como; *switches*, *routers* y otros dispositivos de enlace. Los enlaces pueden ser variados, desde telefonía hasta fibra óptica, incluyendo redes inalámbricas y satelitales.

Su fortaleza radica en el soporte que brinda el cifrado de paquetes y la encriptación de datos, para que no sean atrapados por manos ajenas. Lo anterior porque la red puede usar tanto un medio público o privado de comunicación.

La RPV de una intranet se crea entre la oficina central y una oficina remota, o entre las oficinas centrales y las oficinas dependientes. Esta tecnología generalmente se usa al interior de una empresa. Aunque en ocasiones, dependiendo del tipo de servicio, se permiten accesos del exterior usando tecnología adicional, para asegurar los candados de quienes ingresan.

El acceso remoto en una RPV se crea entre las oficinas centrales y los usuarios móviles. Con un software de cifrado en la computadora móvil se establece el vínculo con la red correspondiente.

En el caso de la extranet, el vínculo se crea entre la empresa y sus clientes, o socios comerciales. Generalmente el acceso se permite vía protocolo web HTTP. Esto permite que a través de firmas digitales se hagan los enlaces pertinentes, ya que existe una entidad emisora que coordina el direccionamiento y el otorgamiento de permisos para accesos por segmentos de información. Los bancos, empresas de gobierno y empresas particulares, recurren bastante a esta tecnología por el control que les permite tener sobre la información.

Existen RPV internas para proteger la información de usuarios de la misma compañía, pues no se debe olvidar que una gran cantidad de ataques vienen precisamente de miembros de la organización, por lo que es necesario tener diferentes niveles de acceso a los sistemas.

Topología de una red privada virtual.

El modelo que se pretende desarrollar utilizará una topología firewall/RPV, que se conecta por medio de políticas de acceso del firewall. Se combina con un software cliente-servidor, para hacer un túnel donde la información quede protegida en un primer nivel, antes de pasar a la identificación del usuario, por medio de las firmas digitales y demás candados que se utilizarán, como se observa en la Figura 1.7.

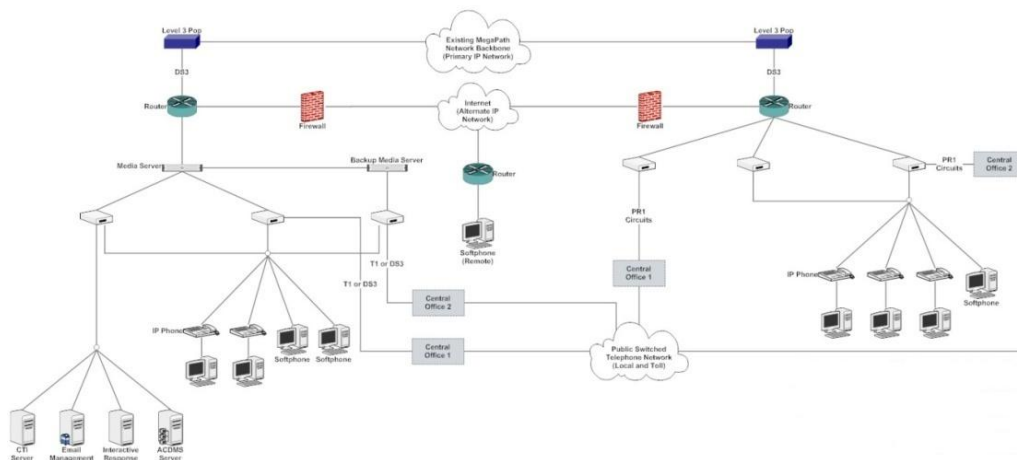


Figura 1.7. Ejemplo de una red privada virtual.

Fuente: Propia.

1.8 Metodología de investigación.

El alcance del proyecto será exploratorio. A pesar de ser un tema bastante conocido en la Unión Europea, algunos países de Asia, Norte América, América Latina y específicamente en

México, se carece de proyectos estratégicos formales que involucren aspectos como; Gobierno Electrónico, Democracia Electrónica, Voto Electrónico, Estrategia Electrónica, entre otros.

Nuestro proceso de investigación se realizará bajo un método mixto. El cual ha de recoger, analizar y vincular datos cuantitativos y cualitativos. Lo que generará posiblemente durante el desarrollo del mismo, posturas a favor y en contra.

Al utilizar este método para la investigación, se tendrá la ventaja de una amplitud, profundidad y diversidad en los datos recolectados. Dando un mayor sentido de entendimiento y riqueza interpretativa.

Se pretende realizar un análisis de las oportunidades estratégicas que existen en el Estado de Colima, para implementar votaciones electrónicas presenciales seguras. Luego, diseñar el modelo correspondiente.

El proyecto de investigación se realizará en tres etapas.

En la primer etapa, se aplicarán encuestas a una muestra representativa en cada uno de los diez municipios del Estado de Colima, para conocer si la sociedad en general está informada acerca de las votaciones electrónicas, si tiene a su alcance la infraestructura necesaria, si sabe cómo utilizarla, entre otros aspectos. Así mismo, se realizará un diagnóstico en los niveles de Gobierno Estatal y Municipal, usando la cadena de valor virtual para conocer la influencia del Gobierno Electrónico a través de los servicios que ofrecen en sus sitios Web y el alcance que tienen en las principales ciudades, hasta las zonas más alejadas.

En la segunda etapa, se hará revisión estadística de los datos, para iniciar los planteamientos de la estrategia a seguir para su posible implementación y seguimientos. Ya que así se tendrá una visión amplia de las opiniones emitidas por los encuestados.

Por último, conforme a los datos obtenidos en el diagnóstico, en la tercera etapa se diseñará el modelo estratégico para implementar votaciones electrónicas presenciales. Esto se muestra de manera gráfica en la Figura 1.8.

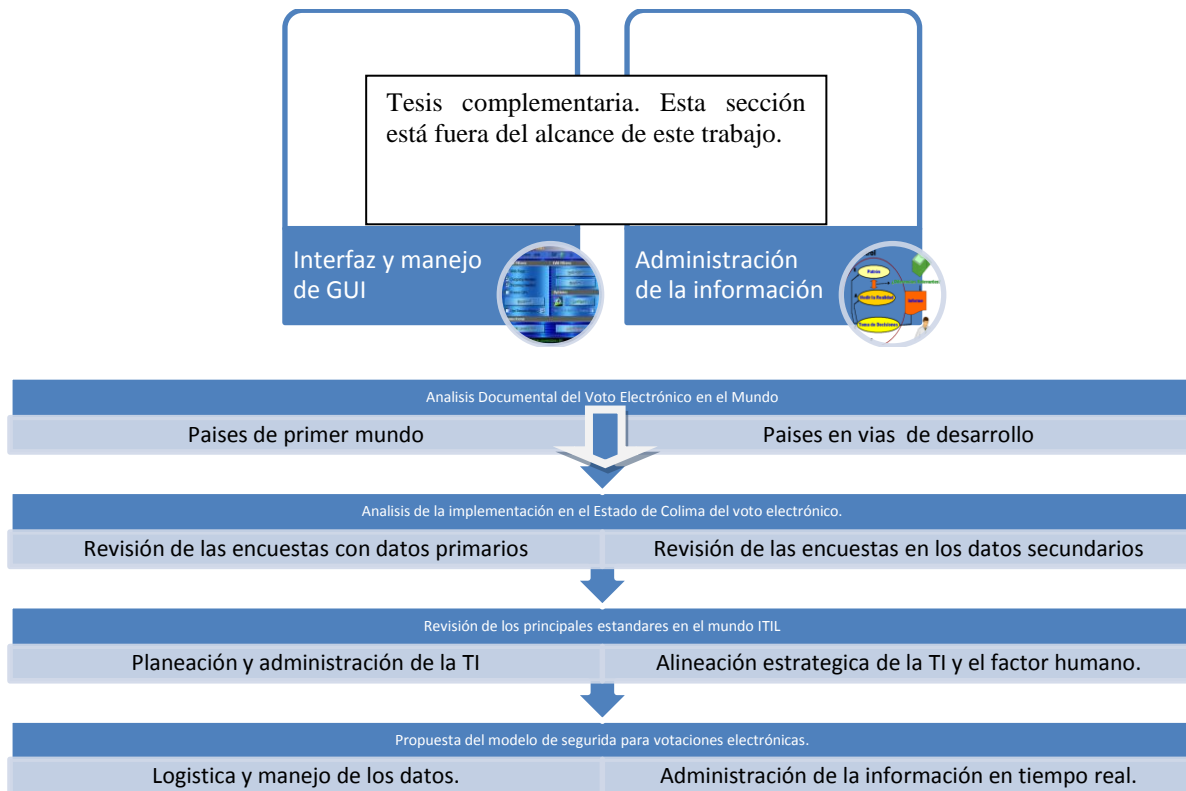


Figura 1.8. Metodología inicial propuesta.

Fuente propia.

1.9 Resultados (a priori) esperados.

- Diagnóstico de la situación actual, mediante las encuestas aplicadas y documentación de la cadena de valor virtual de los servicios electrónicos, ofrecidos por el Gobierno del Estado y los Gobiernos Municipales.
- Un modelo estratégico para implementar votaciones electrónicas presenciales seguras en el Estado de Colima.
- Recomendaciones para llevar a la práctica el modelo propuesto.

1.10 Contribuciones originales esperadas.

- a) Desarrollo de un modelo estratégico para implementar votaciones electrónicas presenciales, seguras, en el Estado de Colima.
- b) Generar un proceso estratégico de logística, acorde a las características particulares del modelo.
- c) Documentar, a través de la cadena de valor virtual y el diamante de Leavitt, un nuevo esquema para votaciones electrónicas presenciales seguras.

1.11 Impacto Social Esperado.

- a) Una nueva cultura bidireccional (sociedad-gobierno) para la adopción y uso de las TIC's.
- b) Involucramiento de la sociedad colimense en general y de personas con capacidades diferentes, en el diseño del modelo propuesto.

1.12 Estructura de la tesis.

Capítulo I.- Antecedentes.

En este capítulo se hace una descripción de los antecedentes del problema, los objetivos a cubrir, la investigación a futuro, su viabilidad y el desarrollo de un marco teórico previo, que nos ayude a tener una visión global del problema a resolver. Así mismo, el tipo de metodología a usar y las etapas que lo integran. Por otro lado, se describen los resultados que esperan ser mostrados en esta investigación y las contribuciones que se preveen obtener.

Capítulo II.- Marco Teórico.

En el marco teórico se ha de recabar toda la información documental que nos ayude a sustentar la investigación, en la intención de profundizar el tema y contribuir a darle significado a la investigación.

En este capítulo se recaba información acerca de las votaciones electrónicas a nivel mundial. En este contexto se pueden observar países de primer mundo en Europa, Asia y Norteamérica, sin dejar de incluir países en vías de desarrollo. Por lo que se obtiene información del nivel de competitividad, que tiene cada uno de los países que ya cuenta con uno o varios esquemas de voto electrónico. La información de la competitividad se toma de los datos que aparecen en el Reporte de Competitividad Global 2009-2010, que publica el Foro Económico Mundial. Del mismo modo se obtiene información del índice de desarrollo de las TIC's del año 2009. Lo anterior nos sirve como una manera de comparar nuestro país con aquellos que tienen este tipo implementaciones, para observar la similitud o diferencia que tenemos con ellos.

En el caso de algunos países, se tiene una descripción de cómo está contenida su democracia y los partidos políticos que integran el sistema político de cada país. Del mismo modo se da una descripción de la evolución del voto electrónico y las diferentes aristas que lo conforman.

En el cierre del capítulo se ha de observar una comparativa de cómo se encuentra, en México, el voto electrónico en algunas localidades donde ya se ha implementado.

Capítulo III.- Antecedentes del Instituto Federal Electoral, Alineación del Proceso de Planeación Estratégica y la Tecnología.

En este capítulo se ha de integrar información detallada del Instituto Federal Electoral, su estructura y el desarrollo del proceso electoral. Se inicia con la apertura de casillas, pasando por la emisión del voto y terminando en el cierre de casillas. Por otro lado, se hace un análisis detallado de los elementos que integran la credencial para votar con fotografía.

Así mismo se realiza la integración de la planeación estratégica, la administración de la seguridad de la información, más el ciclo de vida de desarrollo en los sistemas de seguridad, planeación y desarrollo. Posteriormente, describir los elementos que contiene un sistema de voto electrónico. Finalmente, describir los diferentes lenguajes y plataformas que desarrollan manejadores de bases de datos y esquemas de seguridad que pueden contener.

Capítulo IV.- Metodología de la Investigación.

Establecemos la metodología de la investigación para integrar las diferentes aristas del estudio, cuestionarios y selección de la muestra, a partir del Universo seleccionado. Se establecen los parámetros para la investigación de campo, a partir del cuestionario piloto que permitió reajustar y dirigir de mejor modo la investigación. Por último, la integración de los elementos para diseñar el modelo de seguridad.

Capítulo V.- Modelo de Seguridad para Elecciones Presenciales en el Estado de Colima.

En este apartado se estructura la propuesta de seguridad para el ***Modelo de Seguridad para Elecciones Presenciales en el Estado de Colima.***

Se realizará la descripción del modelo que se ha de implementar en el Instituto Electoral de Colima. Realizaremos una descripción pormenorizada de cada uno de los elementos que han de integrar la seguridad del voto, usando los estándares internacionales que han tenido éxito. Así mismo, las formas de evaluación del sistema, usando el Cuadro de Mando Integral (Balanced Score Card, BSC).

Capítulo II.- Marco de referencia.

El marco teórico permite reunir toda la información documental que se utilizará, para crear un boceto metodológico de la investigación. En esta fase hay que decidir el tipo de información que habrá de recogerse, los métodos que se utilizarán para recopilarla, cómo se analizará y en cuánto tiempo se realizará todo este proceso.

De esta manera, se alcanzará un conocimiento profundo del tema. Lo que contribuirá a darle significado al proceso indagatorio.

Además de que permiten demostrar la validez de la investigación, las teorías en que ésta se apoya, propician la generación de nuevos conocimientos.

Según Hernández Sampieri (2006, p. 64), las funciones principales del marco teórico son:

1. Ayuda a prevenir errores que se han cometido en otros estudios.
2. Orienta sobre cómo habrá de realizarse el estudio.
3. Amplía el horizonte del estudio o guía al investigador para que se centre en su problema, para evitar desviaciones del planteamiento original.
4. Documenta la necesidad de realizar el estudio.
5. Conduce al establecimiento de hipótesis o afirmaciones, que más tarde habrán de someterse a prueba en la realidad. O bien, nos ayuda a no establecerlas por razones fundamentadas.
6. Inspira nuevas líneas y áreas de investigación (Yurén Camarena, 2000).
7. Provee de un marco de referencia para interpretar los resultados del estudio.

2.1. Las votaciones electrónicas a nivel mundial.

En los últimos años, muchos países han venido realizando acciones para adoptar, a mediano y largo plazo, las Nuevas Tecnologías de la Información y Comunicación (NTIC's), como una

herramienta que les permita desempeñar sus funciones en forma eficaz. También para que contribuya al establecimiento de una comunicación estrecha entre los gobernantes y sus gobernados.

El Voto Electrónico forma parte de estas iniciativas que buscan aprovechar los adelantos tecnológicos, para ofrecer esquemas acordes a la modernidad. Que respondan a las demandas populares y que ayuden a construir una sociedad más democrática.

Para obtener un panorama amplio de los avances que se tienen hasta el momento, en el ámbito de las votaciones electrónicas a nivel mundial, se escogieron once países; Estonia, Japón, España, Dinamarca, Polonia, Estados Unidos de Norteamérica, Canadá, Argentina, Brasil, Venezuela y México. Naciones que sobresalieron por su nivel competitivo, la evolución en el desarrollo y uso de las TIC's. Igualmente; por la proporción de hogares con computadora, la evolución del voto electrónico, la participación ciudadana en los últimos procesos electorales y la disponibilidad de la información para su análisis.

A continuación se describen los datos más relevantes de cada nación.

2.2 Estonia.

También conocido como la República de Estonia, este país se localiza al noroeste de Europa y pertenece a la Unión Europea (UE) desde 2004. Su capital es Tallin y es una de las ciudades medievales mejor conservadas de Europa (UE, 2009).

Su sistema político está representado por un gobierno republicano, con un presidente que es elegido cada cinco años por un parlamento unicameral y donde el primer ministro es el responsable de gobernar. El Poder Legislativo está representado por una Asamblea de Estado, compuesta por 101 miembros que son elegidos mediante el sistema proporcional. El Poder

Judicial está organizado por tribunales de primera y segunda instancia (Enciclopedia de las naciones, 2009).

Estonia se caracteriza por ser uno de los primeros países, a nivel mundial, que han adoptado el voto electrónico en las elecciones presidenciales y parlamentarias. Tiene una población aproximada de 1.4 millones de habitantes (UE, 2009).

El nivel competitivo estonense, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010), que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.1:

Tabla 2.1. Nivel competitivo de Estonia.

| Indicador | Lugar* | Subíndices | Lugar | Pilares | Lugar | |
|---------------------------------|----------------------------|-------------------------|-------|----------------------------|--------------------------------------|----|
| Índice de competitividad global | 35 | Requerimientos básicos. | 34 | Instituciones | 31 | |
| | | | | Infraestructura | 34 | |
| | | | | Estabilidad macroeconómica | 47 | |
| | | | | Salud y educación primaria | 28 | |
| | Potenciador de eficacia. | 27 | | | Educación superior y capacitación | 21 |
| | | | | | Eficacia del mercado de bienes | 28 |
| | | | | | Eficacia del mercado de trabajo | 21 |
| | | | | | Sofisticación del mercado financiero | 29 |
| | | | | | Disponibilidad tecnológica | 16 |
| | Factores de la innovación. | 42 | | | Tamaño del mercado | 94 |
| | | | | | Sofisticación comercial | 48 |
| | | | | Innovación | 37 | |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)* que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores como se señala en la Tabla 2.2:

Tabla 2.2. Evolución en el uso de las TIC's: Estonia.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|-----------|-----------|-----------|---------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 690,000 | 760,000 | 660,000 | 680,000 | -0.36% |
| Suscriptores de banda ancha | 179,200 | 228,100 | 290,000 | 330,000 | 16.49% |
| Suscriptores de telefonía móvil | 1'445,300 | 1'658,700 | 1'610,000 | - | 3.66% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Estonia tiene los siguientes índices, que se detallan en las Tablas 2.3 y 2.4:

Tabla 2.3. Índice de desarrollo de las TIC's (IDI*) en Estonia (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 26 | 5.97 | 31 | 3.93 | 7.22% |

Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen

los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.4. Proporción de hogares con computadora en Estonia.

| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 57.0 | 21.8 | 17.37% |

Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

2.2.1 Partidos políticos.

Los partidos políticos más representativos de Estonia se muestran a continuación, en la Tabla 2.5:

Tabla 2.5. Principales partidos políticos en Estonia.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|---|-------------|--|---|--|
| <i>Estonian Reform Party</i> (ERP). | 1994 | Liberal centro-derecha, mercado libre. | Ideas liberales y pensamiento libertario. |  http://www.reform.ee/ |
| <i>Estonian Centre Party</i> (ECP). | 12/Oct/1991 | Centrista, liberal social, populista. | Formar una clase media fuerte en Estonia. |  http://www.keskerakond.ee/ |
| <i>Union of Pro Patria and Res Publica</i> (UPPRP). | 4/Jun/2006 | Conservatismo, conservatismo liberal. | Democracia cristiana. |  http://www.irl.ee/? |
| <i>Social Democratic Party</i> (SDP). | 8/Sep/1990 | Izquierda, Centro-Izquierda. | Democracia social. |  http://www.sotsdem.ee/ |
| <i>Estonian Greens</i> (EG) | 25/Nov/2006 | Centro. | Políticas verdes, ecología. |  http://roheline.erakond.ee/ |
| <i>People's Union of Estonia</i> (PUE). | 29/Sep/1994 | Centro, Centro-Izquierda. | Agraria, con influencia social demócrata. |  http://www.erl.ee/ |

Fuente: Elaboración propia, a partir de *Maps of the world*

(<http://www.mapsofworld.com/estonia/politics-and-government/political-parties.html>).

2.2.2 Evolución del voto electrónico.

El principio fundamental de todo ejercicio democrático, que se catalogue como maduro, transparente y legítimo, es la confianza de todos los que en él participan. En este país se ha utilizado el voto electrónico en dos ocasiones, obteniendo resultados muy alentadores, técnica y políticamente.

Técnicamente, todos los sistemas y procedimientos han funcionado adecuadamente y sin tener problemas de seguridad. Políticamente, los resultados de las elecciones han sido legítimos.

Estonia se ha distinguido a nivel mundial por ser un precursor del voto por Internet y por afrontar satisfactoriamente el desafío de utilizarlo (Maaten & Hall, 2008, pág. 31). En la Figura 2.1 se muestra cómo se soporta el modelo de voto electrónico en Estonia.



Figura 2.1 Soporte para la confianza electoral en Estonia.

Fuente: Madise, pág. 32.

El proyecto de votaciones electrónicas, utilizando una tarjeta de identificación, inició en 1997 a partir de una iniciativa de Ley, presentada en febrero de 1999 con el nombre de Ley de Documentos de Identificación Personal. La cual dio origen a la Ley de Firma Digital, en marzo de 2000. De esta manera, el gobierno aceptó el lanzamiento de la tarjeta de identificación en mayo de 2000, llevándose a cabo la primera emisión el 28 de enero 2002. Para junio de 2006, se emitieron más de 950,000 tarjetas (Madis, pág. 28).

Antes de la incorporación del voto por Internet, fue necesario crear un entorno adecuado que lo soportara. Se inició con la introducción de la Infraestructura de Clave Pública (*Public Key Infrastructure, PKI*), la firma digital y un proceso de autenticación.

Actualmente, este país goza de una adecuada infraestructura en comunicaciones y electores capacitados en el manejo de la tecnología, como resultado de la puesta en marcha del programa *Vaata maailma*. Cuenta con un uso generalizado del documento de identidad nacional, que sirve para autenticar en forma segura a los votantes en línea. Aplica en el uso generalizado del teléfono celular, para efectuar pagos en bancos, supermercados, taxis, hoteles, entre otros comercios. Así como una población relativamente pequeña de 1.3 millones de habitantes. Lo que ha contribuido para que Estonia sea un referente mundial en las votaciones electrónicas (Maaten & Hall, 2008).

Para evaluar la legitimidad del proceso electoral, se aplican principios internacionales, soportados por la Red de Conocimientos Electorales (*Electoral Knowledge Network, ACE*). Además, existen tres niveles diferentes de legitimidad:

- Legitimidad político / legal.
- Transparencia electoral.
- Transparencia del sistema.

En cada nivel, los participantes tienen a su disposición un sistema lo más transparente posible. La legitimidad se mide a través de las acciones que el gobierno realiza, más las acciones de los votantes o las acciones que realizan los administradores electorales, quienes están a cargo de las elecciones (Maaten & Hall, 2008).

2.2.3 Participación ciudadana.

En Estonia se realizaron las elecciones locales en octubre de 2005 y las parlamentarias en marzo de 2007, apoyándose en el uso de Internet, sin que esto representara problema alguno o que se hayan presentado incidentes relevantes entre los electores. El uso de la plataforma electrónica en 2007, fue tres veces mayor en comparación con la jornada realizada en 2005.

Los resultados finales se publicaron, por parte del gobierno, tal como se muestra en la Tabla 2.6:

Tabla 2.6. Estadísticas del voto por Internet en Estonia. Elecciones 2005 y 2007.

| | Elecciones locales 2005 | Elecciones parlamentarias 2007 |
|--|------------------------------------|---|
| Número de votos electrónicos | 9,681 | 31,064 |
| Votos electrónicos repetidos | 364 | 789 |
| Número de electores electrónicos | 9,317 | 30,275 |
| Votos electrónicos cancelados por boletas de papel. | 30 | 32 |
| Votos electrónicos contados | 9,287 | 30,243 |
| % de los votos electrónicos entre el total de votos otorgados. | 1.9% | 5.4% |
| % de votos electrónicos entre el total del voto anticipado | 7.2% | 17.6% |
| % de votos electrónicos emitidos en el extranjero. | n.a | 2% |

Fuente: Maaten & Hall, 2008, pág. 36.

De lo anterior se puede apreciar un crecimiento en el porcentaje de electores, que utilizaron el voto electrónico de 2005 a 2007. En su primer uso, el 1.9% de los votantes decidieron utilizar el método electrónico, mientras que dos años después hubo más participación con el 5.4%.

En una encuesta aplicada a los votantes, después de las elecciones parlamentarias de 2007, 1 de cada 10 electores afirmaron que no habrían votado si la opción de Internet no estuviera disponible (Maaten & Hall, 2008).

Los resultados obtenidos en las elecciones de 2005, sobre la aceptación de la gente para utilizar las TIC's, al momento de emitir su voto, se muestra a continuación, en la Tabla 2.7:

Tabla 2.7. Estadística general de las elecciones para gobierno local en Estonia (2005).

| | |
|---|-----------|
| Número de personas con derecho a voto | 1'059,292 |
| Número de votos | 502,479 |
| Válidos (incluyendo votos electrónicos) | 496,345 |
| Inválidos | 6,134 |
| Tasa de participación | 47% |
| Número total de votos electrónicos | 9,681 |
| Número de la repetición modificada de e-votos (más de 1 voto por votante) | 364 |
| Número de electores electrónicos | 9,317 |
| Número de votos electrónicos elegibles para el recuento | 9,287 |
| Número de votos electrónicos anulados | 30 |
| % de votos electrónicos entre todos los votos | 1.87% |
| % de los electores que votaron durante los días previos a la votación (incluyendo electores electrónicos). | 12% |
| % de los electores electrónicos, entre los votantes de todos los electores, que votaron durante el día de la elección. | 7% |
| Número de electores que utiliza la tarjeta de identificación electrónica por primera vez (para voto electrónico). | 5,774 |
| % de aquellos que utilizan tarjeta de identificación por primera vez, para vía electrónica entre todos los votantes electrónicos. | 61% |

Fuente: Madise & Martens, 2006, pág. 22.

El horario que tuvo mayor participación de la gente fue al inicio y al final de la jornada. En la mañana a las 9:00, y por la tarde, a las 19:00 horas (probablemente debido a que en esas horas la gente llegó a sus centros de trabajo o regresaron a sus casas después de laborar) como se observa en el grafico 2.1.

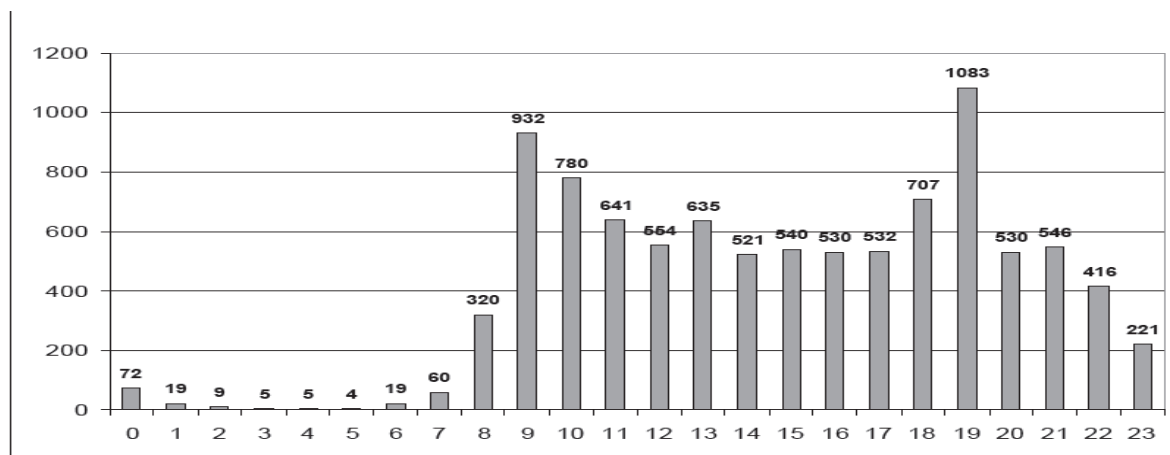


Gráfico 2.1. Frecuencia de la participación en las elecciones locales de Estonia, con voto electrónico (2005).

Fuente: Madise, pág. 41.

Tabla 2.8. Electores del sistema electrónico por edad y género (2005).

| Edades | Mujeres | % | Hombres | % |
|---------------|--------------|------------|--------------|------------|
| Arriba de 29 | 1,062 | 25.0 | 1,512 | 30.0 |
| 30 – 34 | 542 | 12.8 | 908 | 18.0 |
| 35 – 39 | 506 | 11.9 | 688 | 13.6 |
| 40 – 44 | 497 | 11.7 | 553 | 11.0 |
| 45 – 49 | 451 | 10.6 | 433 | 8.6 |
| 50 – 54 | 362 | 8.5 | 345 | 6.8 |
| 55 – 59 | 278 | 6.5 | 228 | 4.5 |
| Después de 60 | 547 | 12.9 | 375 | 7.4 |
| TOTAL | 4,245 | 100 | 5,042 | 100 |

Fuente: Madise y Martens(2006, pág. 22).

Tabla 2.9. Participación en áreas rurales y urbanas (2005).

| Tipo de poblado | Tipo de participación política | | | |
|---|--------------------------------|---------------------------|-------------------|-------------------|
| | No votó | Voto en urna convencional | Voto electrónico | Total |
| Urbana | 67.9% | 67.6% | 70.2% | 68.6% |
| Rural | 32.1% | 32.4% | 29.8% | 31.4% |
| Total (Número de personas que respondieron). | 100.0% (305) | 100% (318) | 100% (315) | 100% (938) |

Fuente: Madise y Martens, (2006, pág. 23)

2.3 Japón.

Esta nación se localiza al Este de Asia. Su capital es Tokio y su forma de gobierno es la Monarquía Parlamentaria Constitucional, representada por un emperador y un parlamento bicameral, conocido como La Dieta, integrado por una cámara de representantes y una cámara de consejeros (Embajada del Japón en México, 2000).

De acuerdo con su Censo de Población, en el 2005 Japón tenía 127.77 millones de habitantes. De los cuales, 62.35 millones eran hombres y 65.42 millones eran mujeres. Actualmente, dicha cantidad no presenta grandes variaciones, debido a los programas de control de natalidad que prevalecen en ese territorio y a la longevidad de su población adulta (*Ministry of Internal Affairs and Communications*, 2005).

El nivel competitivo japonés, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010) que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.10:

Tabla 2.10. Nivel competitivo de Japón.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | | |
|---------------------------------|-------|----------------------------|-------|----------------------------|-------|--------------------------------------|----|
| Índice de competitividad global | 8 | Requerimientos básicos. | 27 | Instituciones | 28 | | |
| | | | | Infraestructura | 13 | | |
| | | | | Estabilidad macroeconómica | 97 | | |
| | | | | Salud y educación primaria | 19 | | |
| | | Potenciador de eficacia. | 11 | | | Educación superior y capacitación | 23 |
| | | | | | | Eficacia del mercado de bienes | 17 |
| | | | | | | Eficacia del mercado de trabajo | 12 |
| | | | | | | Sofisticación del mercado financiero | 40 |
| | | | | | | Disponibilidad tecnológica | 25 |
| | | Factores de la innovación. | 2 | | | Tamaño del mercado | 3 |
| | | | | | | Sofisticación comercial | 1 |
| | | | | Innovación | 4 | | |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)* que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores:

Tabla 2.11. Evolución en el uso de las TIC's: Japón.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|-------------|-------------|-------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 85'290,000 | 87'540,000 | 88'110,000 | 88'500,000 | 0.93% |
| Suscriptores de banda ancha | 22'365,000 | 25'755,100 | 28'300,000 | 30'110,000 | 7.72% |
| Suscriptores de telefonía móvil | 94'745,000 | 101'698,000 | 100'520,000 | 105'830,000 | 2.8% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Japón tiene los siguientes índices:

Tabla 2.12. Índice de desarrollo de las TIC's (IDI*) en Japón (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 12 | 6.64 | 18 | 4.82 | 5.48% |

Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores

de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.13. Proporción de hogares con computadora en Japón.






| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 85.0 | 71.7 | 2.88% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

2.3.1 Partidos políticos.

Los partidos políticos con mayor número de simpatizantes son (*Web Japan*, 2009):

Tabla 2.14. Principales partidos políticos en Japón.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|---|---|-----------------------------|---|--|
| <i>Liberal Democratic Party</i> (LDP). | 15/Nov/1955 | Centro-derecha, conservador | Conservatismo, conservatismo liberal. |  http://www.jimin.jp/index.html |
| <i>The Democratic Party of Japan</i> (DPJ). | 8/Ene/1998 | Centro. | Liberalismo social. |  http://www.dpj.or.jp/ |
| <i>New Komeito</i> (NKP) | 1998 | Centro-derecha. | Influencia budista, conservatismo social. |  http://www.komei.or.jp/ |
| <i>Japanese Communist Party</i> (JCP). | 1922 | Izquierda. | Comunismo, elementos de Marxismo y Leninismo, eurocomunismo y socialismo democrático. |  http://www.jcp.or.jp/ |
| <i>Social Democratic Party</i> (SDP). | 1945 como Socialist Party of Japan y 1996 como SDP. | Izquierdista. | Democracia social. |  http://www5.sdp.or.jp/ |

Fuente: Elaboración propia a partir de *Web Japan*.

(<http://web-jpn.org/links/government/political/political.html>).

2.3.2 Evolución del voto electrónico.

Un rasgo característico del pueblo japonés es su madurez para impulsar vanguardistas reformas de estado, que se apoyan en el uso de las nuevas tecnologías de la información y comunicación. Así como la capacidad de adecuar, a las necesidades actuales, aquellas que ya fueron implementadas, con el propósito de extender su funcionalidad.

El 16 de octubre de 2001, el Ministerio de Administración Pública, Asuntos Locales, Correos y Telecomunicaciones de Japón (*MPHPT, Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan*) anunció la “*National Broadband Initiative*” (*NBI, Iniciativa Nacional de Banda ancha*)”, cuya finalidad era convertir a esa nación en la más avanzada, a nivel mundial, en cuanto a TI se refiere (MPHPT, 2001).

Para que el proyecto *NBI* fuera asimilado plenamente por los estados japoneses, en el año fiscal 2005, se hizo una calendarización que incluía; configurar Internet de alta velocidad/ultra alta velocidad, los roles correspondientes para los sectores público y privado, la prospectiva del número de suscriptores a Internet de alta velocidad/ultra alta velocidad y las expectativas sociales de los beneficios que recibirían con la implementación de Internet de banda ancha (MPHPT, 2001).

La agenda que desarrolló el Gobierno Central para promover el e-Gobierno a nivel nacional y local se muestra enseguida:

Tabla 2.15. Calendario para implementar e-Gobierno en Japón.

| Iniciativas comunes | Año Fiscal 2001 | Año Fiscal 2002 | Año Fiscal 2003 | Comentarios |
|--|--|---|---|--|
| [Archivado electrónico (aplicación, notificación y otros procedimientos)]. | 397 procedimientos (4% de todos los procedimientos). | 3,895 procedimientos (35%, para incrementarse a 50%). | 10,868 procedimientos (98%). | |
| 1. Sistema de portal para el archivado electrónico. - Aceptación del sistema de propósito general (que puede ser utilizado para aceptar varios procedimientos y notificación de los resultados de eso). | Establecimiento de especificaciones uniformes del gobierno (agosto). | Para establecerse por todos los ministerios, para el año fiscal 2002. | | |
| 2. PKI (Infraestructura de Clave Pública). • Administración. - Autoridades de | Inicio de la operación parcial (junio). | Para ser totalmente operativo en el año fiscal 2002. | Servicio disponible en casi todo el país. | 2 compañías acreditadas en septiembre de 2001. |

| | | | | |
|---|--|---|--|--|
| <p>Certificación Ministerial y Autoridad de Certificación Puente.</p> <ul style="list-style-type: none"> • Solicitantes. - Sistema de certificación electrónica basado en el registro comercial. - (Autoridades certificadoras del sector privado basadas en la Ley Concerniente a Firmas Electrónicas y Servicios de Certificación *). - Servicio Público de certificación individual por los gobiernos locales. | <p>Servicio iniciado (principalmente los asientos de las prefecturas). Servicio iniciado (agosto).</p> <p>Documento enviado.</p> | <p>Servicio de expansión regional (principales ciudades locales).</p> <p>Gradualmente expandido.</p> <p>Pruebas de demostración.</p> | <p>Inicio del servicio.</p> | |
| <p>3. Sistema de pago electrónico de cuotas.</p> | | <p>(Desarrollo de la infraestructura por instituciones del sector financiero privado. Expansión gradual de las instituciones financieras*).</p> | <p>Inicio de la operación del sistema de pago electrónico para el fisco (enero de 2004).</p> | |
| <p>4. Redes para asistir las transacciones electrónicas.</p> <ul style="list-style-type: none"> - Conexión de las redes del gobierno central al local. (Central: Kasumigaseki WAN, local: LGWAN). - Sistema de red para los registros básicos de los residentes. | <p>Pruebas de demostración.</p> | <p>Inicio de la conexión (prefecturas, especialmente las ciudades designadas, etc.).</p> <p>Inicio de la operación (agosto).</p> | <p>Inicio de la conexión (todos los municipios).</p> | |
| <p>5. Revisión de las leyes y ordenanzas.</p> | <p>Documento enviado.</p> | | | |
| <p>6. Los sistemas de archivo electrónico para procedimientos individuales.</p> | <p>Para establecerse en todos los ministerios en el año fiscal 2003, en tándem con conversión en línea.</p> | | | |
| <p>[Digitalización de procedimientos para las adquisiciones del gobierno].</p> | | | | |
| <ul style="list-style-type: none"> - Apertura electrónica de la licitación y ofertas para las | <p>Inicio de la operación de la</p> | <p>Operación de prueba</p> | <p>Inicio de la operación</p> | |

| | | | | |
|--|--|--|----------------------------------|---|
| obras no públicas. | base de datos integrada de adquisiciones del gobierno (junio). | (MPHPT) (octubre). | (todos los ministerios). | |
| - Apertura electrónica de la licitación y ofertas para las obras públicas. | Introducido (proyectos de gran escala) (octubre). | Expansión de proyectos de aplicación (proyectos de tipo oferta pública en más de 200 millones de yenes, etc.). | Para ser totalmente introducido. | Ministerio de Tierra, Infraestructura y Transporte. |
| <p>(Notas)</p> <ul style="list-style-type: none"> - Las acciones marcadas con un (*) serán implementadas por el sector privado. - En relación con la garantía de la seguridad de información, para el e-Gobierno en conjunto, un “Plan de acción para garantizar la seguridad de la información para el e-Gobierno” fue adoptado en octubre de 2001 (Secretaría del Gabinete y todos los ministerios). - Los sistemas de adquisición del gobierno, relacionados con los sistemas de información, serán revisados durante el año fiscal 2002 (Ministerio de Administración Pública, Asuntos de Interior, Postes y Telecomunicaciones, Ministerio de Economía, Comercio e Industria, Ministerio de Finanzas, otros ministerios relacionados). - El sistema legislativo para la protección de datos personales, mantenido por órganos administrativos, debe ser realizado y consolidado en línea con el Programa para la Protección de la Información Personal (la Ley Orgánica. El programa incluye provisiones, de manera que las medidas se deben ejecutar con un alcance de un año después de la promulgación). | | | | |

Fuente: MPHPT “National Broadband Initiative”, 2001.

http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol12/Vol12_16.html#2

Para complementar la agenda anterior, el gobierno nipón desarrolló un plan estratégico para implementar las TIC's en las diferentes actividades y servicios que ofrecen a la sociedad. El cual se muestra en la Figura 2.2.

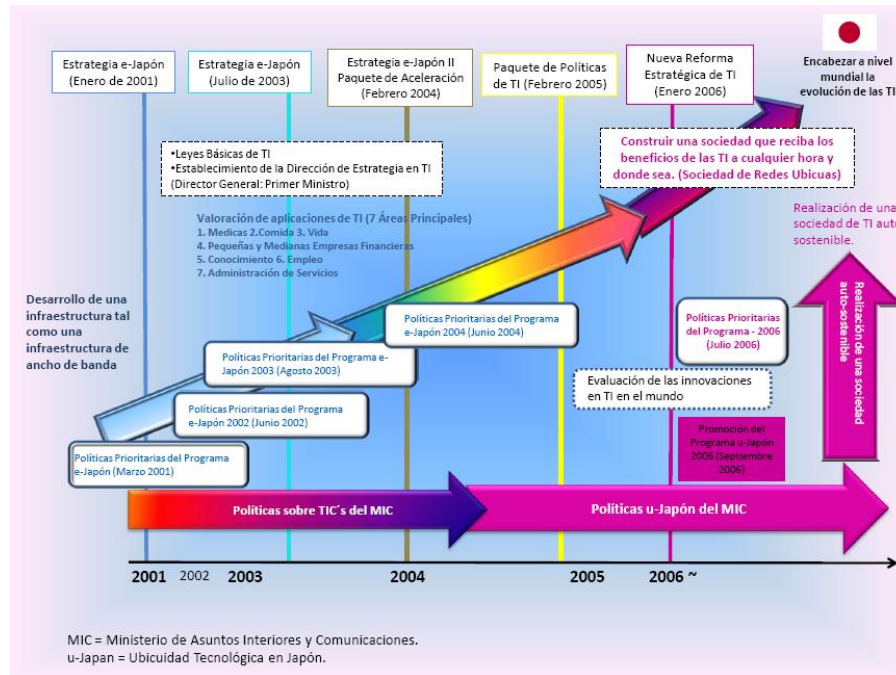


Figura 2.2. Acciones realizadas en Japón para desarrollar su estrategia de TI.

Fuente: *Ministry of Internal Affairs and Communications (MIC)* (Ministerio de Asuntos Internos y Comunicaciones), 2009.

http://www.soumu.go.jp/menu_seisaku/ict/u-japan_en/new_outline01.html

Con la incorporación de las TIC's en el sistema electoral japonés, se modificó el esquema tradicional que estuvo vigente por más de 100 años. Se realizaba de manera escrita, seleccionando el nombre del candidato o el partido político de la preferencia del elector.

Japón hizo su primera implementación de e-vote para la elección de alcalde, en junio de 2002, en la ciudad de Niimi, que es un territorio pequeño con aproximadamente 25,000 personas. Este ejercicio fue posible gracias a la modificación de la Ley Electoral, realizada en febrero de 2001, la cual se hizo oficial el 7 de diciembre y entró en vigor el 1 de febrero de 2002 (Murata, 2009).

Esta ley establece el voto electrónico en las elecciones locales, como un caso especial de la Oficina Pública de la Ley Electoral para elegir a los diputados, miembros de las asambleas y los directores ejecutivos de los gobiernos locales (elecciones locales).

La mencionada ley prevé el voto electrónico, usando un dispositivo electromagnético de grabación. Dicho dispositivo es operado por el votante, quien selecciona un número determinado de candidatos para un cargo público. La máquina registra la elección del elector, para después liberar el dispositivo y poder reutilizarlo cuando otro votante registrado lo necesite. Este procedimiento es sólo para casillas presenciales y no considera votantes ausentes, método braille o voto por correo electrónico.

Este sistema operó de la siguiente manera:

1. Emisión de una tarjeta de votación.

- A su llegada, cada votante se identifica en la lista de electores y se le proporciona una tarjeta electromagnética de votación.

2. Elección.

- El sistema de votación otorga permisos para operar, como las inserciones de los votantes de la tarjeta de votación.
- El elector opera los dispositivos para seleccionar un candidato. Los datos de la votación se registran en el soporte de grabación. Luego, la tarjeta de votación sale automáticamente.

3. Devolución de la tarjeta de votación.

- Después de votar, la tarjeta de votación se regresa a un empleado autorizado, la cual puede ser reutilizada. La tarjeta de voto está garantizada por la tarjeta de identidad (IC), evitando así la duplicación.

En la Tabla 2.16 se hace una cronología de las acciones realizadas en Japón, para desarrollar el primer dispositivo de votación electrónica:

Tabla 2.16. Proceso para el desarrollo del primer dispositivo de votación electrónica, en Japón.

| Fecha | Evento |
|-------------------|--|
| Abril 1989 | Establecimiento de la conferencia (privada) sobre el estudio de E-voting. |
| Marzo 1992 | Propuesta de adopción del dispositivo E-voting para el Ministerio de Asuntos del Interior. |
| Septiembre 1992 | Primera demostración pública del dispositivo sensible al tacto para E-voting. |
| Abril 1999 | Primera participación de la gente con deficiencia visual en una votación falsa. |
| Septiembre 2000 | Los miembros de La Dieta autorizaron las resoluciones para actualizar la votación libre de obstáculos. |
| Diciembre 2000 | Prueba empírica para el inicio del desarrollo de votaciones libres de obstáculos. |
| 30/Noviembre/2001 | Se aprobó la Ley Especial de Votación Electrónica. |
| 1/Febrero/2002 | La Ley Especial de Votación Electrónica entró en efecto. |
| 23/Junio/2002 | Primera votación electrónica en Japón (Ciudad de Niimi). |

Fuente: Takuji, Masatsugu y Ayato, 2002.

2.4 España.

Es una nación soberana que pertenece a la UE y cuyo sistema político está representado por una monarquía parlamentaria.

De acuerdo con el Instituto Nacional de Estadística (INE), este país tiene, hasta el 1 de octubre de 2009, una población total de 45'967,632 habitantes. De los cuales 22'685,242 son varones y 23'282,390 son mujeres (INE, 2009).

El nivel competitivo español, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010) que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.17:

Tabla 2.17. Nivel competitivo de España.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | | |
|---------------------------------|-------|----------------------------|-------|----------------------------|-------|--------------------------------------|----|
| Índice de competitividad global | 33 | Requerimientos básicos. | 38 | Instituciones | 49 | | |
| | | | | Infraestructura | 22 | | |
| | | | | Estabilidad macroeconómica | 62 | | |
| | | | | Salud y educación primaria | 38 | | |
| | | Potenciador de eficacia. | 29 | | | Educación superior y capacitación | 33 |
| | | | | | | Eficacia del mercado de bienes | 46 |
| | | | | | | Eficacia del mercado de trabajo | 97 |
| | | | | | | Sofisticación del mercado financiero | 50 |
| | | | | | | Disponibilidad tecnológica | 29 |
| | | Factores de la innovación. | 35 | | | Tamaño del mercado | 13 |
| | | | | | | Sofisticación comercial | 28 |
| | | | | | | Innovación | 40 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)* que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, que se observan en la Tabla 2.18

Tabla 2.18. Evolución en el uso de las TIC's: España.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|------------|------------|------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 15'119,000 | 18'578,000 | 17'900,000 | 19'810,000 | 6.99% |
| Suscriptores de banda ancha | 4'994,274 | 6'654,900 | 8'030,000 | 9'060,000 | 16.06% |
| Suscriptores de telefonía móvil | 41'327,911 | 46'152,000 | 48'400,000 | 52'370,000 | 6.1% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, España tiene los siguientes índices:

Tabla 2.19. Índice de desarrollo de las TIC's (IDI) en España (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|----------|------|----------|------|---------------------|
| Posición | IDI | Posición | IDI | IDI |
| 27 | 5.91 | 28 | 4.10 | 6.28% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores

de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.20. Proporción de hogares con computadora en España.

| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 60.4 | 36.1 | 8.96% |

Fuente: Elaboración propia, a partir de ITU. *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

2.4.1 Partidos políticos.

En el territorio español, los partidos políticos están clasificados en cuatro bloques:

- **Partidos estatales con representación en las Cortes Generales.** Las Cortes Generales están formadas por el Congreso de los Diputados y el Senado.
- **Partidos autónomos con representación en las Cortes Generales.** Algunos de estos partidos son de tipo nacionalista periférico o regionalista, los cuales tienen representación en las Cortes Generales de la IX Legislatura.
- **Partidos autónomos sin representación en las Cortes Generales.** Son aquellos que no tienen representación en las Cortes, pero sí en el ámbito autonómico o local.
- **Otros partidos.** Se caracterizan por no tener representación pública. Aglutinan a un pequeño número de simpatizantes.

Los partidos políticos más representativos en las elecciones generales del 9 de marzo de 2008 se muestran en la Tabla 2.21:

Tabla 2.21. Resultados de las elecciones generales del 9 de marzo de 2008.

| Partido | Escaños | Votos | % votos |
|--|---------|------------|---------|
| PSOE (Partido Socialista Obrero Español) | 169 | 11'064,524 | 43.64 |
| PP (Partido Popular) | 153 | 10'169,973 | 40.11 |
| CiU (Convergencia i Unió) | 11 | 774,371 | 3.05 |
| EAJ-PNV (Euzko Alderdi Jeltzalea-Partido Nacionalista Vasco) | 6 | 303,246 | 1.20 |
| ERC (Esquerra Republicana de Catalunya) | 3 | 296,473 | 1.17 |
| IU (Izquierda Unida) | 2 | 963,040 | 3.80 |
| BNG (Bloque Nacionalista Galego) | 2 | 209,042 | 0.82 |
| CC-PNC (Coalición Canaria-Partido Nacionalista Canario) | 2 | 164,255 | 0.65 |
| UPyD (Unión Progreso y Democracia) | 1 | 303,535 | 1.20 |
| Na-Bai (Nafarroa Bai) | 1 | 62,073 | 0.24 |

Fuente: <http://www.elpais.com/especial/elecciones-generales/>

Tabla 2.22. Principales partidos políticos en España.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|---|-------------|-------------------|--|--|
| Partido Socialista Obrero Español (PSOE). | 2/May/1879 | Centro-izquierda. | Socialdemócrata, progresismo. |  http://www.psoe.es/ |
| Partido Popular (PP) | 20/Ene/1989 | Centro-derecha. | Españolismo, liberalismo, conservadurismo, democracia cristiana. |  http://www.pp.es/ |
| Convergencia i Unió (CiU). | 1978 | Centrista. | Nacionalista, catalán, liberal, democracia cristiana. |  http://www.ciu.cat/ |
| Euzko Alderdi Jeltzalea-Partido Nacionalista Vasco (EAJ-PNV). | 1895 | Centro-derecha. | Nacionalismo vasco, democracia cristiana, federalismo europeo. |  http://www.eaj-pnv.eu/eusk/ |

| | | | | |
|---|-------------|----------------------|--|--|
| Esquerra Republicana de Catalunya(ERC). | 1931 | Izquierda | Republicanismo, nacionalismo catalán, independentism o catalán, socialismo, catalanismo. |  http://www.esquerra.cat/ |
| Izquierda Unida(IU) | 1986 | Izquierda | Socialismo del siglo XXI, republicanismo, federalismo, ecologismo y comunismo. |  http://www.izquierda-unida.es/ |
| Bloque Nacionalista Galego (BNG). | 1982 | Izquierda | Nacionalismo gallego, europeísmo. |  http://www.bng-galiza.org/ |
| Partido Nacionalista Canario (PNC). | 1924 | Izquierda | Nacionalista, interclasista, democrático, progresista y social. |  http://www.pnc-canarias.eu/ |
| Coalición Canaria (CC) | 1993 | Centro. | Nacionalismo canario. |  http://www.coalicioncanaria.org |
| Unión Progreso y Democracia (UPyD). | 26/Sep/2007 | Izquierda o derecha. | Progresismo, transversalismo, laicismo, oposición al nacionalismo. |  http://www.upyd.es/ |
| Nafarroa Bai (Na-Bai) | 2003 | Izquierda | Vasquista, socialismo, progresismo, nacionalismo vasco. |  http://www.nafarroabai.org/ |

Fuente: Elaboración propia, a partir de la información incluida en los sitios Web de los partidos políticos.

Los partidos políticos más importantes de España son: el PSOE y el PP. El PSOE ha permanecido en el poder la mayor parte del régimen constitucional, que inició en 1978 con

una monarquía parlamentaria. A partir de las elecciones generales, que se realizaron el 14 de marzo de 2004, este partido encabeza el gobierno español.

2.4.2 Evolución del voto electrónico.

El territorio español está organizado jurídicamente en comunidades autónomas, que se dividen en provincias y estas, a su vez, en municipios. Eso ha provocado conflictos en la transición del voto tradicional al voto electrónico, porque cada comunidad es autónoma en sus gestiones, administración y legislación.

LOREG

Las adecuaciones hechas a la Ley Orgánica del Régimen Electoral General (LOREG) y a las leyes de las comunidades autónomas, han contribuido a la automatización de los procesos democráticos españoles. Sin embargo, a pesar de las actualizaciones que se han realizado, no se ha podido homologar completamente la manera en que se llevan a cabo las jornadas electorales en ese país.

Fernández Rodríguez et al. (2007) mencionan que:

Cuando se estudian herramientas, como el voto electrónico, nos parece que cualquier perspectiva de análisis debe contemplar como marco general, en primer lugar, el estado de la legislación electoral en la que potencialmente aquella operaría (LOREG). Es precisamente así, como se podrá confirmar o desmentir que el modo de voto, que tal legislación contempla para esa determinada sociedad, padece deficiencias, aspectos mejorables o incluso vicios de forma o de fondo que subsanar. En segundo lugar, evidentemente condicionado por las conclusiones que hubiésemos obtenido, resultaría imprescindible conocer muy bien dicha herramienta.

A partir de la década de los noventa, se hicieron importantes reformas a la LOREG. Algunas de las peticiones hechas en aquel entonces, para ser tomadas en cuenta, fueron (Fernández Rodríguez et al., 2007):

- Apertura de las listas electorales.
- Adopción de un sistema electoral de carácter mixto (combinando fórmulas mayoritarias y proporcionales).
- Aumento de la proporcionalidad de la relación votos/escaños.
- Tamaño de la circunscripción.
- El problema de los partidos nacionalistas y su representación parlamentaria.
- La financiación de los partidos políticos.
- La presencia de los medios de comunicación en el desarrollo de los procesos electorales.
- El censo electoral y el desarrollo de sus competencias.
- El voto por correo.
- Las barreras electorales.

Ley 15/1998

Uno de los primeros avances para adoptar el voto electrónico, en España, fue la actualización de la Ley 15/1998 para elegir al parlamento vasco. En la exposición de motivos II (Ministerio del Interior de España, 1998) se menciona que:

En los albores del siglo XXI, la investigación y el estudio comparado de los procedimientos más avanzados de votación, regulados en el derecho electoral europeo, conducen al reto de la implantación del voto electrónico en el actual sistema autónomo.

La regulación en la presente Ley del voto electrónico, constituye una innovación en el proceso electoral deudora del progreso tecnológico, estando la papeleta electoral en soporte magnético. Las nuevas tecnologías permiten la articulación de formas de participación de los ciudadanos, en la red pública, que deben ser incorporadas. Su

utilización es el resultado de un análisis sustentado en el avance tecnológico. Las nuevas tecnologías deben de encontrar aplicación en la acción pública, no solamente como tecnologías de control, sino, además como tecnologías que favorezcan la libertad.

Ley 2004

Un segundo paso fue el proyecto de Ley 2004. Un nuevo intento que establecía la normatividad para implementar el voto electrónico en el ordenamiento jurídico de la Comunidad Vasca. Sin embargo, dicho proyecto no se culminó. Se realizaron las elecciones y cambió de legislatura, sin tomar en cuenta la propuesta.

El Grupo parlamentario popular argumentaba que no había una demanda clara de la población, para solicitar el cambio de procedimiento electoral o alguna mejora del proceso en lo particular. Para ellos, el sistema clásico de sobres y papeletas era considerado; seguro, eficaz y participativo.

La realidad es que no había confianza de la población, ni legisladores. Inclusive de los mismos autores del proyecto, motivo por el cual no prosperó. Esto se aprecia claramente en la Disposición Final Segunda del texto (Fernández Rodríguez et al., 2007):

1. Lo dispuesto en el artículo primero de esta Ley, respecto del Voto Electrónico, será aplicado gradualmente en las elecciones al Parlamento Vasco que se celebren con posterioridad al año 2001, atendiendo principalmente a la disponibilidad del equipamiento, a las adaptaciones instrumentales necesarias y a otras cuestiones técnicas y operativas. En la segunda y posteriores aplicaciones del Voto Electrónico, también se podrá tener en cuenta el nivel de aceptación social de dicho sistema electrónico de votación. A tal fin, el Gobierno, previa comunicación al Parlamento Vasco, determinará mediante decreto, el grado de implantación progresiva del Voto Electrónico, fijando las circunscripciones electorales o municipios en los que se aplicará dicho sistema.

Elecciones a Cortes Generales

El 14 de marzo de 2004, el Ministerio del Interior (MIR) recibió la aprobación de la Junta Electoral Central, para efectuar pruebas de votación electrónica a través de Internet de tipo experimental. En dicha prueba, se eligieron los municipios de las provincias de Lugo y Zamora. Los habitantes utilizaron la tarjeta electrónica con certificado digital, emitida por la Subsecretaría del Ministerio del Interior para votar. La empresa encargada de realizar el simulacro fue Indra Sistemas S.A., quien utilizó el software denominado Internet vote (Sistema de Votación por Internet).

Entre las principales características del sistema (Indra, 2004), el voto estaba cifrado. Se firmaba y enviaba a una urna electrónica virtual que separaba la identidad del votante y la opción que elegía. Al término de la jornada electoral, la autoridad encargada de hacer el recuento, procedió a la apertura de la urna virtual y al recuento, después de que el escrutinio provisional fue anunciado por el gobierno.

De acuerdo con la información proporcionada por la empresa Indra, el sistema es seguro, fiable secreto y rápido (MIR, 2004).

Referéndum 2005

En febrero de 2005, el Ministerio del Interior, a través de la Dirección General de Política Interior, puso en marcha una prueba de voto electrónico, que coincidió con el referéndum del 20 de febrero de ese mismo año (MIR, 2005).

Fue la prueba más importante de este tipo que se realizó en España. El objetivo era modernizar el proceso electoral, mantener a ese país a la vanguardia de la sociedad de la información y las nuevas tecnologías.

El ejercicio se realizó entre el 1 y el 18 de febrero, concluyendo antes del 20 de febrero, día en que la votación sobre la Constitución Europea sí tuvo efecto jurídico. Participaron 52 ayuntamientos (uno por cada provincia) que fueron seleccionados en base a su

representatividad. Se utilizó un censo de dos millones de ciudadanos: aproximadamente el 6% del total del censo nacional.

Se utilizaron certificados digitales emitidos específicamente para ese evento, con el propósito de conferirle al sistema las máximas garantías de; seguridad, autenticidad, confidencialidad, integridad y no repudio (MIR, 2005).

Los ciudadanos tuvieron que presentarse en los lugares donde se ubicaban los módulos de cómputo autorizados, para registrarse y obtener el certificado digital correspondiente. La participación fue voluntaria y no se condicionó la intervención para tener derecho a votar en el proceso, que sí tuvo validez jurídica.

Sólo participaron electores residentes en España, porque era necesaria la presencia física del elector para el registro y emisión del certificado digital.

Los resultados de la prueba se difundieron después de hacerse públicos los resultados provisionales del referéndum del 20 de febrero. Para que esa información no influyera en el libre ejercicio de los ciudadanos de participar en una jornada electoral.

2.4.3 Participación Ciudadana.

Del 28 al 30 de junio de 2004 se realizó la consulta electrónica “Madrid Participa”, sobre democracia electrónica y participación ciudadana. Representó el ejercicio más relevante, hasta el momento, en cuanto al uso de las TIC’s en España.

Esta consulta popular fue impulsada por el Ayuntamiento de Madrid. Tuvo sus orígenes en septiembre de 2003, donde empresas importantes como Scytl, Accenture, Oracle, Telefónica, HP e Intel, unieron esfuerzos para realizar una experiencia piloto sobre votación electrónica. La cual sirvió para determinar la factibilidad técnica y social de las herramientas utilizadas.

Igualmente, para valorar la participación de la gente y detectar áreas de oportunidad que se puedan mejorar en futuros eventos.

La herramienta se aplicó en el Distrito Centro del municipio de Madrid, con una población de 136,227 personas, utilizando diferentes canales de participación; Internet, telefonía Java, mensajes SMS y centros presenciales (Barrat y Reniu, 2004).

El Distrito Centro está integrado por seis barrios; Palacio, Embajadores, Cortes, Justicia, Universidad y Sol. Se eligió ese lugar por su estructura urbana complicada (es una zona de ocupación antigua) y las características de su población, conformada por adultos mayores y un número significativo de inmigrantes.

Desde el punto de vista sociológico, destacan los siguientes aspectos del estudio (Barrat y Reniu, 2004):

- Los datos mostraron una baja participación de jóvenes, entre 16 y 24 años, así como de la tercera edad. Sin embargo, la participación de los ciudadanos, entre los 25 y 69 años, la valoraron de manera positiva, como lo muestran la Figura 2.3 y la Tabla 2.23.



Figura 2.3. Distribución de los encuestados por sexo (en %).

Fuente: Barrat y Reniu, 2004.

Tabla 2.23. Distribución de los encuestados por grupos de edad.

| Grupos de edad | % |
|----------------|------|
| 16 a 24 años | 4,3 |
| 25 a 34 años | 23,9 |
| 35 a 44 años | 27,1 |
| 45 a 54 años | 17,4 |
| 55 a 64 años | 12,4 |
| Más de 65 años | 14,9 |

Fuente: Barrat y Reniu, 2004.

- La mayoría de los participantes fueron ciudadanos españoles. Sin embargo, también participó un número importante de ciudadanos comunitarios y latinoamericanos. Lo que puede servir para facilitar la integración de las diferentes comunidades residentes en el Distrito Centro, como se observa en la Figura 2.4.

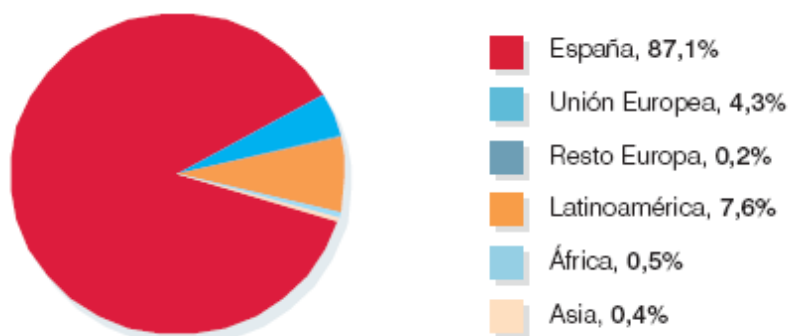


Figura 2.4. Distribución de los encuestados, según su nacionalidad.

Fuente: Barrat y Reniu, 2004.

- Se reafirmó la vinculación entre el nivel de renta, más el acceso a las Nuevas Tecnologías de la Información y las Comunicaciones (NTIC), como lo enmarca las Tablas 2.24 y 2.25.

Tabla 2.24. Nivel de ingresos mensuales y posesión de computadora en el domicilio (en %).

| | Con PC | Sin PC |
|-----------------------|--------|--------|
| Menos de 800 € | 52,6 | 47,4 |
| Entre 800 y 1.200 € | 57,1 | 42,9 |
| Entre 1.200 y 1.600 € | 78,9 | 21,1 |
| Más de 1.600 € | 92,5 | 7,5 |

Fuente: Barrat y Reniu, 2004.

Tabla 2.25. Acceso a Internet según nivel de ingresos mensuales (en %).

| | Conexión a Internet en el domicilio | Tipo de conexión | | |
|-----------------------|-------------------------------------|------------------|------|-----------|
| | | Módem | ADSL | Otro tipo |
| Menos de 800 € | 21,0 | 58,9 | 41,1 | – |
| Entre 800 y 1.200 € | 18,4 | 50,0 | 40,0 | 10,0 |
| Entre 1.200 y 1.600 € | 24,0 | 41,5 | 53,9 | 4,6 |
| Más de 1.600 € | 36,5 | 49,0 | 49,0 | 2,0 |

Fuente: Barrat y Reniu, 2004.

- El perfil socio-tecnológico de los encuestados, respondió a la posesión de teléfono móvil y computadora en el domicilio, de más de dos años de edad, con conexión a Internet a través de módem. El acceso a la red se produce diariamente desde el domicilio y el lugar de trabajo, con una finalidad laboral y de envío de correos electrónicos, como se ve en la Figura 2.25.

Tabla 2.26. Perfil tecnológico de los encuestados (en %).

| ¿Tiene... | | | | | |
|--------------------------------|------------------|-----------------------------|-------------|-----------------------------|-------------|
| ...Teléfono móvil? | | ...Ordenador en casa? | | | |
| Sí | No | Sí | No | | |
| 82,9 | 17,1 | 68,7 | 31,3 | | |
| ¿Qué edad tiene su ordenador? | | ¿Tiene conexión a Internet? | | | |
| Menos de 1 año | Entre 1 y 2 años | Más de 2 años | Sí | | |
| 18,0 | 27,4 | 54,6 | No | | |
| | | 82,1 | | | |
| ¿Qué tipo de conexión utiliza? | | | | | |
| Módem | ADSL | Cable | Otro tipo | | |
| 50,2 | 46,5 | 1,7 | 1,6 | | |
| ¿Dónde se conecta? | | ¿Con qué frecuencia? | | Uso principal del ordenador | |
| Domicilio | 52,3 | Cada día | 74,4 | Trabajo | 57,3 |
| Trabajo | 38,8 | Semanalmente | 18,1 | Ocio/juegos | 9,0 |
| Universidad | 0,5 | Mensualmente | 2,3 | Correo-e | 31,6 |
| Cibercafé | 2,9 | Casi nunca | 5,2 | Compra-e | 1,0 |
| Centro Cívico | 3,4 | | | Chats | 1,0 |
| Otro lugar | 2,1 | | | | |

Fuente: Barrat y Reniu, 2004.

- El canal de información proporcionado por el Ayuntamiento, con mayor impacto, fueron los trípticos informativos enviados al domicilio de los ciudadanos, como se muestra en la Figura 2.5. Por otro lado, las Asociaciones de Vecinos operaron también como excelentes canales de información.

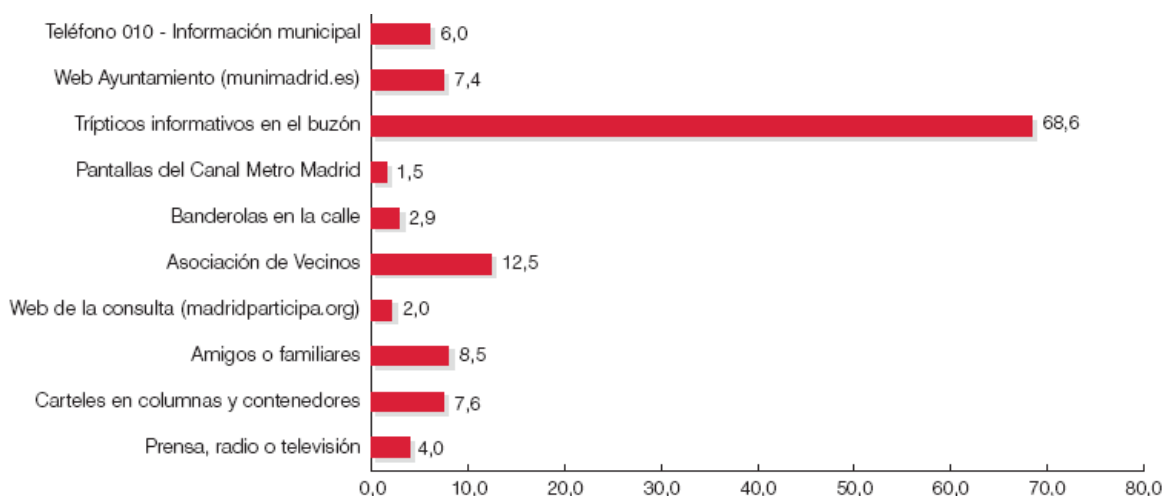


Figura 2.5. Canales de información sobre la Consulta Ciudadana “Madrid Participa” (en %).

Fuente: Barrat y Reniu, 2004.

- Los encuestados valoraron muy positivamente la necesidad de ese tipo de consultas, aunque fueron críticos con las preguntas realizadas y las opciones de respuesta disponibles, como lo señala la Figura 2.6.

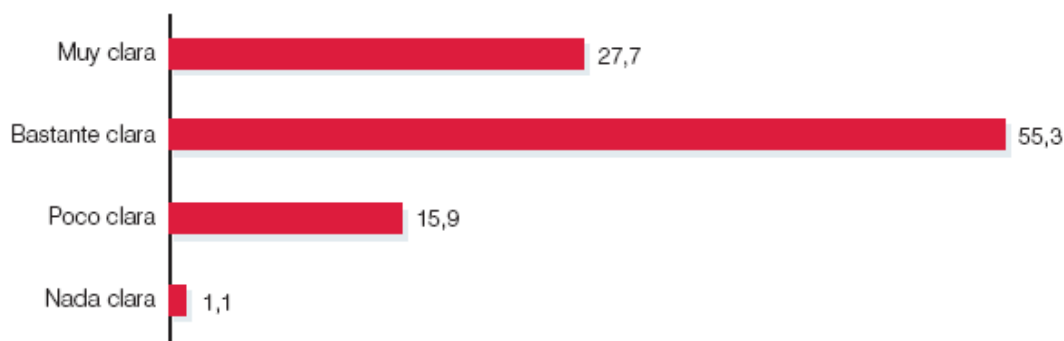


Figura 2.6. Evaluación de la información recibida (en %).

Fuente: Barrat y Reniu, 2004.

- La posible coexistencia, en el futuro, de sistemas tradicionales y electrónicos de votación, resultó ser la opción que recabó más apoyo por parte de los encuestados, como se observa en las Figuras 2.7 y 2.8.

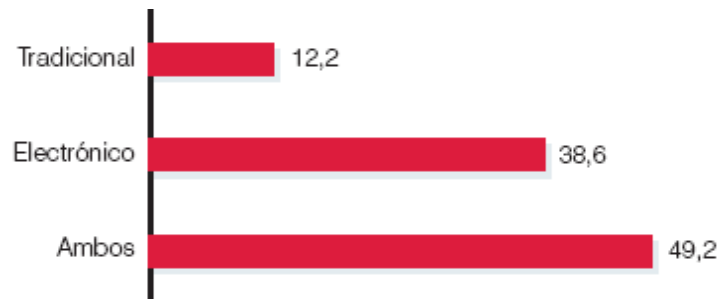


Figura 2.7. Sistema de votación preferido por los encuestados (en %).

Fuente: Barrat y Reniu, 2004.

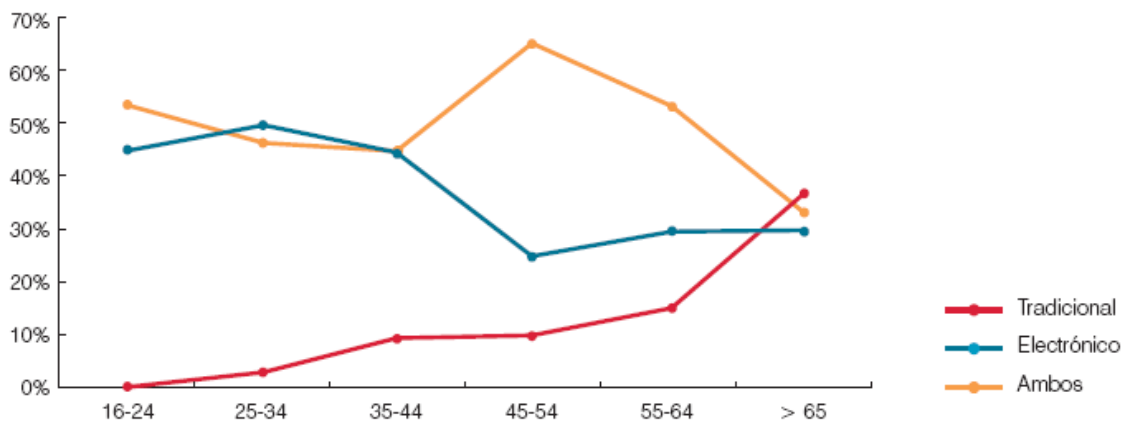


Figura 2.8. Sistema de votación preferido por los encuestados, según grupos de edad.

Fuente: Barrat y Reniu, 2004.

- La tecnología que se utilizó en la Consulta Ciudadana fue recibida en forma satisfactoria por los ciudadanos. Especialmente en lo referente a; rapidez, sencillez y seguridad en el proceso electoral, como se ve en la Figura 2.9.

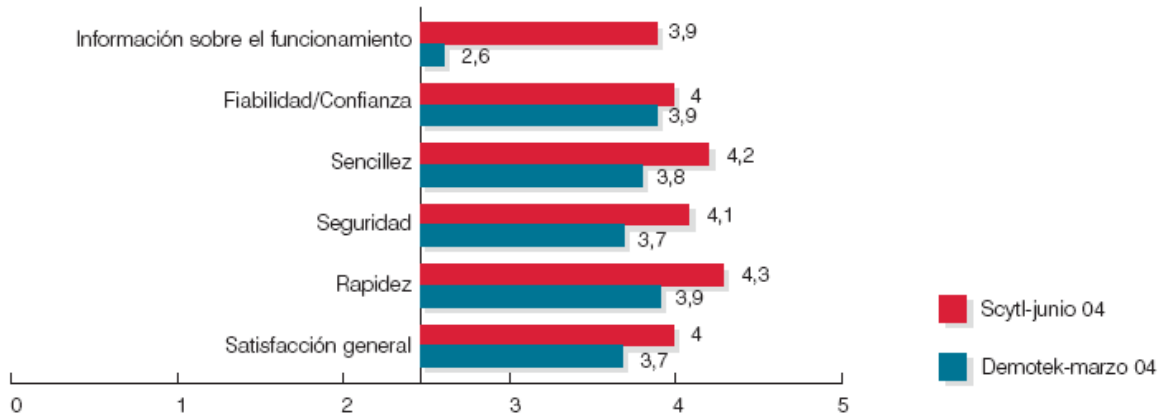


Figura 2.9. Valoración comparativa de tecnologías de voto electrónico.

Fuente: Barrat y Reniu, 2004.

- El nivel de renta y edad fueron los elementos principales que determinaron, un mayor o menor apoyo, a la generalización de los sistemas electrónicos para votar. Los encuestados mayores de 45 años prefieren el sistema tradicional. Lo mismo que los encuestados con ingresos inferiores a 1,200 € por mes, como lo señalan las Figuras 2.10 y 2.11.

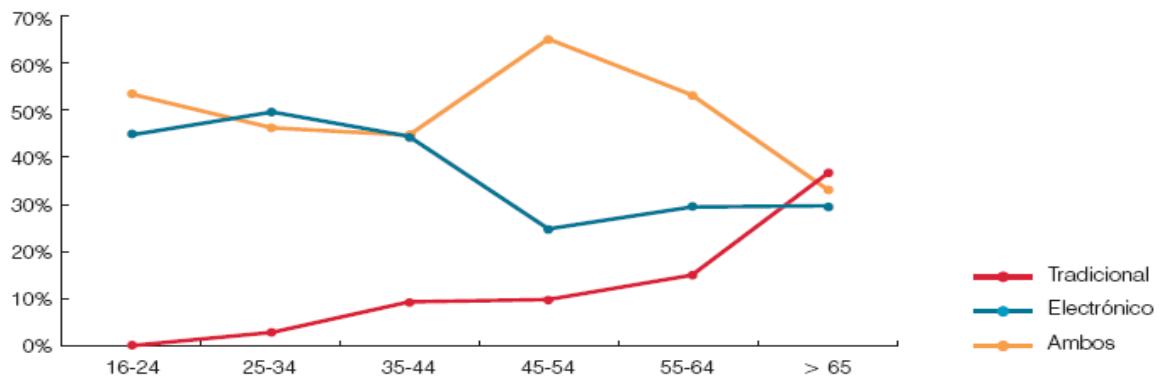


Figura 2.10. Sistema de votación preferido por los encuestados, según grupos de edad.

Fuente: Barrat y Reniu, 2004.

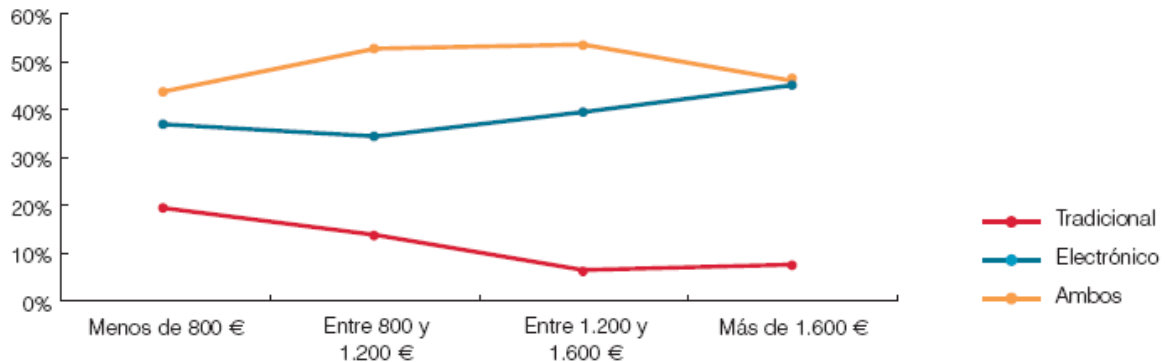


Figura 2.11. Sistema de votación preferido por los encuestados, según nivel de renta.

Fuente: Barrat y Reniu, 2004.

- La participación en procesos electorales no representó algún incentivo para una mayor predisposición, para aceptar las NTIC, ni para confirmar el supuesto efecto movilizador, como lo muestran las Figuras 2.12 y 2.13.

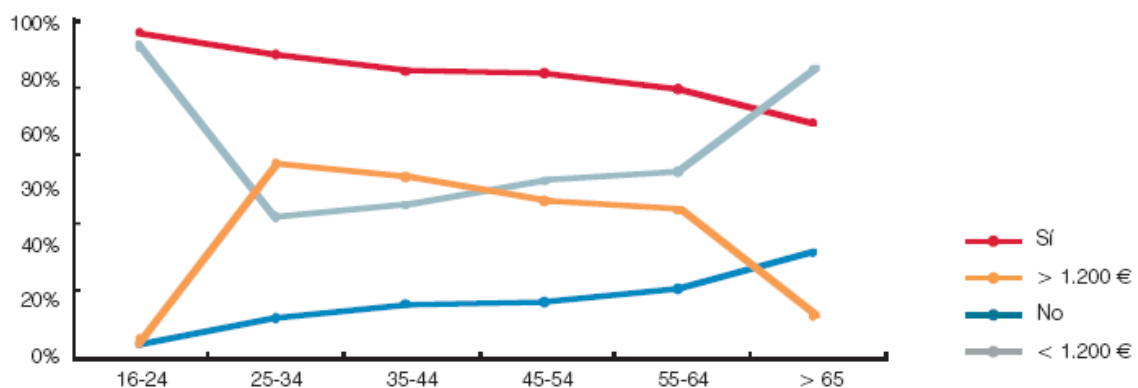


Figura 2.12. Predisposición al uso de las NTIC y nivel de ingresos, según grupos de edad.

Fuente: Barrat y Reniu, 2004.

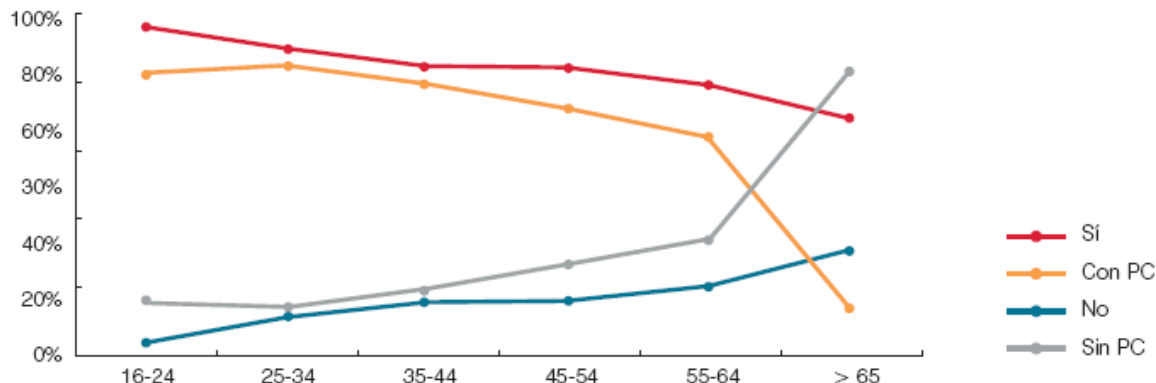


Figura 2.13. Predisposición al uso de las NTIC y nivel tecnológico, según grupos de edad.

Fuente: Barrat y Reniu, 2004.

- La mitad de los encuestados apostaron decididamente por el uso de sistemas electrónicos, para cualquier tipo de procesos electorales, ya sea en consultas ciudadanas parecidas a Madrid Participa o elecciones vinculantes. Sólo el 15% de los encuestados se oponen a su uso en comicios vinculantes. Lo anterior, como se observa en la Tabla 2.27 y en las Figuras 2.14, 2.15 y 2.16.

Tabla 2.27. Escenario futuro de utilización de un sistema electrónico de votación.

| ¿Utilizaría un sistema electrónico en... | | | |
|--|-----------------------------|---------------|-----|
| ...una Consulta Ciudadana? | ...una elección vinculante? | | |
| | Sí | Probablemente | No |
| Sí | 50,9 | 14,7 | 8,2 |
| Probablemente | 2,2 | 14,5 | 6,1 |
| No | 0,2 | – | 3,2 |

Fuente: Barrat y Reniu, 2004.

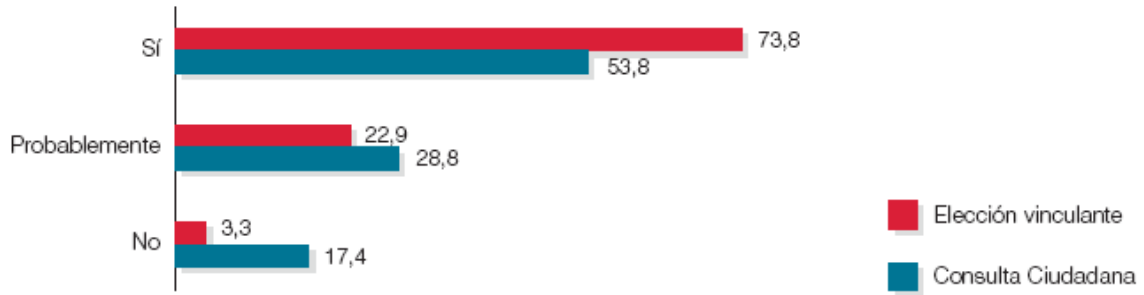


Figura 2.14. Predisposición a la utilización de un sistema electrónico de votación, según el tipo de proceso participativo (en %).

Fuente: Barrat y Reniu, 2004.

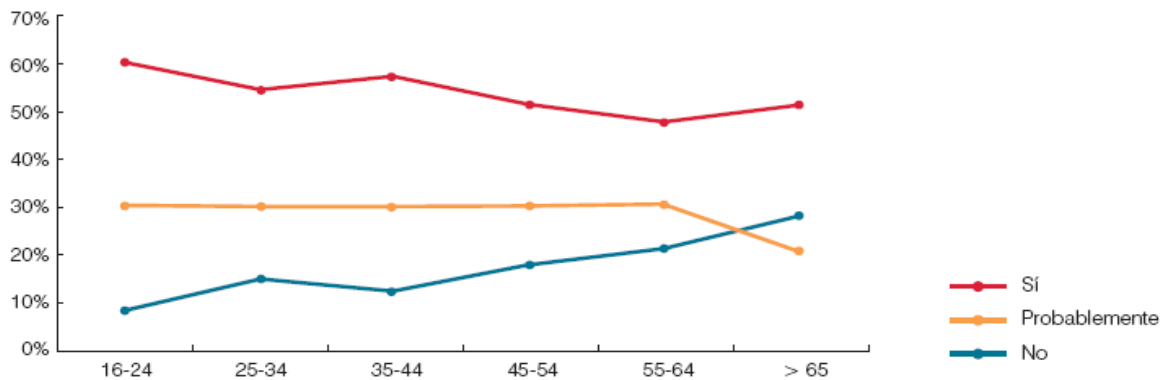


Figura 2.15. Predisposición a la utilización de un sistema electrónico de votación en elecciones vinculantes, según grupos de edad.

Fuente: Barrat y Reniu, 2004.

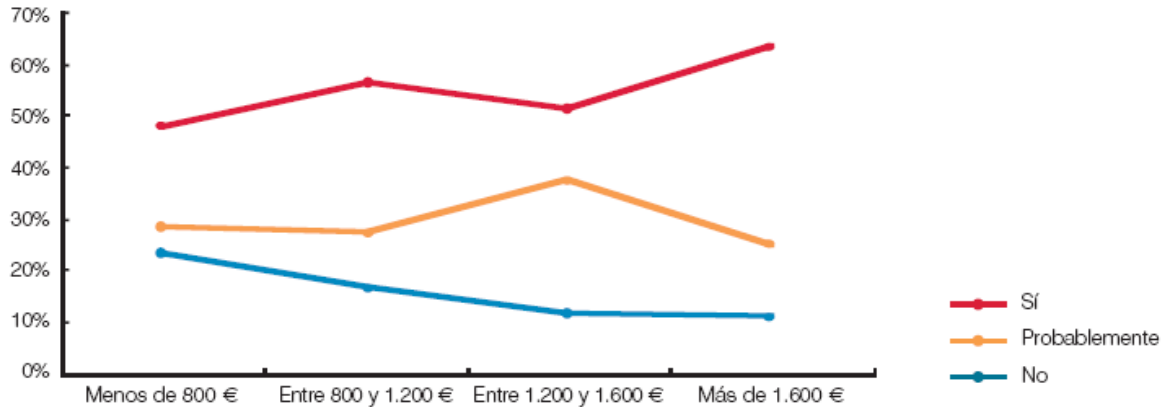


Figura 2.16. Predisposición a la utilización de un sistema electrónico de votación, en elecciones vinculantes, según nivel de ingresos.

Fuente: Barrat y Reniu, 2004.

2.5 Dinamarca.

Es un país con capital en Copenhague. Se ubica al norte de la Comunidad Europea y está conformado por tres regiones autónomas: Dinamarca, Groenlandia y las Islas Faroe.

La forma de gobierno que prevalece en ese territorio es la Monarquía Constitucional.

El nivel competitivo danés, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010), que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.28:

Tabla 2.28. Nivel competitivo de Dinamarca.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | | |
|---------------------------------|-------|----------------------------|-------|----------------------------|-------|--------------------------------------|----|
| Índice de competitividad global | 5 | Requerimientos básicos. | 4 | Instituciones | 3 | | |
| | | | | Infraestructura | 12 | | |
| | | | | Estabilidad macroeconómica | 14 | | |
| | | | | Salud y educación primaria | 6 | | |
| | | Potenciador de eficacia. | 6 | | | Educación superior y capacitación | 2 |
| | | | | | | Eficacia del mercado de bienes | 7 |
| | | | | | | Eficacia del mercado de trabajo | 5 |
| | | | | | | Sofisticación del mercado financiero | 8 |
| | | | | | | Disponibilidad tecnológica | 4 |
| | | | | | | Tamaño del mercado | 49 |
| | | Factores de la innovación. | 7 | | | Sofisticación comercial | 8 |
| | | | | | | Innovación | 10 |

Fuente: Elaboración propia a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)* que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, como se señala en la Tabla 2.28

Tabla 2.29. Evolución en el uso de las TIC's: Dinamarca.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|-----------|-----------|-----------|-----------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 2'887,000 | 3'205,200 | 3'240,000 | 3'380,000 | 4.02% |
| Suscriptores de banda ancha | 1'356,283 | 1'738,500 | 1'980,000 | 2'030,000 | 10.61% |
| Suscriptores de telefonía móvil | 5'511,878 | 5'890,900 | 6'240,000 | 6'590,000 | 4.57% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Dinamarca tiene los siguientes índices, como lo señalan las Tablas 2.30 y 2.31:

Tabla 2.30. Índice de desarrollo de las TIC's (IDI*) en Dinamarca (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 3 | 7.22 | 4 | 5.78 | 3.78% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100

habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.31. Proporción de hogares con computadora en Dinamarca.

| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 83.0 | 72.2 | 2.35% |

Fuente: Elaboración propia, a partir de ITU. *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009.*

2.5.1 Partidos políticos.

En la Tabla 2.32 se enmarcan los partidos políticos más representativos en Dinamarca.

Tabla 2.32. Principales partidos políticos en Dinamarca.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|--|-------------|-----------------|---|---|
| <i>Det Radikale Venstre</i> (DRV). | 1905 | Centro. | Socio liberalismo. |  http://www.radikale.dk/ |
| <i>Venstre Danmarks Liberale Parti</i> (VDLP). | 1870 | Centro-Derecha. | Liberalismo. |  http://www.venstre.dk/ |
| <i>Det Konservative Folkeparti</i> (DKF). | 1915 | Derecha. | Conservadurismo, liberalismo. |  http://www.konservative.dk/ |
| <i>Socialistisk Folkeparti</i> (SF). | 15/Feb/1959 | Izquierda. | Socialismo democrático, eco-socialismo. |  http://www.sf.dk/ |
| <i>Socialdemokrati et</i> (SDP). | 1871 | Izquierda. | Socialdemocracia. |  Socialdemokraterne http://www.socialdemokraterne.dk/ |

Fuente: Elaboración propia, a partir de *Political Resources on the Net.*

El partido político que mayor número de adeptos tiene, en el territorio danés, es el *Venstre Danmarks Liberale Parti*.

2.6 Polonia.

Polonia se ubica al centro de Europa. Su Capital es Varsovia.

El sistema político está representado por una Democracia Parlamentaria.

El nivel competitivo polaco, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010) que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.33:

Tabla 2.33. Nivel competitivo de Polonia.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | |
|---------------------------------|-------|----------------------------|-------|----------------------------|--------------------------------------|----|
| Índice de competitividad global | 46 | Requerimientos básicos. | 71 | Instituciones | 66 | |
| | | | | Infraestructura | 103 | |
| | | | | Estabilidad macroeconómica | 74 | |
| | | | | Salud y educación primaria | 35 | |
| | | Potenciador de eficacia. | 31 | | Educación superior y capacitación | 27 |
| | | | | | Eficacia del mercado de bienes | 53 |
| | | | | | Eficacia del mercado de trabajo | 50 |
| | | | | | Sofisticación del mercado financiero | 44 |
| | | | | | Disponibilidad tecnológica | 48 |
| | | Factores de la innovación. | 46 | | Tamaño del mercado | 20 |
| | | | | | Sofisticación comercial | 44 |
| | | | | | Innovación | 52 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)* que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, como lo señala la Tabla 2.34:

Tabla 2.34. Evolución en el uso de las TIC's: Polonia.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|------------|------------|------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 10'000,000 | 11'000,000 | 12'940,000 | 14'450,000 | 9.64% |
| Suscriptores de banda ancha | 1'243,949 | 2'640,000 | 3'200,000 | 5'010,000 | 41.66% |
| Suscriptores de telefonía móvil | 29'260,000 | 36'745,500 | 40'620,000 | 44'030,000 | 10.76% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Polonia tiene los siguientes índices, como se ve en las Tablas 2.35 y 2.36:

Tabla 2.35. Índice de desarrollo de las TIC's (IDI*) en Polonia (2002 y 2007).

| 2007 | | 2002 | | Tasa decrecimiento |
|------------|------|----------|------|--------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 39 | 4.95 | 37 | 3.34 | 6.78% |

Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.36. Proporción de hogares con computadora en Polonia.



| 2007 | 2002 | Tasa decrecimiento |
|------|------|-----------------------|
| 54.0 | 23.1 | 15.2% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

2.6.1 Partidos políticos.

En la Tabla 2.37 se enmarcan los partidos políticos más representativos en Polonia.

Tabla 2.37. Principales partidos políticos en Polonia.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|---|-------------|-------------------|---|--|
| <i>Platforma Obywatelska</i> (PO). | 1/Jul/2001 | Centro-derecha. | Demócrata cristiano, liberal conservador. |  http://www.platforma.org/ |
| <i>Prawo i Sprawiedliwość</i> (PiS). | 13/Jun/2001 | Centro-derecha. | Conservatismo nacional, democracia cristiana. |  http://www.pis.org.pl/ |
| <i>Sojusz Lewicy Demokratycznej</i> (SLD). | 15/Abr/1999 | Centro-izquierda. | Democracia social. |  http://www.sld.org.pl/ |
| <i>Polskie Stronnictwo Ludowe</i> (PSL) | 5/May/1990 | Centro. | Agrarianismo, centrismo y democracia cristiana. |  http://www.psl.pl/ |
| <i>Stronnictwo Demokratyczne</i> (SD). | 18/Sep/1937 | Centro. | Democracia social, liberalismo social, centrismo. |  http://www.sd.org.pl/ |
| <i>Socjaldemokracja Polska</i> (SP). | 26/Mar/2004 | Centro-izquierda. | Democracia social. |  http://www.sdpl.org.pl/ |
| <i>Unia Pracy</i> (UP) | 1992 | Izquierda | Democracia social. |  http://www.uniapraczy.org.pl/ |
| <i>Lewica i Demokraci</i> (LiD). | 3/Sep/2006 | Izquierda. | Democracia social, liberalismo social. |  http://www.lid.org.pl/ |
| <i>Partia Demokratyczna</i> (PD). | 2005 | Centro. | Liberalismo social. |  http://www.demokraci.pl/ |
| <i>Samoobrona Rzeczpospolitej Polskiej</i> (SRP). | 1992 | Izquierda. | Agrarianismo, nacionalismo izquierdista. |  http://www.samoobrona.org.pl/ |
| <i>Liga Polskich Rodzin</i> (LPR). | 2001 | Derecha radical. | Cristianismo, nacionalismo. |  http://www.lpr.pl/ |

Fuente: Elaboración propia, a partir de *Parties and Elections in Europe*.<http://www.parties-and-elections.de/poland.html>

2.7 Estados Unidos de Norteamérica.

Su nombre oficial es Estados Unidos de América. Está ubicado casi totalmente en América del Norte. Su capital es Washington.

La forma de gobierno está representada por una República Federal Presidencialista.

De acuerdo con el Sitio Web U.S. Census Bureau, la población norteamericana, al 11 de diciembre de 2009, es de 308'127,695 habitantes.

El nivel competitivo norteamericano, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010) que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.38:

Tabla 2.38. Nivel competitivo de Estados Unidos.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | | |
|---------------------------------|-------|----------------------------|-------|----------------------------|-------|--------------------------------------|----|
| Índice de competitividad global | 2 | Requerimientos básicos. | 28 | Instituciones | 34 | | |
| | | | | Infraestructura | 8 | | |
| | | | | Estabilidad macroeconómica | 93 | | |
| | | | | Salud y educación primaria | 36 | | |
| | | Potenciador de eficacia. | 1 | | | Educación superior y capacitación | 7 |
| | | | | | | Eficacia del mercado de bienes | 12 |
| | | | | | | Eficacia del mercado de trabajo | 3 |
| | | | | | | Sofisticación del mercado financiero | 20 |
| | | | | | | Disponibilidad tecnológica | 13 |
| | | | | | | Tamaño del mercado | 1 |
| | | Factores de la innovación. | 1 | | | Sofisticación comercial | 5 |
| | | | | | | Innovación | 1 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)* que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, como se observa en la Tabla 2.39:

Tabla 2.39. Evolución en el uso de las TIC's: Estados Unidos.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|-------------|-------------|-------------|-------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | - | 208'980,600 | 183'620,000 | 190'780,000 | -2.99% |
| Suscriptores de banda ancha | 49'391,060 | 58'254,900 | 66'210,000 | 79'070,000 | 12.48% |
| Suscriptores de telefonía móvil | 201'650,000 | 236'451,800 | 255'400,000 | 270'330,000 | 7.6% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Estados Unidos tiene los siguientes índices, como se aprecia en las Tablas 2.40 y 2.41:

Tabla 2.40. Índice de desarrollo de las TIC's (IDI*) en Estados Unidos (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 17 | 6.44 | 11 | 5.25 | 3.46% |

Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100

habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.41. Proporción de hogares con computadora en Estados Unidos.






| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 70.2 | 59.0 | 2.94 |

Fuente: Elaboración propia, a partir de ITU. *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

2.7.1 Partidos políticos.

En la Tabla 2.42 se enmarcan los partidos políticos más representativos en Estados Unidos.

Tabla 2.42. Principales partidos políticos en Estados Unidos.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|---------------------------------|-------------|-----------------------------------|---|--|
| <i>Democratic Party (DP).</i> | 1828 | Centro-izquierda, centro-derecha. | Liberalismo americano, liberalismo social, centrismo, progresismo, democracia social, conservadora. |  http://www.democrats.org/ |
| <i>Republican Party (RP).</i> | 1854 | Centro-derecha. | Conservatismo americano, conservatismo social, conservatismo fiscal, liberalismo económico, neoconservatismo. |  http://www.gop.com/ |
| <i>Libertarian Party (LP)</i> | 11/Dic/1971 | Derechista. | Libertaria, no intervencionismo. |  http://www.lp.org/ |
| <i>Constitution Party (CP).</i> | 1992 | Derecha cristiana. | Nacionalismo americano, conservatismo social, paleoconservatismo. |  http://constitutionparty.com/ |
| <i>Green Party (GP)</i> | 2001 | Centro-izquierda. | Política verde, democracia popular, liberalismo social, democracia social, progresismo social. |  http://www.gp.org/ |

Fuente: Elaboración propia, a partir de *Department of State United States of America.*

<http://www.america.gov/st/washfile-english/2007/January/20070109140913HMnietsua0.1988794.html>

2.8 Canadá.

Se localiza en América del Norte. A nivel mundial, es el segundo país con mayor extensión territorial. El sistema de gobierno está representado por una Monarquía Constitucional Parlamentaria.

Al 1 de enero de 2006, Canadá tenía 32.7 millones de habitantes (Statcan, 2006).

El nivel competitivo canadiense, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010) que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.43:

Tabla 2.43. Nivel competitivo de Canadá.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | |
|---------------------------------|-------|----------------------------|-------|----------------------------|--------------------------------------|----|
| Índice de competitividad global | 9 | Requerimientos básicos. | 10 | Instituciones | 17 | |
| | | | | Infraestructura | 7 | |
| | | | | Estabilidad macroeconómica | 31 | |
| | | | | Salud y educación primaria | 7 | |
| | | Potenciador de eficacia. | 4 | | Educación superior y capacitación | 9 |
| | | | | | Eficacia del mercado de bienes | 16 |
| | | | | | Eficacia del mercado de trabajo | 7 |
| | | | | | Sofisticación del mercado financiero | 11 |
| | | | | | Disponibilidad tecnológica | 11 |
| | | | | | Tamaño del mercado | 14 |
| | | Factores de la innovación. | 12 | | Sofisticación comercial | 17 |
| | | | | | Innovación | 12 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)* que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, como se percibe en la Tabla 2.44:

Tabla 2.44. Evolución en el uso de las TIC's: Canadá.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|------------|------------|------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 22'000,000 | - | 19'200,000 | 20'000,000 | -2.35% |
| Suscriptores de banda ancha | 6'706,699 | 7'675,500 | 8'680,000 | 9'210,000 | 8.25% |
| Suscriptores de telefonía móvil | 16'600,000 | 17'017,000 | 19'920,000 | 21'460,000 | 6.63% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Canadá tiene los siguientes índices, como se enuncian en las Tablas 2.45 y 2.46:

Tabla 2.45. Índice de desarrollo de las TIC's (IDI*) en Canadá (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 19 | 6.34 | 9 | 5.33 | 2.93% |

Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.46. Proporción de hogares con computadora en Canadá.



| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 79.1 | 64.0 | 3.59% |












Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.







2.8.1 Partidos políticos.

Los partidos políticos (*Elections Canada, 2009*) que actualmente tienen un registro oficial, son los que se enuncian en la Tabla 2.47:

Tabla 2.47. Principales partidos políticos en Canadá.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|--|-------------|-------------------|--|--|
| <i>Animal Alliance Environment Voters Party of Canada</i> (AAEVP C). | 2005 | Centro | Activismo de los derechos animales, ambientalismo. |  http://www.environmentvoters.org/ |
| <i>Bloc Québécois (BQ)</i> | 15/Jun/1991 | Centro-izquierda. | Democracia social, nacionalismo, independentismo. |  http://www.blocqueb.com/ |

| | | | | |
|---|-------------|---------------------------|---|--|
| | | | | ecois.org/ |
| <i>Canadian Action Party (CAP).</i> | 1997 | Izquierda. | Nacionalismo izquierdista, anti-globalización, reforma monetaria, progresismo, populismo. |  www.CanadianActionParty.ca http://www.canadianactionparty.ca/ |
| <i>Christian Heritage Party of Canada (CHP).</i> | 1987 | Derecha. | Conservatismo social, liberalismo económico, cristianismo. |  http://www.chp.ca/ |
| <i>Communist Party of Canada (CP).</i> | 1921 | Izquierda. | Comunismo. |  http://www.comunist-party.ca/ |
| <i>Conservative Party of Canada (CPC).</i> | 7/Dic/2003 | Derecha. | Conservatismo. |  http://www.conservative.ca/ |
| <i>First Peoples National Party of Canada (FPNPOC).</i> | 2004 | Centro. | Abogar por los derechos de los aborígenes, nacionalismo indígena. |  http://www.fpnpo.ca/ |
| <i>Green Party of Canada (GPC).</i> | 1983 | Centro. | Ambientalista. |  http://www.greenparty.ca/ |
| <i>Liberal Party of Canada (LP).</i> | 1/Jul/1867 | Centro, centro-izquierda. | Liberalismo. |  http://www.liberal.ca/ |
| <i>Libertarian Party of Canada (LPC).</i> | 1975 | Centro. | Libertarianismo. |  http://www.libertarian.ca/ |
| <i>Marijuana Party (MP)</i> | 2000 | Centro. | Anti-prohibicionismo radical (mariguana). |  http://www.marijuana-party.ca/ |
| <i>Marxist-Leninist Party of Canada (MLPC).</i> | 31/Mar/1970 | Izquierda. | Comunismo, Leninismo, Marxismo. |  http://www.mlpc.ca/ |
| <i>Neorhino.ca (NCA)</i> | 21/May/2006 | Centro. | Satírico, partido político del chiste. |  http://www.neorhino.ca/ |

| | | | | |
|--|-------------|-------------------------|--|--|
| | | | | ca/ |
| <i>New Democratic Party</i> (NDP). | 17/Jun/1961 | Izquierda. | Socialismo democrático, progresismo. |  http://www.ndp.ca/ |
| <i>Newfoundland and Labrador First Party</i> (NLFP). | 15/Nov/2007 | Centro. | Beneficiar en todos los aspectos a los habitantes de Newfoundlady Labrador. |  http://www.nfirst.ca/ |
| <i>People's Political Power Party of Canada</i> (PPPPC). | 2006 | Centro-derecha. | Populismo, feminismo, proteger los derechos de los aborígenes, conservatismo social. |  http://www.peoplespoliticalpower.ca/ |
| <i>Progressive Canadian Party</i> (PCP). | 29/Mar/2004 | Centro, centro-derecha. | Progresismo. |  http://www.progressivecanadian.ca/ |
| <i>Western Block Party</i> (WBP). | 29/Dic/2005 | Derecha. | Separatismo canadiense occidental, conservatismo. |  http://www.westernblockparty.com/ |
| <i>Work Less Party</i> (WLP). | 2003 | Centro. | Proteger los derechos de los trabajadores, anti consumismo. |  http://www.worklessparty.org/ |

Fuente: Elaboración propia, a partir de *Elections Canada On-Line*.

<http://www.elections.ca/content.asp?section=pol&document=index&dir=par&lang=e>

De la lista anterior, sobresalen: el Partido Liberal de Canadá (Liberal Party of Canada), el Partido Conservador de Canadá (Conservative Party of Canada) y el Partido Nuevo Democrático (New Democratic Party), quienes poseen un mayor número de simpatizantes.

2.8.2 Evolución del voto electrónico.

Canadá es uno de los países más avanzados en el continente americano, en cuanto a voto electrónico. Está distribuido en 308 circunscripciones. Las provincias están organizadas de igual modo, aunque con menor cantidad de distritos.

Históricamente ha usado boletas de papel en todos sus eventos democráticos. En algunos casos, ha sido válido el voto por correo postal. La introducción del voto electrónico se produce a mitad de la década de 1990, usando los sistemas de primera generación: Diebold y ES&S, diseñados antes de que se emitieran las Normas de Sistemas de Votación (*Federal Election Comissions*, 2009). Igualmente, los estándares HAVA (*Help America Vote Act of 2002*), lo cual ocasionó que estos sistemas no cumplieran con estándares como; facilidad de acceso, seguridad, transparencia, entre otros.

De acuerdo con la Subdivisión de Investigación Parlamentaria (Acharya, 2003): “el grupo de votantes registrados en elecciones federales canadienses ha disminuido constantemente, a partir del 80.6% de 1958, a una disminución récord de 61.2% en la elección federal pasada en 2000”. Esto se puede apreciar en la Figura 2.17

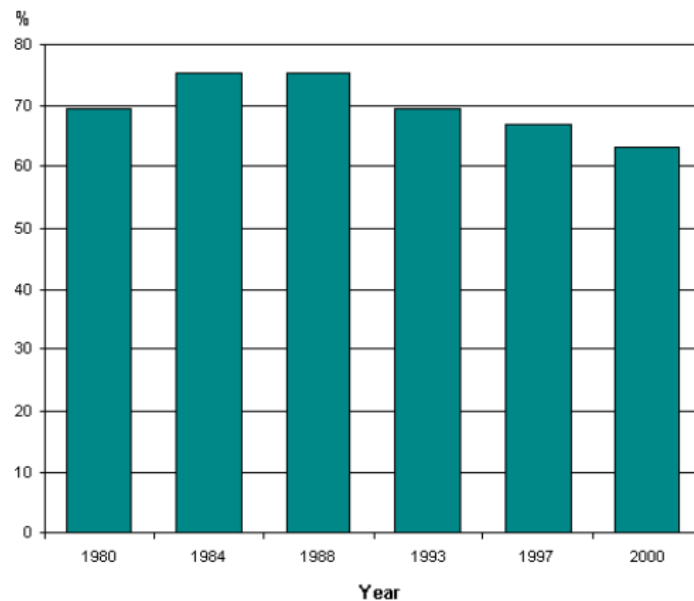


Figura 2.17. Porcentaje de participación en las Elecciones Federales de Canadá (1980-2000).

Fuente:<http://www.statcan.ca/english/freepub/89F0123XIE/00002/32.htm>.

Estos datos se han convertido en un factor crítico para una sociedad de primer mundo, consolidada en sus procesos democráticos, y sobre todo, madurez en el uso de TIC's.

De acuerdo con la página del Órgano Electoral Canadiense (*Federal Election Commissions*, 2009), independientemente de cómo se realice un proceso electoral, se deben cumplir las siguientes 17 máximas:

1. Democracia.
2. Precisión.
3. Seguridad.
4. Secreto.
5. Verificabilidad / Auditabilidad.
6. Privacidad / Confidencialidad.
7. Transparencia.
8. Accesibilidad.
9. Neutralidad.
10. Simplicidad.
11. Flexibilidad.
12. Escalabilidad.
13. Valorización.
14. Movilidad.
15. Velocidad de recuento.
16. Costo-Efectividad.
17. Durabilidad técnica.

Con estas premisas, ya incluidas en los nuevos sistemas para votar, se llevó a cabo un nuevo test (ver Figura 2.18). Eso permitió retomar el proceso de modernización que el colegio electoral canadiense había iniciado en enero de 2003, cuando el Nuevo Partido Demócrata empleó un sistema de votación electrónica (proporcionado por election.com) para elegir a un

nuevo líder. Los miembros del partido podían votar a través del correo, Internet o personalmente en la convención.

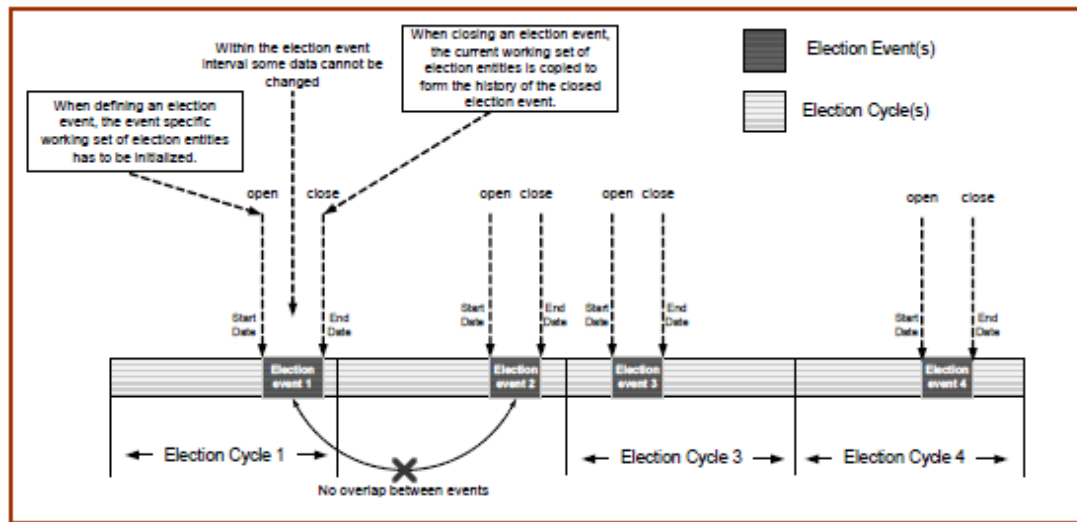


Figura 2.18. Flujo de trabajo para automatizar el proceso electoral en Canadá.

Fuente: Robert Krimmer, *Electronic Vote 2006* (p.132).

Los archivos que se utilizan en las elecciones canadienses, se depositan en una base de datos común, en formato binario y encriptado. Además de establecer los lineamientos para llevar a cabo el evento, con el propósito de tener un canal único, para evitar errores de conteo, como se observa en las Figuras 2.19 y 2.20.

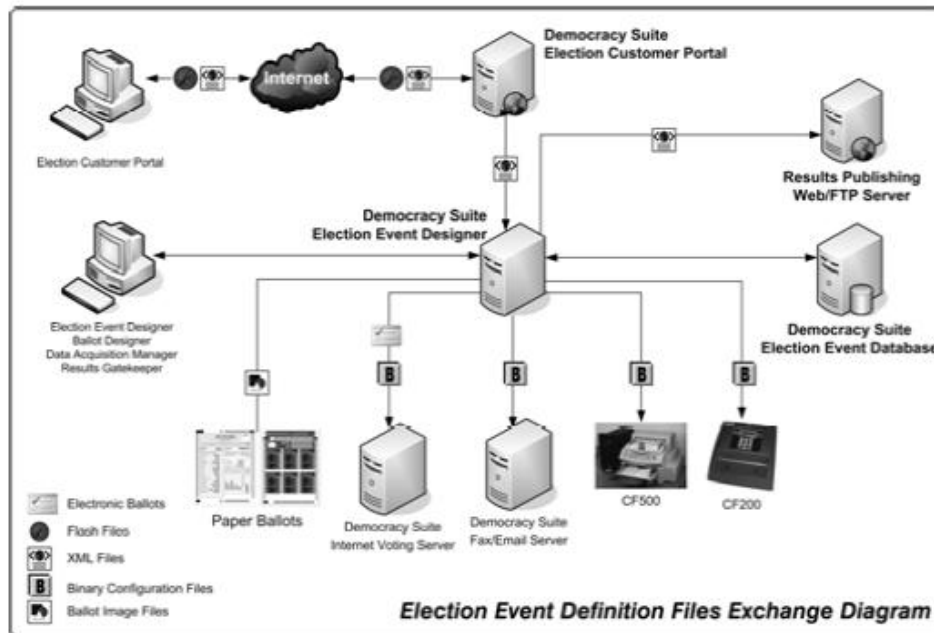


Figura 2.19. Definición de los archivos electorales.

Fuente: Robert Krimmer, *Electronic Vote 2006* (p.133).

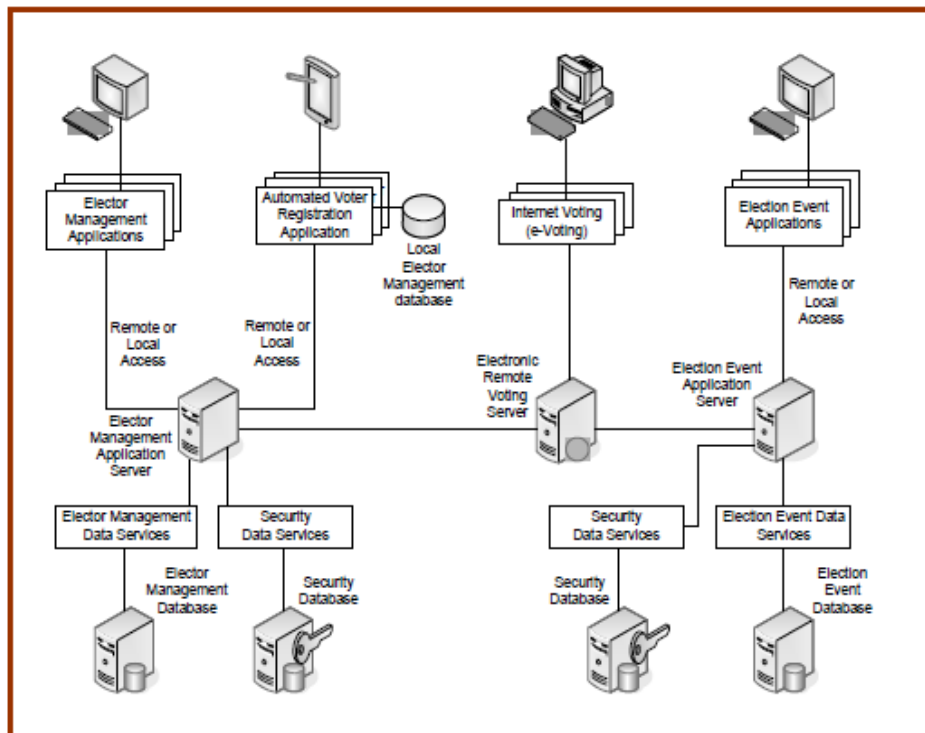


Figura 2.20. Modelo de datos para la elección de los servicios automatizados.

Fuente: Robert Krimmer, *Electronic Vote 2006* (p.135).

Las bases de datos que se utilizan en el proceso, se clasifican de la siguiente manera:

- a) Lógicamente separada del evento electoral.
- b) Lógicamente adjunta a la elección de eventos.
- c) Lógicamente adosadas en caso de las elecciones.

La validez de las entidades anteriores tiene una temporalidad, de acuerdo con las elecciones, para evitar posibles corruptelas. Además de cumplir con las características de un sistema de bases de datos de alto desempeño:

- Concurrencia.
- Multiusuario.
- Multiprocesos.
- Seguridad.
- Arreglos de discos.
- Mapeo de servicios.
- Respaldo en línea.

De acuerdo con Krimmer (2006), el proceso canadiense de voto electrónico es el siguiente:

Fase 1. Gestión del elector. Esta fase es común para cualquier tipo de elección, independientemente del método de votación que se emplea. Al final de la gestión del proceso de elector, el sistema genera la invitación para votar (NRC). Tarjetas que se envían por correo a los votantes elegibles. Cada tarjeta contiene información acerca de la NRC del votante, incluyendo; nombre, dirección, identificador único elector (Elector ID), etc.

Fase 2. Registro de Voto Electrónico. A la recepción de sus tarjetas NRC, los votantes pueden elegir, usando una boleta de papel tradicional en el centro de votación, o inscribirse para usar el voto por Internet. Si un elector decide votar a través de Internet, primero debe registrarse en el sitio designado (Internet Registro). Con base en

esta información, el sistema genera un único Número de Identificación Electoral (*EIN*). Este número se comunica a los electores, mediante el servicio de correo seguro.

Fase 3. Descarga de boleta electrónica. En el día de la elección, los electores que recibieron los códigos *EIN*, acceden al Servidor de Emisión de Boletas en Internet y proceden a votar mediante la descarga de una boleta electrónica. Cada boleta se genera en forma dinámica con la información mapeada del elector, contenida en la base de datos. Además, cada boleta contiene un número generado aleatoriamente, llamado Código de Activación de la Boleta (*BAC*), que está impreso en la boleta electoral en forma de matriz de códigos de barras 2D. Este código garantiza que una votación se otorgue y emita sólo una vez.

Fase 4. E-Voting. La boleta electrónica puede recibir ayuda del sistema, configurar las opciones de marcado; cuadrado, óvalo, círculo, flecha, X, marca, etcétera. Igualmente; capacidades de audio, características de ampliación, entre otros. Esto es especialmente importante para las personas con deficiencias visuales. El proceso de votación es idéntico al que se realiza mediante una boleta de papel. Después de hacer una elección, se debe presionar el botón Enviar. El elector recibe acuse de recibo, se contabiliza el voto y se pone en serie, en el Servidor de Votación de Internet, mediante un enlace de comunicación seguro. En este punto, el código *EIN* es destruido y el estado de voto del elector se cambia.

Fase 5. Resultados totales y presentación de informes. La fase de resultados y reportes es igual a la de cualquier método para votar. El servidor de voto por Internet produce archivos, con los resultados, en el mismo formato que los producidos por los dispositivos tabuladores de las boletas de papel.

En las Figuras 2.21 y 2.22 se presentan pantallas del sistema canadiense.

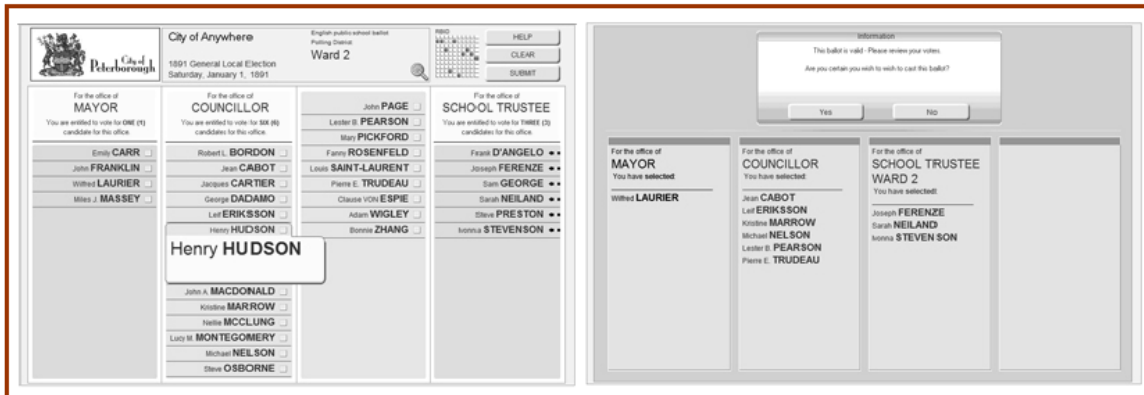


Figura 2.21. Ejemplo de una boleta electrónica.

Fuente: Robert Krimmer, *Electronic Vote 2006* (p.140).

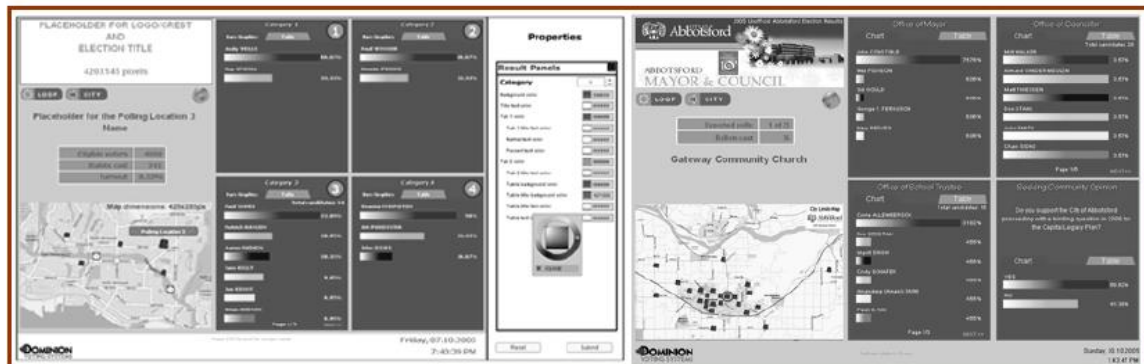


Figura 2.22. Reporte y procesamiento de la elección.
Fuente: Robert Krimmer, *Electronic Vote 2006* (p.141).

2.9 Argentina.

Se localiza al sureste de América. Su capital es Buenos Aires. El sistema de gobierno está representado por una República Federal Democrática.

El nivel competitivo argentino, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010), que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.48:

Tabla 2.48. Nivel competitivo de Argentina.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | | |
|---------------------------------|----------------------------|--------------------------|-------|----------------------------|-------------------------|--------------------------------------|-----|
| Índice de competitividad global | 85 | Requerimientos básicos. | 84 | Instituciones | 126 | | |
| | | | | Infraestructura | 88 | | |
| | | | | Estabilidad macroeconómica | 48 | | |
| | | | | Salud y educación primaria | 59 | | |
| | | Potenciador de eficacia. | 84 | | | Educación superior y capacitación | 55 |
| | | | | | | Eficacia del mercado de bienes | 124 |
| | | | | | | Eficacia del mercado de trabajo | 123 |
| | | | | | | Sofisticación del mercado financiero | 116 |
| | Disponibilidad tecnológica | | | | | 68 | |
| | Factores de la innovación. | 76 | | | Tamaño del mercado | 23 | |
| | | | | | Sofisticación comercial | 73 | |
| | | | | | Innovación | 86 | |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)*, que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, como se muestra en la Tabla 2.48:

Tabla 2.49. Evolución en el uso de las TIC's: Argentina.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|------------|------------|------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 6'863,466 | 8'183,700 | 16'000,000 | 20'000,000 | 30.65% |
| Suscriptores de banda ancha | 841,000 | 1'567,700 | 2'330,000 | 3'010,000 | 37.54% |
| Suscriptores de telefonía móvil | 22'100,000 | 31'510,040 | 40'400,000 | 46'510,000 | 20.44% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Argentina tiene los siguientes índices, como se aprecia en las Tablas 2.49 y 2.50:

Tabla 2.50. Índice de desarrollo de las TIC's (IDI*) en Argentina (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 47 | 4.12 | 44 | 3.06 | 5.08% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.51. Proporción de hogares con computadora en Argentina.






| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 36.4 | 27.0 | 5.1% |

Fuente: Elaboración propia, a partir de ITU. *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009.*







2.9.1 Partidos políticos.

En la Tabla 2.52 se describen los partidos políticos en Argentina.

Tabla 2.52. Principales partidos políticos en Argentina.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|------------------------------|------------|-------------------|--|--|
| Partido de la Victoria (PV). | 2003 | Centro-izquierda. | Reforma política, democracia real. |  Partido de la Victoria http://www.partidodelavictoria.com.ar/ |
| Partido Federal (PF) | 8/Dic/1973 | Centro. | Valores republicanos, defensa del federalismo y autonomías provinciales. |  http://www.federal.org.ar/ |
| Partido Frente Grande (PFG). | 1993 | Centro-derecha. | Justicia social, inclusión social. |  http://www.frentegrande.org.ar/ |
| Partido Humanista (PH). | 1984 | Izquierda. | Humanismo, no violencia, no discriminación, nuevo modelo económico. |  http://www.partidohumanista.deargentina.org/ |
| Partido Intransigente (PI). | 1972 | Izquierda. | Democracia social, yrigoyenismo. |  http://www.pi.org.ar/ |
| Partido Justicialista (PJ). | 1947 | Derecha. | Peronista. |  http://www.pjcapital.com.ar/ |

| | | | | |
|--|-------------|-----------------------------|--|--|
| Partido Obrero (PO) | 1964 | Izquierda. | Comunismo, trotskismo. |  http://www.po.org.ar/ |
| Partido Progreso Social (PPS). | 1996 | Izquierda. | Socialismo humanista. |  http://partidoprogressocial.blogspot.com |
| Partido Socialista (PS). | 28/Jun/1896 | Centro-izquierda. | Socialismo democrático. |  http://www.partidosocialista.org.ar/ |
| Recrear para el Crecimiento (RPC). | 2002 | Centro-derecha. | Liberalismo. |  http://recrear.org.ar/ |
| Unión Cívica Radical (UCR). | 26/Jun/1891 | Izquierda. | Radicalismo, liberalismo social. |  http://www.ucr.org.ar/ |
| Unión de Centro Democrático (UCD). | 1982 | Derecha. | Conservadurismo. |  http://ucdenacional.blogspot.com/ |
| Afirmación para una República Igualitaria (ARI). | 2002 | Centro-izquierda. | Democracia social. |  http://www.ari.org.ar/ |
| Confederación Coalición Cívica (CCC). | 11/Abr/2007 | Centro, derecha, izquierda. | Diversidad de ideologías. |  http://www.coalicioncivica.org.ar/ |
| Movimiento al Socialismo (MAS). | 1982 | Izquierda. | Marxista, trotskista. |  http://www.mas.org.ar/ |
| Movimiento de Integración y Desarrollo (MID). | 1963 | Izquierda. | Desarrollismo, liberalismo progresista. |  http://www.mid.org.ar/ |
| Movimiento por la Dignidad y la Independencia (MODIN). | 1988 | Derecha. | Militarismo, conservadurismo, populismo. |  http://www.modin.org.ar/ |
| Política Abierta para la | 1995 | Centro-izquierda. | Equidad social, independencia |  |

| | | | | |
|---|-------------|-----------------------------|---|--|
| Integridad Social (PAIS). | | | económica, soberanía política. | http://www.partidopais.com.ar/ |
| Partido Demócrata Cristiano (PDC). | 1954 | Centro-derecha. | Social cristianismo, democracia cristiana. |  http://www.democraciacristiana.com.ar/ |
| Partido Demócrata Progresista (PDP). | 1914 | Centro-derecha. | Liberalismo. |  http://www.demoprogresista.org.ar/ |
| Partido de los Trabajadores Socialistas (PTS). | 1988 | Izquierda. | Comunismo, trotskismo. |  http://www.pts.org.ar/ |
| Partido Nacionalista Constitucional UNIR (PNCUNIR). | 1982 | Centro, izquierda, derecha. | Nacionalismo, valores éticos y de identidad, cohesión cultural. |  http://pnc-unir.org.ar/ |
| Partido Popular de la Reconstrucción (PPR). | 1996 | Ultraderecha. | Nacionalismo, catolicismo, conservadurismo. |  http://www.niunpasoatrasppr.com.ar/ |
| Partido Socialista Auténtico (PSA). | 14/Dic/1892 | Centro-izquierda. | Socialismo democrático. |  http://www.psa.org.ar/ |

Fuente: Elaboración propia, a partir del Poder Judicial de la Nación República Argentina.
<http://www.pjn.gov.ar/cne/documentos/seminario/Sistema%20de%20Partidos%202009.pdf>

2.10 Brasil.

Su capital es Brasilia. El sistema de gobierno que está vigente en ese país es la República Federal Presidencial.

De acuerdo con el Instituto Brasileño de Geografía y Estadística (IBGE), al 11 de diciembre de 2009 existía una población de 192'168,326 habitantes.

El nivel competitivo brasileño, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010) que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.53:

Tabla 2.53. Nivel competitivo de Brasil.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | |
|---------------------------------|-------|----------------------------|-------|----------------------------|--------------------------------------|----|
| Índice de competitividad global | 56 | Requerimientos básicos. | 91 | Instituciones | 93 | |
| | | | | Infraestructura | 74 | |
| | | | | Estabilidad macroeconómica | 109 | |
| | | | | Salud y educación primaria | 79 | |
| | | Potenciador de eficacia. | 42 | | Educación superior y capacitación | 58 |
| | | | | | Eficacia del mercado de bienes | 99 |
| | | | | | Eficacia del mercado de trabajo | 80 |
| | | | | | Sofisticación del mercado financiero | 51 |
| | | | | | Disponibilidad tecnológica | 46 |
| | | | | | Tamaño del mercado | 10 |
| | | Factores de la innovación. | 38 | | Sofisticación comercial | 32 |
| | | | | | Innovación | 43 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)*, que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, enmarcados en la Tabla 2.54:

Tabla 2.54. Evolución en el uso de las TIC's: Brasil.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|------------|-------------|-------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 36'356,000 | 42'600,000 | 45'000,000 | 50'000,000 | 8.29% |
| Suscriptores de banda ancha | 3'304,000 | 5'921,900 | 7'720,000 | 10'020,000 | 31.96% |
| Suscriptores de telefonía móvil | 86'210,000 | 99'918,600 | 120'980,000 | 150'640,000 | 14.97% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, Brasil tiene los siguientes índices, como se muestra en las Tablas 2.55 y 2.56:

Tabla 2.55. Índice de desarrollo de las TIC's (IDI*) en Brasil (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 60 | 3.48 | 54 | 2.55 | 5.32% |

Fuente: Elaboración propia a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.56. Proporción de hogares con computadora en Brasil.

| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 20.8 | 14.2 | 6.57% |




Fuente: Elaboración propia, a partir de ITU. *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009.*

2.10.1 Partidos políticos.

En la Tabla 2.56 se describen los partidos políticos en Brasil.

Tabla 2.57. Principales partidos políticos en Brasil.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|--|-------------|-------------------|-------------------------|--|
| <i>Partido dos Trabalhadores (PT).</i> | 10/Feb/1980 | Izquierda. | Socialismo democrático. |  http://www.pt.org.br/ |
| <i>Partido da Social Democracia Brasileira (PSDB).</i> | 25/Jun/1988 | Centro-izquierda. | Liberalismo social. |  https://www2.psdb.org.br/ |
| <i>Partido do Movimento Democrático Brasileiro (PMDB).</i> | 30/Jun/1981 | Centro. | Democracia. |  http://www.pmdb.org.br/ |
| <i>Partido Socialista Brasileiro (PSB).</i> | 1988 | Izquierda. | Socialismo. |  http://www.psbnational.org.br/ |
| <i>Partido Socialismo e Liberdade (PSOL).</i> | 2005 | Izquierda. | Socialismo. |  http://www.psol.org.br/ |
| <i>Partido Democrático Trabalhista (PDT).</i> | 19/Jun/1979 | Izquierda. | Democracia social. |  http://www.pdt.org.br/ |

| | | | | |
|---|-------------|-----------------|---|--|
| <i>Partido Social Democrata Cristão (PSDC).</i> | 5/Ago/1997 | Centro-derecha. | Democracia social. |  http://www.psdcbrazil.org.br/ |
| <i>Partido Republicano Progressista (PRP).</i> | 22/Nov/1991 | Centro-derecha. | Libertad, igualdad, fraternidad, justicia, paz, progreso y orden. |  http://www.prp.org.br/ |
| <i>Partido Social Liberal (PSL).</i> | 2/Jun/1998 | Centro. | Neoliberalismo, democracia social. |  http://www.pslnacional.org.br/ |

Fuente: Elaboración propia, a partir del Tribunal Superior Electoral de Brasil.

http://www.tse.gov.br/internet/partidos/fundo_partidario/2009.htm

2.11 Venezuela.

Está ubicado en América del Sur. Oficialmente es conocida como la República Bolivariana de Venezuela. Su capital es Caracas.

Tiene un gobierno Presidencialista Multipartidista.

De acuerdo con el Instituto Nacional de Estadística (INE), al 11 de diciembre de 2009, este país cuenta con una población de 28'582,987 habitantes.

El nivel competitivo venezolano, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010), que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.58:

Tabla 2.58. Nivel competitivo de Venezuela.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | | |
|---------------------------------|-------|----------------------------|-------|----------------------------|-------|--------------------------------------|-----|
| Índice de competitividad global | 113 | Requerimientos básicos. | 104 | Instituciones | 133 | | |
| | | | | Infraestructura | 106 | | |
| | | | | Estabilidad macroeconómica | 91 | | |
| | | | | Salud y educación primaria | 81 | | |
| | | Potenciador de eficacia. | 108 | | | Educación superior y capacitación | 83 |
| | | | | | | Eficacia del mercado de bienes | 132 |
| | | | | | | Eficacia del mercado de trabajo | 133 |
| | | | | | | Sofisticación del mercado financiero | 126 |
| | | | | | | Disponibilidad tecnológica | 91 |
| | | Factores de la innovación. | 130 | | | Tamaño del mercado | 37 |
| | | | | | | Sofisticación comercial | 132 |
| | | | | | | Innovación | 123 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)*, que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, este país presenta los siguientes indicadores, como se aprecia en la Tabla 2.59:

Tabla 2.59. Evolución en el uso de las TIC's: Venezuela.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|------------|------------|------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 3'313,000 | 4'139,800 | 5'720,000 | 7'170,000 | 21.29% |
| Suscriptores de banda ancha | 356,898 | 537,500 | 860,000 | 1'330,000 | 38.94% |
| Suscriptores de telefonía móvil | 12'495,721 | 18'789,500 | 23'820,000 | 27'080,000 | 21.33% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009), que publica la *ITU*, Venezuela tiene los siguientes índices, como se describe en las Tablas 2.60 y 2.61:

Tabla 2.60. Índice de desarrollo de las TIC's (IDI*) en Venezuela (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 67 | 3.34 | 69 | 2.18 | 7.37% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.61. Proporción de hogares con computadora en Venezuela.

| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 11.9 | 5.1 | 15.17% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

2.11.1 Partidos políticos.

En la Tabla 2.62 se describen los partidos políticos en Venezuela.

Tabla 2.62. Principales partidos políticos en Venezuela.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|---|-------------|---------------------------|---|--|
| Acción Democrática (AD). | 13/Sep/1941 | Centrismo. | Democracia social. |  http://acciondemocratica.org.ve/ |
| Partido Comunista de Venezuela (PCV). | 5/Mar/1931 | Izquierda. | Comunismo, marxismo-leninismo. |  http://www.pcv-venezuela.org/ |
| Patria Para Todos (PPT). | 27/Sep/1997 | Izquierda. | Pluralismo. |  http://www.ppt.org.ve/ |
| Primero Justicia (PJ) | 2003 | Centro-derecha. | Centrismo, liberalismo, humanismo y reformismo. |  http://www.primerojusticia.org.ve/ |
| Partido Socialista Unido de Venezuela (PSUV). | 2007 | Izquierda revolucionaria. | Socialismo, marxismo, bolivarianismo, nacionalismo, antiimperialismo. |  http://www.psuve.org.ve/ |
| Fuerza Liberal (FL) | 2003 | Centro-derecha. | Liberalismo progresista. |  http://www.fuerzaliberal.org.ve/ |

| | | | | |
|--|-------------|-------------------|---|--|
| Partido Federal Republicano (PFR). | 20/Oct/2003 | Centro-izquierda. | Conservadora social progresista, nacionalista, federalista. |  http://www.federalrepublicano.org.ve/ |
| Un Nuevo Tiempo (UNT). | 2006 | Centro. | Democracia social, humanismo liberal, justicia social. |  http://www.partidounnuevotiempo.org/ |
| Comité de Organización Política Electoral Independiente (COPEI). | 13/Ene/1946 | Centro-derecha. | Reformista, democracia cristiana, humanismo cristiano. |  http://www.partidocopei.org.ve/ |
| Movimiento al Socialismo (MAS). | 1971 | Centro-izquierda. | Democracia social. |  http://movimientoalsocialismo.blogspot.com/ |
| Por la democracia social (Podemos). | 2002 | Centro-izquierda. | Democracia social, humanismo. |  http://www.podemos.com.ve/ |

Fuente: Elaboración propia, a partir del Consejo Nacional Electoral de la República Bolivariana de Venezuela.

<http://www.cne.gob.ve/noticiaDetallada.php?id=4303&>

2.12 México.

Es reconocido oficialmente como los Estados Unidos Mexicanos. Su gobierno está representado por una República Federal.

De acuerdo con el Censo de Población y Vivienda 2005, realizado por el Instituto Nacional de Estadística Geografía e Informática (INEGI), nuestro país tiene una población de 103'300,000 habitantes.

El nivel competitivo mexicano, de acuerdo con los datos que aparecen en *The Global Competitiveness Report 2009-2010* (Reporte de Competitividad Global 2009-2010), que publica el *World Economic Forum* (Foro Económico Mundial, FEM), se muestra en la Tabla 2.63:

Tabla 2.63. Nivel competitivo de México.

| Indicador | Lugar | Subíndices | Lugar | Pilares | Lugar | | |
|---------------------------------|-------|----------------------------|-------|----------------------------|-------|--------------------------------------|-----|
| Índice de competitividad global | 60 | Requerimientos básicos. | 59 | Instituciones | 98 | | |
| | | | | Infraestructura | 69 | | |
| | | | | Estabilidad macroeconómica | 28 | | |
| | | | | Salud y educación primaria | 65 | | |
| | | Potenciador de eficacia. | 55 | | | Educación superior y capacitación | 74 |
| | | | | | | Eficacia del mercado de bienes | 90 |
| | | | | | | Eficacia del mercado de trabajo | 115 |
| | | | | | | Sofisticación del mercado financiero | 73 |
| | | | | | | Disponibilidad tecnológica | 71 |
| | | | | | | Tamaño del mercado | 11 |
| | | Factores de la innovación. | 67 | | | Sofisticación comercial | 62 |
| | | | | | | Innovación | 78 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

* Total de países considerados en el reporte: 133

Por otro lado, conforme a los datos que aparecen en el *IER (Information Economy Report, Reporte de Información Económica)*, que publica la *UNCTAD (United Nations Conference on Trade and Development, Conferencia de las Naciones Unidas sobre Comercio y Desarrollo)*, nuestro país presenta los siguientes indicadores, como lo muestra la Tabla 2.64:

Tabla 2.64. Evolución en el uso de las TIC's: México.

| Indicador | Año | | | | Tasa de crecimiento |
|---------------------------------|------------|------------|------------|------------|---------------------|
| | 2005 | 2006 | 2007 | 2008 | |
| Usuarios de Internet | 18'622,509 | 22'000,000 | 20'850,000 | 22'340,000 | 4.66% |
| Suscriptores de banda ancha | 2'304,520 | 3'728,200 | 4'550,000 | 5'700,000 | 25.41% |
| Suscriptores de telefonía móvil | 47'462,108 | 57'016,400 | 68'240,000 | 75'300,000 | 12.23% |

Fuente: Elaboración propia, a partir del *IER (UNCTAD)*. Cálculos basados en los indicadores de la base de datos Telecomunicaciones en el Mundo de la Unión Internacional de Telecomunicaciones (*ITU*), 2006-2009.

Finalmente, en el documento *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009* (Midiendo la Sociedad de la Información, Índice de Desarrollo de las TIC's 2009) que publica la *ITU*, México tiene los siguientes índices, como se señalan en las Tablas 2.65 y 2.66:

Tabla 2.65. Índice de desarrollo de las TIC's (IDI*) en México (2002 y 2007).

| 2007 | | 2002 | | Tasa de crecimiento |
|------------|------|----------|------|---------------------|
| Posición** | IDI | Posición | IDI | IDI |
| 75 | 3.09 | 64 | 2.38 | 4.45% |

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

*IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's. El índice se genera a partir del número de líneas telefónicas fijas por cada 100 habitantes. Más el número de suscriptores de telefonía celular por cada 100 habitantes. Incluye el ancho de banda que tienen los usuarios de Internet, a nivel internacional (bps). Toma en cuenta; la proporción de hogares con computadora, proporción de hogares con Internet, usuarios de Internet por cada 100 habitantes, suscriptores de Internet de banda ancha fija por cada 100 habitantes, suscriptores de banda ancha móvil por cada 100 habitantes, tasa de alfabetización adulta y proporción de la matrícula total (nivel secundario y terciario).

** Total de países considerados en el reporte: 154.

Tabla 2.66. Proporción de hogares con computadora en México.








| 2007 | 2002 | Tasa de crecimiento |
|------|------|---------------------|
| 22.1 | 15.2 | 6.44% |

Fuente: Elaboración propia, a partir de ITU. *Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009.*

2.12.1 Partidos políticos.

En la Tabla 2.67 se enumeran los diferentes partidos políticos que existen en México.

Tabla 2.67. Principales partidos políticos en México.

| Partido | Fundación | Corriente | Filosofía | Logotipo / Sitio Web |
|---|-------------|-------------------|--|--|
| Partido Revolucionario Institucional (PRI). | 18/Ene/1946 | Centro-izquierda. | Democracia social, liberalismo social. |  http://www.pri.org.mx/ |
| Partido Acción Nacional (PAN). | 15/09/1939 | Derecha. | Democracia cristiana, conservador. |  http://www.pan.org.mx/ |
| Partido de la Revolución Democrática (PRD). | 5/May/1989 | Izquierda. | Democracia social, socialismo. |  http://www.prd.org.mx/ |
| Partido Nueva Alianza (PANAL). | 2005 | Centro. | Neoliberalismo. |  http://www.nueva-alianza.org.mx/ |
| Partido Verde Ecologista de México (PVEM). | 1986 | Centro. | Política verde. |  http://www.partidoverde.org.mx/ |
| Partido del Trabajo (PT). | 8/Dic/1990 | Izquierda. | Socialismo democrático. |  http://partidodeltrabajo.org.mx/ |
| Convergencia | 1/Ago/1999 | Centro-izquierda. | Democracia social. |  http://www.convergencia.org.mx/ |

Fuente: Elaboración propia, a partir del Instituto Federal Electoral: Partidos Políticos Nacionales.

http://www.ife.org.mx/portal/site/ifev2/Directorio_y_documentos_basicos/

2.12.2 Evolución del voto electrónico.

En nuestro país, los gobiernos estatales, junto con Instituciones Electorales, han venido realizando diferentes acciones con el propósito de implantar, a mediano y largo plazo, el voto electrónico. A nivel nacional es evidente el liderazgo que ejerce el Instituto Electoral y de Participación Ciudadana de Coahuila (IEPCC) en el ámbito de las votaciones electrónicas.

Fernández et. al. (2007) afirman que:

el diseño de la urna del IEPCC ha sido uno de los escasos ejemplos de coincidencia del desarrollo tecnológico innovador, junto con el sentido común de su implementación. A diferencia de otras experiencias mexicanas e internacionales, los diferentes prototipos de la urna electrónica coahuilense han ido construyéndose, a partir de la introducción de mejoras, con el objetivo de garantizar la plena seguridad de los votantes, mejorando sus protocolos criptográficos, así como la autonomía del equipo y su usabilidad. Pero más allá de esas consideraciones, lo más interesante es la política de divulgación emprendida.

Esta urna electrónica se ha utilizado no solamente en procesos políticos públicos, como la elección local de septiembre de 2005, sino también en diferentes procesos electivos vinculantes. Igualmente, en el ámbito académico se ha utilizado para elegir autoridades académicas y consejos o sociedades estudiantiles.

Por otro lado, en los procesos electorales de carácter federal y local, que se realizaron el 2 de julio de 2006, el Instituto Electoral del Distrito Federal (IEDF) llevó a cabo una prueba piloto, con las urnas electrónicas desarrolladas por ese organismo. Para ello, previamente se llegó a un acuerdo con el Consejo General del IEDF, en abril de ese año, para decidir que la prueba piloto se hiciera con una urna por cada distrito electoral uninominal del Distrito Federal (40 urnas en total).

Además del simulacro, se aplicó una encuesta de salida a la gente que acudió a las urnas, para recoger sus opiniones sobre la urna electrónica.

Los resultados obtenidos fueron los siguientes:

- 43,433 votantes en las secciones donde estuvieron disponibles las urnas electrónicas.
- Cerca del 13% de los votantes participaron en la prueba piloto.
- El tiempo promedio empleado por los electores para realizar su voto estuvo entre 40 y 55 segundos.
- Hubo baja participación de votantes, mayores de 65 años, en la prueba (283 votantes, lo que equivale al 4.9% del total).
- El grupo más numeroso fue el de los votantes con edades entre los 18 y 39 años (3,156 votantes, lo que equivale al 54.2%).

Tras la culminación de la prueba piloto efectuada en la Ciudad de México, el IEDF desplazó al Estado de Chiapas 17 urnas: 13 para ser utilizadas y 4 quedaron disponibles para prevenir cualquier contingencia. El motivo era efectuar otra prueba de votación electrónica, junto con el proceso electoral estatal del 20 de agosto de 2006, el cual fue coordinado por el Instituto Estatal Electoral de Chiapas (IEECH).

Al igual que en el anterior simulacro, los objetivos que se buscaban eran verificar el funcionamiento de la urna electrónica. Asimismo, recoger experiencias para mejorar el diseño y funcionamiento de la misma.

Cabe aclarar que hubo una diferencia notable con respecto a la prueba piloto efectuada en el Distrito Federal, pues en esta ocasión las urnas se establecieron sin seguir el criterio de vincularlas con los centros de votación existentes, sino que ahora los criterios fueron los siguientes (IEDF, 2006b: 13):

- Lugares con la mayor afluencia ciudadana en el distrito electoral, tales como; plazas públicas, centros sociales, escuelas, entre otros.
- Instalar las urnas en lugares con espacios amplios.
- Que los sitios en donde se instalaron las urnas electrónicas contaran con los elementos necesarios para el funcionamiento de las mismas, tales como; tomas de corriente eléctrica en buen estado, techados y buena iluminación.
- Preferentemente que fueran de fácil y libre acceso para los ciudadanos y garantizaran las medidas de seguridad necesarias para el adecuado desarrollo de las pruebas. Así como de las personas que participaron en el evento.

De esta manera sólo cinco distritos tuvieron la presencia de urnas electrónicas, prevaleciendo su ubicación en los centros comerciales.

Los resultados que se obtuvieron de la prueba fueron:

- Participaron 1,086 ciudadanos.
- Predominó la participación de los hombres (67%) con respecto a las mujeres (33%).
- El tiempo promedio que se invirtió para realizar el voto fue menor a un minuto (55 segundos).

Otro estado que se distingue como precursor del voto electrónico en México, junto con Coahuila y el Distrito Federal, es San Luis Potosí. No obstante, por diversas razones no se ha podido llevar a la práctica hasta el momento.

En octubre de 2001, el Presidente del Consejo Estatal Electoral de San Luis Potosí presentó el proyecto de una urna electrónica propia, que pudiera utilizarse en los siguientes comicios estatales (Instituto de Investigaciones Jurídicas de la UNAM, 2010).

A este proyecto lo denominaron Sistema Integral de Verificación y Monitoreo (SIVEM), el cual contemplaba disponer de 30 equipos, para usarse en zonas rurales que tuvieran suministro deficiente de energía (Téllez Valdés, 2004).

La compañía Alta Tecnología fue la encargada de desarrollar los prototipos que se utilizaron para efectuar las pruebas (Fernández et. al., 2007).

2.12.3 Participación ciudadana.

Las últimas elecciones federales de México se realizaron en 2006, integrando por primera vez la votación de los ciudadanos mexicanos que residen en el extranjero y ejercieron su derecho al voto.

Los resultados finales de dicho proceso se muestran a continuación, en las Tablas 2.68, 2.69, 2.70 y 2.71:

Tabla 2.68. Participación de los ciudadanos mexicanos residentes en el extranjero (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006).

| | Lista nominal | Participación ciudadana | % Participación | Abstención | % Abstención |
|-----------------------|----------------------|--------------------------------|------------------------|-------------------|---------------------|
| Total Nacional | 40,876 | 33,131 | 81.05 | 7,745 | 18.95 |

Totales por entidad federativa

| | | | | | |
|-----------------------|-------|-------|-------|-----|-------|
| Aguascalientes | 412 | 319 | 77.43 | 93 | 22.57 |
| Baja California Norte | 1,582 | 1,337 | 84.51 | 245 | 15.49 |
| Baja California Sur | 63 | 51 | 80.95 | 12 | 19.05 |

| | | | | | |
|------------------|-------|-------|--------|-----|-------|
| Campeche | 40 | 36 | 90.00 | 4 | 10.00 |
| Coahuila | 584 | 465 | 79.62 | 119 | 20.38 |
| Colima | 345 | 277 | 80.29 | 68 | 19.71 |
| Chiapas | 169 | 121 | 71.60 | 48 | 28.40 |
| Chihuahua | 1,235 | 1,004 | 81.30 | 231 | 18.70 |
| Distrito Federal | 6,281 | 5,402 | 86.01 | 879 | 13.99 |
| Durango | 616 | 473 | 76.79 | 143 | 23.21 |
| Guanajuato | 2,793 | 2,317 | 82.96 | 476 | 17.04 |
| Guerrero | 1,117 | 848 | 75.92 | 269 | 24.08 |
| Hidalgo | 721 | 514 | 71.29 | 207 | 28.71 |
| Jalisco | 5,047 | 4,182 | 82.86 | 865 | 17.14 |
| Estado de México | 4,149 | 3,350 | 80.74 | 799 | 19.26 |
| Michoacán | 3,368 | 2,661 | 79.01 | 707 | 20.99 |
| Morelos | 1,053 | 845 | 80.25 | 208 | 19.75 |
| Nayarit | 432 | 348 | 80.56 | 84 | 19.44 |
| Nuevo León | 1,799 | 1,353 | 75.21 | 446 | 24.79 |
| Oaxaca | 889 | 698 | 78.52 | 191 | 21.48 |
| Puebla | 1,631 | 1,298 | 79.58 | 333 | 20.42 |
| Querétaro | 571 | 577 | 101.05 | 0 | 0.00 |
| Quintana Roo | 151 | 138 | 91.39 | 13 | 8.61 |
| San Luis Potosí | 955 | 668 | 69.95 | 287 | 30.05 |
| Sinaloa | 584 | 461 | 78.94 | 123 | 21.06 |
| Sonora | 679 | 549 | 80.85 | 130 | 19.15 |
| Tabasco | 160 | 121 | 75.63 | 39 | 24.37 |
| Tamaulipas | 991 | 704 | 71.04 | 287 | 28.96 |
| Tlaxcala | 169 | 137 | 81.07 | 32 | 18.93 |
| Veracruz | 1,191 | 988 | 82.96 | 203 | 17.04 |
| Yucatán | 200 | 165 | 82.50 | 35 | 17.50 |
| Zacatecas | 899 | 724 | 80.53 | 175 | 19.47 |

Fuente: Elaboración propia, a partir de Instituto Federal Electoral: Voto de los mexicanos residentes en el extranjero.

http://www.ife.org.mx/documentos/OE/participacion2006/reportes/nac_votomex.html

Tabla 2.69. Paquetes electorales postales enviados y recibidos por continente. Participación de los ciudadanos mexicanos residentes en el extranjero (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006).

| | Paquetes electorales postales enviados. | Sobres con votos recibidos que fueron turnados a escrutinio y cómputo. | % de participación |
|--------------|--|---|---------------------------|
| Total | 40,876 | 32,632 | 79.83 |

Totales por continente

| | | | |
|----------------------|--------|--------|-------|
| Continente Africano | 13 | 7 | 53.85 |
| Continente Americano | 37,204 | 29,613 | 79.60 |
| Continente Asiático | 149 | 118 | 79.19 |
| Continente Europeo | 3,509 | 2,894 | 82.47 |
| Oceanía | 1 | 0 | 0 |

Fuente: Elaboración propia, a partir de Instituto Federal Electoral: Voto de los mexicanos residentes en el extranjero.

http://www.ife.org.mx/documentos/OE/participacion2006/reportes/nac_sobres.html

Tabla 2.70. Participación ciudadana a nivel nacional y por entidad federativa * (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006).

| | Lista nominal | Participación ciudadana | % Participación | Abstención | % Abstención |
|-----------------------|----------------------|--------------------------------|------------------------|-------------------|---------------------|
| Total Nacional | 71'374,373 | 41'791,322 | 58.55 | 29'583,051 | 41.45 |

Totales por entidad federativa

| | | | | | |
|-----------------------|-----------|---------|-------|-----------|-------|
| Aguascalientes | 703,700 | 413,897 | 58.82 | 289,803 | 41.18 |
| Baja California Norte | 2'024,311 | 950,720 | 46.97 | 1'073,591 | 53.03 |
| Baja California Sur | 329,952 | 180,847 | 54.81 | 149,105 | 45.19 |

| | | | | | |
|------------------|---------------|-----------|-------|---------------|-------|
| Campeche | 483,244 | 312,522 | 64.67 | 170,722 | 35.33 |
| Coahuila | 1'707,90 4 | 929,944 | 54.45 | 777,960 | 45.55 |
| Colima | 410,285 | 258,126 | 62.91 | 152,159 | 37.09 |
| Chiapas | 2'594,04 4 | 1'272,623 | 49.06 | 1'321,4 21 | 50.94 |
| Chihuahua | 2'382,46 0 | 1'161,633 | 48.76 | 1'220,8 27 | 51.24 |
| Distrito Federal | 7'111,11 8 | 4'839,285 | 68.05 | 2'271,8 33 | 31.95 |
| Durango | 1'052,05 2 | 572,043 | 54.37 | 480,009 | 45.63 |
| Guanajuato | 3'425,08 1 | 1'961,051 | 57.26 | 1'464,0 30 | 42.74 |
| Guerrero | 2'135,21 3 | 992,131 | 46.47 | 1'143,0 82 | 53.53 |
| Hidalgo | 1'621,72 7 | 945,590 | 58.31 | 676,137 | 41.69 |
| Jalisco | 4'711,39 9 | 2'910,366 | 61.77 | 1'801,0 33 | 38.23 |
| Estado de México | 9'155,39 6 | 5'701,032 | 62.27 | 3'454,3 64 | 37.73 |
| Michoacán | 2'952,11 4 | 1'495,097 | 50.64 | 1'457,0 17 | 49.36 |
| Morelos | 1'176,59 8 | 709,101 | 60.27 | 467,497 | 39.73 |
| Nayarit | 673,987 | 365,847 | 54.28 | 308,140 | 45.72 |
| Nuevo León | 2'947,53 2 | 1'769,218 | 60.02 | 1'178,3 14 | 39.98 |
| Oaxaca | 2'322,94 9 | 1'349,183 | 58.08 | 973,766 | 41.92 |
| Puebla | 3'436,51 9 | 1'984,166 | 57.74 | 1'452,3 53 | 42.26 |
| Querétaro | 1'033,11 4 | 660,384 | 63.92 | 372,730 | 36.08 |
| Quintana Roo | 675,884 | 385,722 | 57.07 | 290,162 | 42.93 |
| San Luis Potosí | 1'592,13 6 | 951,724 | 59.78 | 640,412 | 40.22 |
| Sinaloa | 1'732,09 6 | 980,684 | 56.62 | 751,412 | 43.38 |
| Sonora | 1'669,40 3 | 934,327 | 55.97 | 735,076 | 44.03 |
| Tabasco | 1'335,45 | 911,113 | 68.22 | 424,341 | 31.78 |

| | | | | | |
|------------|---------------|-----------|-------|---------------|-------|
| | 4 | | | | |
| Tamaulipas | 2'225,12 9 | 1'225,922 | 55.09 | 999,207 | 44.91 |
| Tlaxcala | 704,648 | 410,230 | 58.22 | 294,418 | 41.78 |
| Veracruz | 4'875,67 7 | 2'942,364 | 60.35 | 1'933,3 13 | 39.65 |
| Yucatán | 1'178,71 9 | 789,155 | 66.95 | 389,564 | 33.05 |
| Zacatecas | 994,528 | 525,275 | 52.82 | 469,253 | 47.18 |

* Incluye los votos de los ciudadanos mexicanos residentes en el extranjero.

Fuente: Elaboración propia, a partir del Instituto Federal Electoral.

<http://www.ife.org.mx/documentos/OE/participacion2006/reportes/nac.html>

2.13 Entorno del voto electrónico seguro.

2.13.1 Seguridad.

Un entorno seguro, en todos los ámbitos democráticos, es lo que se ha venido persiguiendo en las dos últimas décadas de la vida política del país. La seguridad del voto electrónico va a influir en mucho a certificar la validez o no del sistema, ya que viene a ser una de las columnas vertebrales de la implementación. Dentro de la seguridad intervienen factores críticos, como los que se enuncian a continuación:

- Acceso a las urnas en sitio.
- Políticas de acceso al sistema.
- Seguridad en la red de comunicaciones.
- Sistemas de criptografía que garanticen la secrecía del voto.
- Seguridad en los Sistemas Operativos (administración correcta).
- Sistemas de respaldo en línea.
- Sistemas de respaldo de suministro eléctrico.
- Correcta capacitación al personal que ha de llevar a cabo la gestión de los equipos.
- Logística certificada por parte del órgano electoral.

Las características antes mencionadas son las mínimas indispensables, para operar un esquema de voto electrónico que se digne de tener confianza para el público elector. Que ofrezca y sea garante de la confidencialidad que debe dar a todos los involucrados en una elección vinculante.

2.13.2 Confiabilidad.

Básicamente, la confiabilidad de los sistemas se gana de acuerdo al uso permanente y la forma en como salen bien librados de los diferentes escenarios que surjan en el camino. Es por eso que gran parte de la tarea de los órganos electorales es la de crear confianza alrededor de estos tipos de sistemas. Dándolos a conocer a la sociedad, familiarizando su uso y potencialidad. Con lo anterior se logra a mediano plazo la aceptación y por ende, la legitimidad del proceso mismo.

Además, es importante mencionar que las auditorías que se den, deben ser abiertas a quien desee presenciarlas, para dar fe de este proceso.

La Dra. Mercuri (2010) señala, en su tesis doctoral, que existen un sinnúmero de medios para detectar el fraude en el voto electrónico, o posibles errores en el sistema. Tal es el caso del uso de criptografía, el uso de boletas de papel para su posterior verificación, las bitácoras propias del sistema, entre otros.

Así mismo, sugiere el uso de las boletas como fiel testimonio del voto emitido, conocido también como Comprobante de Auditoría de Papel Verificado por el Votante (*Voter Verified Paper Audit Trail*, VVPAT). Este comprobante es fácilmente interpretado por el elector, sin necesidad de un dispositivo para su interpretación.

Finalmente, caemos en un paradigma: ¿Qué es la confianza?. La Dra. Mercuri señala que es un concepto que, en ocasiones, cae en un ideal sin que sea definido correctamente, pues deben ser precisos sus alcances y limitaciones.

La Dra. Mercuri (2005) refiere al respecto: “Muchos significados de la palabra confianza se invocan cuando los profesionales de la computación usan la frase "computación confiable". La definición fundamental es la de su dependencia. Como en "Confío en que usted..." pero también hay algo de optimismo o esperanza en el futuro. Al igual que "podemos confiar en que el resultado debe...". Ciertamente el concepto de custodia o cuidado también participa, con "colocado en la confianza de los...". Haciendo hincapié en las relaciones entre entidades comerciales o sociales, como; organizaciones de beneficencia, fideicomisos de tierras, fideicomisos bancarios y los fideicomisos”.

2.13.3 Auditoría de las votaciones.

Como en todas las acciones que toca el hombre, siendo este el factor más inestable en una cadena de logística, la tecnología, en algún punto donde intervenga la mano del hombre, no se libra de esto, por mucho que se implanten estándares de seguridad. Como menciona Soucre O. (2004): “En toda tecnología, particularmente en las tecnologías de seguridad informática, el factor humano es un componente crítico”. Y con toda razón lo señala, pues se han reportado grandes fraudes que de manera posterior se han señalado por obra de las auditorías que las realizan.

A la fecha no se conoce algún sistema que sea capaz de resolver todos los riesgos que lo integran. El diseño de un sistema, cuando se contemplan todas las aristas que lo componen, se vuelve un tanto complicado. Recordemos que en las auditorías digitales, como en las instancias financieras o transacciones comerciales de cualquier índole, es muy complejo revisar el proceso. No sucede lo mismo en sistemas pequeños, donde podemos revisar; quién la realizó, de qué lugar, dirección, entre otra información que se obtiene. Esto es sencillo auditar, pues existe una relación lineal de la información.

En los sistemas electorales digitales, una de las condiciones que son necesarias es el anonimato del escrutinio. Situación que impone una cuestión compleja para las auditorías. En

algunos esquemas que se han implementado, en una primera etapa, es que se aplican de manera paralela: el sistema de boletas y el sistema electrónico. Lo anterior, conforme se maduran los procedimientos y los electores van otorgándole confianza al sistema electrónico, para que se vaya eliminando gradualmente el sistema de boletas.

Por lo regular, para que un sistema cumpla, se deben integrar diferentes auditorías, que deben ser:

- a) Los modelos previos serán inspeccionados por entidades no gubernamentales y organizaciones que validen el sistema libre de errores, que cumpla con la normativa en cada uno de los requerimientos, para su correcta función.
- b) Se debe garantizar que las máquinas distribuidas a los centros de votación, sean iguales a las que se revisaron previamente y que cualquier modificación que se hiciera en adelante, sea de acuerdo a los estándares vigentes.
- c) Los equipos deben ser certificados, para que sean preparados para la jornada electoral, de forma tal que estos operen de manera adecuada.

Así mismo, los sistemas deben ser probados y de cierto modo, relacionados con la población electoral que ha de emitir el sufragio. De tal forma que reciban una inducción a su mecanismo, de otro modo serían totalmente ajenos.

Algunos autores refieren que se ha asegurar todo el proceso mediante una verificación criptográfica. Esto es, que los votantes puedan verificar que han votado y verificar su voto por medio de alguna firma digital, emitida por la autoridad, como lo refieren Rodríguez-Henríquez et al (2007) y Chou-Chen et al (2004). Existe el problema que si no es diseñado correctamente, la verificabilidad podría dar pie al rastreo del voto, situación que intimidaría al elector de que alguien pudiera saber su elección.

2.13.4 Validez.

La validez del voto electrónico se ha de garantizar con los diferentes elementos que lo integran; seguridad, confiabilidad y auditabilidad. También debe garantizar su seguridad, pues se debe señalar esto con hincapié, ya que los elementos de la urna y el voto electrónico han ser evaluados de manera exhaustiva y pormenorizada. Otros factores que deben analizarse son los requisitos del entorno sociopolítico, pues este último, como lo señalan diferentes autores, es el factor más difícil de integrar al modelo (Carrancedo Gallardo & Pérez Belleboni).

Tabla 2.71. Porcentaje de participación ciudadana a nivel nacional y por entidad federativa* que representan los votos válidos y los votos nulos (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006).

| | Lista Nomin al. | Particip ación Ciudadana. | % Particip ación. | Votos Válidos. | % Participac ión ciudadana que represent an los votos válidos. | Voto s Nulo s. | % Participa ción ciudadana que represent an los votos nulos. |
|-----------------------|------------------------|----------------------------------|--------------------------|-----------------------|---|-----------------------|---|
| Total nacional | 71'374 ,373 | 41'791,3 22 | 58.55 | 40'886 ,718 | 97.84 | 904,6 04 | 2.16 |

Totales por entidad federativa

| | | | | | | | |
|-----------------------|-----------|-----------|-------|-----------|-------|--------|------|
| Aguascalientes | 703,700 | 413,897 | 58.82 | 406,228 | 98.15 | 7,669 | 1.85 |
| Baja California Norte | 2'024,311 | 950,720 | 46.97 | 933,621 | 98.20 | 17,099 | 1.80 |
| Baja California Sur | 329,952 | 180,847 | 54.81 | 178,046 | 98.45 | 2,801 | 1.55 |
| Campeche | 483,244 | 312,522 | 64.67 | 303,008 | 96.96 | 9,514 | 3.04 |
| Coahuila | 1'707,904 | 929,944 | 54.45 | 915,025 | 98.40 | 14,919 | 1.60 |
| Colima | 410,285 | 258,126 | 62.91 | 253,535 | 98.22 | 4,591 | 1.78 |
| Chiapas | 2'594,044 | 1'272,623 | 49.06 | 1'225,296 | 96.28 | 47,327 | 3.72 |
| Chihuahua | 2'382,460 | 1'161,633 | 48.76 | 1'136,228 | 97.81 | 25,405 | 2.19 |
| Distrito Federal | 7'111,118 | 4'839,285 | 68.05 | 4'769,732 | 98.56 | 69,553 | 1.44 |
| Durango | 1'052,052 | 572,043 | 54.37 | 561,170 | 98.10 | 10,873 | 1.90 |
| Guanajuato | 3'425,081 | 1'961,051 | 57.26 | 1'911,155 | 97.46 | 49,896 | 2.54 |
| Guerrero | 2'135, | 992,131 | 46.47 | 967,95 | 97.56 | 24,17 | 2.44 |

| | | | | | | | |
|------------------|-----------|-----------|-------|-----------|-------|---------|------|
| | 213 | | | 9 | | 2 | |
| Hidalgo | 1'621,727 | 945,590 | 58.31 | 920,954 | 97.39 | 24,636 | 2.61 |
| Jalisco | 4'711,399 | 2'910,366 | 61.77 | 2'848,637 | 97.88 | 61,729 | 2.12 |
| Estado de México | 9'155,396 | 5'701,032 | 62.27 | 5'599,144 | 98.21 | 101,888 | 1.79 |
| Michoacán | 2'952,114 | 1'495,097 | 50.64 | 1'463,252 | 97.87 | 31,845 | 2.13 |
| Morelos | 1'176,598 | 709,101 | 60.27 | 694,039 | 97.88 | 15,062 | 2.12 |
| Nayarit | 673,987 | 365,847 | 54.28 | 358,869 | 98.09 | 6,978 | 1.91 |
| Nuevo León | 2'947,532 | 1'769,218 | 60.02 | 1'730,007 | 97.78 | 39,211 | 2.22 |
| Oaxaca | 2'322,949 | 1'349,183 | 58.08 | 1'307,166 | 96.89 | 42,017 | 3.11 |
| Puebla | 3'436,519 | 1'984,166 | 57.74 | 1'930,552 | 97.30 | 53,614 | 2.70 |
| Querétaro | 1'033,114 | 660,384 | 63.92 | 644,933 | 97.66 | 15,451 | 2.34 |
| Quintana Roo | 675,884 | 385,722 | 57.07 | 378,708 | 98.18 | 7,014 | 1.82 |
| San Luis Potosí | 1'592,136 | 951,724 | 59.78 | 914,392 | 96.08 | 37,332 | 3.92 |
| Sinaloa | 1'732,096 | 980,684 | 56.62 | 961,457 | 98.04 | 19,227 | 1.96 |
| Sonora | 1'669,403 | 934,327 | 55.97 | 917,592 | 98.21 | 16,735 | 1.79 |
| Tabasco | 1'335,454 | 911,113 | 68.22 | 896,993 | 98.45 | 14,120 | 1.55 |
| Tamaulipas | 2'225,129 | 1'225,922 | 55.09 | 1'201,819 | 98.03 | 24,103 | 1.97 |
| Tlaxcala | 704,648 | 410,230 | 58.22 | 401,347 | 97.83 | 8,883 | 2.17 |
| Veracruz | 4'875,677 | 2'942,364 | 60.35 | 2'869,952 | 97.54 | 72,412 | 2.46 |
| Yucatán | 1'178,719 | 789,155 | 66.95 | 773,871 | 98.06 | 15,284 | 1.94 |
| Zacatecas | 994,528 | 525,275 | 52.82 | 512,031 | 97.48 | 13,244 | 2.52 |

* Incluye los votos de los ciudadanos mexicanos residentes en el extranjero.

Fuente: Elaboración propia, a partir del Instituto Federal Electoral.

http://www.ife.org.mx/documentos/OE/participacion2006/reportes/nac_val.html

2.14 Conclusiones.

Es importante tener una visión clara de cómo se encuentra el entorno nacional, para que se conozca de manera clara la meta a la cual se quiere llegar. Tener un comparativo, con los mismos parámetros e indicadores, ofrece una visión de las posibilidades que se tienen para el éxito, o no, de un proyecto como es nuestro caso.

Por otro lado, se debe considerar el tipo de democracias y sistemas políticos, que imperan en las diferentes latitudes donde se han implementados estos proyectos de democracia digital, pues las condiciones que imperan en Venezuela, son muy diferentes a las que tiene Canadá o Japón.

A continuación se enmarca un resumen con los indicadores que se enumeraron páginas arriba, para que sirva de contexto y referencia en los siguientes capítulos Tabla 2.72.

Tabla 2.72. Índice de competitividad global.

| Lugar | Subíndices | | | | | | | | | | | | |
|-------|------------------------|-----------------|-------------|---|-------------------------|--------------------------------|------------|---------|--|-------------------------|------------|--|--|
| | Requerimientos básicos | | | | Potenciador de eficacia | | | | Factores de la innovación. | | | | |
| | | | | | | | | | | | | | |
| Lugar | Pilares | | | | | | | | | | | | |
| | Instituciones | Infraestructura | Estabilidad | Macroeconómica Salud y educación primaria | Y superior | Eficacia del mercado de bienes | de mercado | mercado | Disponibilidad tecnológica del mercado | Sofisticación comercial | Innovación | | |
| | | | | | | | | | | | | | |


| País | Lugares | | | | | | | | | | | | |
|----------------|---------|-----|-----|-----|----|-----|-----|-----|-----|-----|----|-----|-----|
| Estonia | 35 | 34 | | | | 27 | | | | 42 | | | |
| | | 31 | 34 | 47 | 28 | 21 | 28 | 21 | 29 | 16 | 94 | 48 | 37 |
| Japón | 8 | 27 | | | | 11 | | | | 2 | | | |
| | | 28 | 13 | 97 | 19 | 23 | 17 | 12 | 40 | 25 | 3 | 1 | 4 |
| España | 33 | 38 | | | | 29 | | | | 35 | | | |
| | | 49 | 22 | 62 | 38 | 33 | 46 | 97 | 50 | 29 | 13 | 28 | 40 |
| Dinamarca | 5 | 4 | | | | 6 | | | | 7 | | | |
| | | 3 | 12 | 14 | 6 | 2 | 7 | 5 | 8 | 4 | 49 | 8 | 10 |
| Polonia | 46 | 71 | | | | 31 | | | | 46 | | | |
| | | 66 | 103 | 74 | 35 | 27 | 53 | 50 | 44 | 48 | 20 | 44 | 52 |
| Estados Unidos | 2 | 28 | | | | 1 | | | | 1 | | | |
| | | 34 | 8 | 93 | 36 | 7 | 12 | 3 | 20 | 13 | 1 | 5 | 1 |
| Canadá | 9 | 10 | | | | 4 | | | | 12 | | | |
| | | 17 | 7 | 31 | 7 | 9 | 16 | 7 | 11 | 11 | 14 | 17 | 12 |
| Argentina | 85 | 84 | | | | 84 | | | | 76 | | | |
| | | 126 | 88 | 48 | 59 | 55 | 124 | 123 | 116 | 68 | 23 | 73 | 86 |
| Brasil | 56 | 91 | | | | 42 | | | | 38 | | | |
| | | 93 | 74 | 109 | 79 | 58 | 99 | 80 | 51 | 46 | 10 | 32 | 43 |
| Venezuela | 113 | 104 | | | | 108 | | | | 130 | | | |
| | | 133 | 106 | 91 | 81 | 83 | 132 | 133 | 126 | 91 | 37 | 132 | 123 |


| | | | | | | | | | | | | |
|--------|----|----|----|----|----|----|----|---------|----|----|----|----|
| México | 60 | 59 | | | | 55 | | | | | 67 | |
| | | 98 | 69 | 28 | 65 | 74 | 90 | 11 5 | 73 | 71 | 11 | 62 |

Fuente: Elaboración propia, a partir del Reporte de Competitividad Global 2009-2010 (FEM).

Tabla 2.73. Usuarios de Internet 2005-2008.

| País | 2005 | 2006 | 2007 | 2008 | Tasa de crecimiento |
|----------------|------------|-------------|-------------|-------------|---------------------|
| Estonia | 690,000 | 760,000 | 660,000 | 680,000 | -0.36% |
| Japón | 85'290,000 | 87'540,000 | 88'110,000 | 88'500,000 | 0.93% |
| España | 15'119,000 | 18'578,000 | 17'900,000 | 19'810,000 | 6.99% |
| Dinamarca | 2'887,000 | 3'205,200 | 3'240,000 | 3'380,000 | 4.02% |
| Polonia | 10'000,000 | 11'000,000 | 12'940,000 | 14'450,000 | 9.64% |
| Estados Unidos | - | 208'980,600 | 183'620,000 | 190'780,000 | -2.99% |
| Canadá | 22'000,000 | - | 19'200,000 | 20'000,000 | -2.35% |
| Argentina | 6'863,466 | 8'183,700 | 16'000,000 | 20'000,000 | 30.65% |
| Brasil | 36'356,000 | 42'600,000 | 45'000,000 | 50'000,000 | 8.29% |
| Venezuela | 3'313,000 | 4'139,800 | 5'720,000 | 7'170,000 | 21.29% |
| México | 18'622,509 | 22'000,000 | 20'850,000 | 22'340,000 | 4.66% |

 País con mayor tasa de crecimiento.

 País con menor tasa de crecimiento.

Tasa de crecimiento = $\left(\left(\frac{\text{Valor Final}}{\text{Valor Inicial}} \right)^{\frac{1}{N}} - 1 \right) * 100$.


N = Número de períodos (4).


Fuente: Elaboración propia, a partir de UNCTAD. Cálculos basados en los indicadores de la base de datos de Telecomunicación Mundial de la Unión Internacional de Telecomunicaciones (ITU), 2006-2009.

Tabla 2.74. Suscriptores de banda ancha 2005-2008.

| País | 2005 | 2006 | 2007 | 2008 | Tasa de crecimiento |
|----------------|------------|------------|------------|------------|---------------------|
| Estonia | 179,200 | 228,100 | 290,000 | 330,000 | 16.49% |
| Japón | 22'365,148 | 25'755,100 | 28'300,000 | 30'110,000 | 7.72% |
| España | 4'994,274 | 6'654,900 | 8'030,000 | 9'060,000 | 16.06% |
| Dinamarca | 1'356,283 | 1'738,500 | 1'980,000 | 2'030,000 | 10.61% |
| Polonia | 1'243,949 | 2'640,000 | 3'200,000 | 5'010,000 | 41.66% |
| Estados Unidos | 49'391,060 | 58'254,900 | 66'210,000 | 79'070,000 | 12.48% |

| | | | | | |
|-----------|-----------|-----------|-----------|------------|--------|
| Unidos | | | | | |
| Canadá | 6'706,699 | 7'675,500 | 8'680,000 | 9'210,000 | 8.25% |
| Argentina | 841,000 | 1'567,700 | 2'330,000 | 3'010,000 | 37.54% |
| Brasil | 3'304,000 | 5'921,900 | 7'720,000 | 10'020,000 | 31.96% |
| Venezuela | 356,898 | 537,500 | 860,000 | 1'330,000 | 38.94% |
| México | 2'304,520 | 3'728,200 | 4'550,000 | 5'700,000 | 25.41% |

 País con mayor tasa de crecimiento.

 País con menor tasa de crecimiento.


Tasa de crecimiento = $\left(\left(\frac{\text{Valor Final}}{\text{Valor Inicial}}\right)^{\frac{1}{N}} - 1\right) \times 100$.


N = Número de períodos (4).

Fuente: Elaboración propia, a partir de UNCTAD. Cálculos basados en los indicadores de la base de datos de Telecomunicación Mundial de la Unión Internacional de Telecomunicaciones (ITU), 2006-2009.

Tabla 2.75. Suscriptores de telefonía móvil 2005-2008.

| País | 2005 | 2006 | 2007 | 2008 | Tasa de crecimiento |
|----------------|-------------|-------------|-------------|-------------|---------------------|
| Estonia | 1'445,300 | 1'658,700 | 1'610,000 | - | 3.66% |
| Japón | 94'745,000 | 101'698,000 | 100'520,000 | 105'830,000 | 2.8% |
| España | 41'327,911 | 46'152,000 | 48'400,000 | 52'370,000 | 6.1% |
| Dinamarca | 5'511,878 | 5'890,900 | 6'240,000 | 6'590,000 | 4.57% |
| Polonia | 29'260,000 | 36'745,500 | 40'620,000 | 44'030,000 | 10.76% |
| Estados Unidos | 201'650,000 | 236'451,800 | 255'400,000 | 270'330,000 | 7.6% |
| Canadá | 16'600,000 | 17'017,000 | 19'920,000 | 21'460,000 | 6.63% |
| Argentina | 22'100,000 | 311'510,040 | 40'400,000 | 46'510,000 | 20.44% |
| Brasil | 86'210,000 | 99'918,600 | 120'980,000 | 150'640,000 | 14.97% |
| Venezuela | 12'495,721 | 18'789,500 | 23'820,000 | 27'080,000 | 21.33% |
| México | 47'462,108 | 57'016,400 | 68'240,000 | 75'300,000 | 12.23% |

 País con mayor tasa de crecimiento.

 País con menor tasa de crecimiento.

Tasa de crecimiento = $\left(\left(\frac{\text{Valor Final}}{\text{Valor Inicial}}\right)^{\frac{1}{N}} - 1\right) \times 100$.


N = Número de períodos (4).


Fuente: Elaboración propia, a partir de UNCTAD. Cálculos basados en los indicadores de la base de datos de Telecomunicación Mundial de la Unión Internacional de Telecomunicaciones (ITU), 2006-2009.



Tabla 2.76. Índice de desarrollo de las TIC's (IDI) (2002 y 2007).

| País | 2007 | | 2002 | | Tasa de crecimiento |
|----------------|----------|------|----------|------|---------------------|
| | Posición | IDI | Posición | IDI | IDI |
| Estonia | 26 | 5.97 | 31 | 3.93 | 7.22% |
| Japón | 12 | 6.64 | 18 | 4.82 | 5.48% |
| España | 27 | 5.91 | 28 | 4.10 | 6.28% |
| Dinamarca | 3 | 7.22 | 4 | 5.78 | 3.78% |
| Polonia | 39 | 4.95 | 37 | 3.34 | 6.78% |
| Estados Unidos | 17 | 6.44 | 11 | 5.25 | 3.46% |
| Canadá | 19 | 6.34 | 9 | 5.33 | 2.93% |
| Argentina | 47 | 4.12 | 44 | 3.06 | 5.08% |
| Brasil | 60 | 3.48 | 54 | 2.55 | 5.32% |
| Venezuela | 67 | 3.34 | 69 | 2.18 | 7.37% |
| México | 75 | 3.09 | 64 | 2.38 | 4.45% |

 País con mayor tasa de crecimiento.

 País con menor tasa de crecimiento.

Tasa de crecimiento = $\left(\left(\frac{\text{Valor Final}}{\text{Valor Inicial}}\right)^{\frac{1}{N}} - 1\right) * 100$.

N = Número de períodos (6).

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

IDI = *ICT's Development Index*, Índice de Desarrollo de las TIC's.

Tabla 2.77. Proporción de hogares con computadora.

| País | 2007 | 2002 | Tasa de crecimiento |
|----------------|------|------|---------------------|
| Estonia | 57.0 | 21.8 | 17.37% |
| Japón | 85.0 | 71.7 | 2.88% |
| España | 60.4 | 36.1 | 8.96% |
| Dinamarca | 83.0 | 72.2 | 2.35% |
| Polonia | 54.0 | 23.1 | 15.2% |
| Estados Unidos | 70.2 | 59.0 | 2.94% |
| Canadá | 79.1 | 64.0 | 3.59% |
| Argentina | 36.4 | 27.0 | 5.1% |
| Brasil | 20.8 | 14.2 | 6.57% |
| Venezuela | 11.9 | 5.1 | 15.17% |
| México | 22.1 | 15.2 | 6.44% |

■ País con mayor tasa de crecimiento.

■ País con menor tasa de crecimiento.

Tasa de crecimiento = $\left(\left(\frac{\text{Valor Final}}{\text{Valor Inicial}} \right)^{\frac{1}{N}} - 1 \right) * 100$.

N = Número de períodos (6).

Fuente: Elaboración propia, a partir de *ITU. Measuring the Information Society, The Information and Communication Technologies (ICTs) Development Index 2009*.

Capítulo III.- Antecedentes del Instituto Federal Electoral, Alineación del Proceso de Planeación Estratégica y la Tecnología.

A partir de la Independencia de México, los alcaldes, jefes políticos regionales y locales, se encargaban de organizar las elecciones. Al no tener una normatividad que los guiara en dicho proceso, tenían que aplicar, a discreción, su criterio para establecer las reglas bajo las cuales se llevaría a cabo. Lo que no siempre aseguraba la imparcialidad y transparencia mínima requerida.

Tuvieron que pasar los años para que en 1946 se formalizara la estructura electoral, con la fundación de la Comisión Federal de Vigilancia Electoral (COFEVE). Era dirigida por el Secretario de Gobernación, un miembro del gabinete presidencial, un diputado, un senador y dos representantes de los partidos políticos con mayor jerarquía. Simultáneamente se crearon las comisiones electorales locales y el Consejo del Padrón Electoral, lo que dio mayor pluralidad al proceso, pero sin llegar a cumplir plenamente las expectativas de los participantes.

En 1951, la COFEVE fue responsable de coordinar la inscripción de nuevos partidos políticos y al término del proceso electoral, expedir las constancias de mayoría a los ganadores. En 1973 se creó la Comisión Federal Electoral (COFE). Era integrada por todos los partidos políticos registrados, a quienes se les permitía expresar sus opiniones y votar. Durante ese mismo año, el Registro Nacional de Electores (RENAE) alcanzó el estatus de organismo autónomo.

Enseguida, en 1977, se autorizó la Ley de Organizaciones Políticas y Procesos Electorales (LOPPE). Su principal característica era la anuencia para que participaran fuerzas políticas discriminadas, a las que años atrás se les prohibía participar. A través de la LOPPE, se logró modificar la integración de la COFE, permitiendo que los partidos políticos registrados participaran, ya sea de manera condicionada o definitiva, en igualdad de circunstancias. De esta manera, la Comisión quedó integrada por el Secretario de Gobernación, un delegado de

cada una de las cámaras legislativas, un delegado de cada partido político registrado y un notario público.

Más adelante, en 1987, hubo una reforma que ya contemplaba la representación proporcional para formar parte del organismo electoral. Es así como en las elecciones de 1988, la COFE quedó representada por 16 miembros del Partido Revolucionario Institucional (PRI), 15 integrantes tanto del Poder Ejecutivo y Legislativo, como de los restantes partidos políticos.

Debido a las múltiples inconformidades en las elecciones de 1988, recordadas por la famosa “caída del sistema”, fue necesario reformar la Constitución Política de los Estados Unidos Mexicanos al año siguiente. De estos trabajos surgió, en 1990, el Código Federal de Instituciones y Procedimientos Electorales (COFIPE). El cual hizo posible la creación del Instituto Federal Electoral (IFE), el 11 de octubre de 1990, durante la primera sesión del Consejo General.

Este órgano nació para responder a las demandas sociales, que exigían un organismo electoral imparcial que ofreciera; credibilidad, transparencia y legitimidad a los partidos políticos involucrados en la contienda. Eso, como primera condición hacia la democracia de México. Desde su creación, el IFE se ha esmerado por ganarse la credibilidad de los ciudadanos, procurando que los comicios estén alejados de la ilegitimidad, la duda, inseguridad y sospechas.

Con el paso del tiempo, esta institución ha ido ganando adeptos, que confían en su desempeño para organizar procesos electorales; federales, estatales y municipales. Al final del evento se encargan de contabilizar los votos y dar a conocer los resultados. Cabe resaltar también la participación de los partidos políticos, que contribuyen vigilando, antes, durante y después de la contienda, si se presenta algún hecho relevante que pudiera ocasionar la anulación de la actividad. Por otro lado, también es relevante la colaboración activa de los ciudadanos que asisten a las urnas para votar. También los que tienen la responsabilidad de fungir como

observadores electorales durante la recepción y conteo de votos, para asegurar que prevalezca la neutralidad y justicia.

3.1 Estructura.

La estructura organizacional del IFE se divide en cuatro niveles jerárquicos:

Órganos centrales:

- Consejo General.
- Presidencia del Consejo General.
- Junta General Ejecutiva.
- Secretaría Ejecutiva.
- Unidad de Fiscalización de los Recursos de los Partidos Políticos.
- Contraloría General.

Direcciones Ejecutivas:

- Dirección Ejecutiva del Registro Federal de Electores.
- Dirección Ejecutiva de Prerrogativas y Partidos Políticos.
- Dirección Ejecutiva de Organización Electoral.
- Dirección Ejecutiva de Servicio Profesional Electoral.
- Dirección Ejecutiva de Capacitación Electoral y Educación Cívica.
- Dirección Ejecutiva de Administración.

Unidades Técnicas:

- Coordinación de Asuntos Internacionales.
- Dirección del Secretariado.
- Dirección Jurídica.
- Centro para el Desarrollo Democrático.
- Unidad de Servicios de Informática.

- Coordinación Nacional de Comunicación Social.
- Unidad Técnica de Servicios de Información y Documentación.

Organismos Desconcentrados:

- Juntas Locales y Distritales.

3.2 Consejo General.

Conforme a lo establecido en el artículo 110 del Código Federal de Instituciones y Procedimientos Electorales (COFIPE), el Consejo General estará integrado de la siguiente manera:

- Consejero Presidente.
- Secretario Ejecutivo.
- Consejeros Electorales Propietarios.
- Consejeros del Poder Legislativo (Propietarios y Suplentes).
- Representantes de los partidos políticos (Propietarios y Suplentes).

3.3 Proceso Electoral.

De acuerdo con el IFE (2007), el Proceso Electoral Federal en México se concibe como:

El conjunto ordenado y secuencial de actos y actividades, regulados por la Constitución y la Ley Electoral que realizan las autoridades, los partidos políticos y los ciudadanos, con el propósito de renovar periódicamente a los integrantes de los poderes Legislativo y Ejecutivo de la Unión.

Sobre esta base, la división del proceso electoral en etapas, no sólo tiene como propósito distinguir y diferenciar claramente la secuencia temporal de los diversos actos o actividades que lo integran, sino además y fundamentalmente, asegurar que se cumpla con el principio de definitividad. Es decir, otorgar firmeza y certidumbre jurídica a la realización y conclusión de las distintas actividades. Así como garantizar que cada acto, realizado por las autoridades electorales, los partidos políticos y los ciudadanos, se ajuste a los términos y plazos previstos legalmente.

3.4 Actividades previas.

El Proceso Electoral Federal Ordinario abarca cuatro etapas secuenciales (IFE, 2007):

- **Preparación de la elección.** Da inicio con la primera sesión organizada por el Consejo General del IFE, la primera semana de octubre del año, previo al que habrán de realizarse las elecciones federales ordinarias y concluye cuando se inicia la jornada electoral.
- **Jornada electoral.** Comienza a las 08:00 horas del primer domingo de julio y termina cuando se clausuran las casillas (mesas para votar), instaladas para recibir y computar los votos.
- **Resultados y declaraciones de validez de las elecciones.** Se inicia con el envío de documentación y expedientes electorales de casillas, de las elecciones de diputados y senadores, a los consejos distritales. Finaliza con los cómputos y declaraciones de validez que hagan los consejos del IFE, o las resoluciones emitidas por el Tribunal Electoral del Poder Judicial de la Federación. De acuerdo con la ley, esta etapa debe finalizar en la última semana de agosto.
- **Dictamen y declaración de validez de la elección y de presidente electo.** Esta etapa empieza cuando se resuelve el último medio de impugnación que se haya interpuesto contra la elección o cuando exista constancia de que no se presentó ninguno. Concluye cuando la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación

aprueba el dictamen, que contiene el cómputo final y las declaraciones de validez de la elección y del presidente electo. Conforme a la ley, esta etapa debe concluir en el mes de septiembre.

3.5 Instalación y apertura de casillas.

Inicia a las 08:00 horas del día en que habrá elecciones, cuando los cuatro miembros propietarios de cada mesa directiva instalan la casilla, en presencia de los representantes de los partidos políticos que contendrán. No se permite instalar una casilla antes de las 08:00 horas, ni que se retiren los funcionarios de la mesa directiva antes de haberla clausurado.

Si por alguna razón no se llegara a instalar una casilla, conforme al procedimiento ordinario, la legislación electoral contempla diferentes alternativas secuenciales. Lo anterior, hasta lograr que los representantes de partidos políticos, en ausencia de los funcionarios de casilla, designados con anterioridad o de personal del IFE, designen por mayoría a los funcionarios que integrarán la mesa directiva de casilla. Evento a realizar sólo entre los electores de la sección electoral presentes para votar. De lo contrario, los nombramientos se harán entre los representantes de los partidos políticos.

Una casilla puede instalarse en un lugar diferente al designado por el órgano electoral competente. La votación será válida solamente si existe una razón justificada para instalarla en otro sitio, distinto al acordado por el correspondiente consejo distrital. En caso de que la mesa directiva necesite cambiar de lugar la instalación de la casilla, la nueva ubicación debe hacerse en la misma sección y en el lugar adecuado más próximo, dejando un aviso del cambio, en el exterior del sitio original. Si no se procede de esta manera, la votación de esa casilla se anulará.

3.6 Votación.

Después de que se llena y firma el apartado correspondiente, a la instalación de la casilla, en el acta de la jornada electoral, da inicio la votación a través del anuncio emitido por el presidente de la mesa directiva de casilla.

Los electores podrán realizar su voto conforme vayan llegando a las casillas. Para lo cual deben mostrar, obligatoriamente, su credencial para votar con fotografía. En seguida, se debe comprobar en las listas nominales que aparezca el elector. El presidente procede a entregar las boletas de las elecciones, para que libremente y en secreto, marque el área correspondiente al partido político de su preferencia.

Si la persona que va a votar no sabe leer, o tiene algún impedimento físico para marcar las boletas electorales, puede recibir el apoyo de una persona de su confianza.

A continuación, el elector deposita sus boletas en la urna correspondiente, según la elección de que se trate. Luego, el secretario de la casilla anota la palabra “votó”, en la lista nominal. Perfora la credencial para votar e impregna el dedo pulgar derecho del elector con tinta indeleble. En ese momento concluye el procedimiento de votación para cada ciudadano.

3.7 Escrutinio.

Al cierre de la votación, los integrantes de la mesa directiva deben hacer el escrutinio y cómputo de los votos efectuados en la casilla. El escrutinio (IFE, 2006) “consiste en la revisión y clasificación puntual del total de las boletas electorales, recibidas originalmente por cada mesa de casilla. El cómputo implica el conteo de la votación emitida”. Al término de ambos procesos, los integrantes de cada una de las mesas directivas de casilla deberán informar acerca de:

- La cantidad de personas que votaron en la casilla.
- La cantidad de votos emitidos a favor de cada uno de los partidos políticos o candidatos.
- La cantidad de votos anulados por los integrantes de la mesa directiva. Un voto se considera nulo cuando fue emitido y depositado en la urna por un elector y éste no marcó sólo el círculo, o cuadro, donde aparece el escudo de un partido político o coalición.
- La cantidad de boletas sobrantes de cada elección.

Por último, después de que la mesa directiva integró debidamente los expedientes, el presidente de la mesa deberá colocar avisos con los resultados de cada una de ellas, en sitios visibles, afuera de los locales a donde acudieron los votantes. Dichos resultados pueden ser firmados por los representantes de los partidos políticos que así lo deseen.

3.8 Cierre de casillas.

Para finalizar con la jornada electoral, los funcionarios de la mesa directiva deben clausurar la casilla. Levantarán un acta donde se mencione; la hora en que ocurrió, así como los nombres de los funcionarios y representantes que entregarán el paquete que contiene el expediente de casilla, ante el consejo distrital correspondiente. Este documento deberá ser firmado por los funcionarios de casilla y los representantes de los partidos políticos que así lo decidan.

Después de haberse cerrado las casillas, su presidente es responsable de entregar los paquetes y expedientes al consejo distrital correspondiente, en los plazos perentorios que contempla la ley, de acuerdo con la hora en que la casilla cerró y su ubicación geográfica. Hay tres plazos que la ley contempla para la entrega de los paquetes electorales:

- **Inmediato**, cuando se trata de casillas instaladas en las cabeceras de los distritos uninominales.

- **Hasta 12 horas**, cuando se trata de casillas urbanas ubicadas fuera de las cabeceras del distrito electoral.
- **Hasta 24 horas**, si se trata de casillas localizadas en zonas rurales.

Para las actas de escrutinio y cómputo de los sufragios emitidos en el extranjero, la ley contempla que la Junta General Ejecutiva del IFE entregará una copia al comité distrital correspondiente, a través de los medios más adecuados, antes del miércoles siguiente al día en que hubo elecciones.

3.9 Credencial para votar.

La credencial para votar es la identificación oficial que permite a los ciudadanos mexicanos, mayores de 18 años, ejercer su derecho al voto. Incluye diferentes características y elementos de seguridad, que sirven para verificar su autenticidad.

3.9.1 Parte frontal.

La parte frontal tiene las siguientes características y elementos de seguridad:

1. Al exponer la credencial, ante una lámpara de luz negra, deberán apreciarse varios escudos nacionales, como se muestra en la Figura 3.1.



Figura 3.1. Apreciación de los escudos nacionales.

Fuente: http://www.ife.org.mx/documentos/DERFE/RFE2/cred/CredencialVotar_anverso.swf

2. Los cuatro números de la sección deben corresponder con los primeros cuatro números del OCR, que está en el reverso, como se observa en la Figura 3.2.



Figura 3.2. Los cuatro números de la sección.

Fuente: http://www.ife.org.mx/documentos/DERFE/RFE2/cred/CredencialVotar_anverso.swf

3. Incluye una imagen de seguridad con el logotipo del IFE, que cubre parcialmente la parte inferior izquierda de la fotografía, como se aprecia en la Figura 3.3.



Figura 3.3. Imagen de seguridad con el logotipo del IFE.

Fuente: http://www.ife.org.mx/documentos/DERFE/RFE2/cred/CredencialVotar_anverso.swf

4. La fotografía tiene dos tramas de seguridad, como se expone en la Figura 3.4:
 - Las siglas del IFE aparecen cuando se expone a una lámpara de luz negra.
 - Se observa una trama ondulada de color amarillo, que se aprecia a simple vista.



Figura 3.4. Fotografía con las dos tramas de seguridad.

Fuente: http://www.ife.org.mx/documentos/DERFE/RFE2/cred/CredencialVotar_anverso.swf

- Incluye una fotografía digital impresa, que debe corresponder con el titular, como lo muestra la Figura 3.5.



Figura 3.5. Fotografía digital impresa.

Fuente: http://www.ife.org.mx/documentos/DERFE/RFE2/cred/CredencialVotar_anverso.swf

- Tiene una impresión de micro línea en el contorno de la fotografía, con el nombre completo y la fecha en que se realizó el trámite, como lo presenta la Figura 3.6.



Figura 3.6. Micro línea que aparece en el contorno de la fotografía.

Fuente: http://www.ife.org.mx/documentos/DERFE/RFE2/cred/CredencialVotar_anverso.swf

- El nombre del titular debe aparecer cuando se expone la credencial ante una lámpara de luz negra, como se aprecia en la Figura 3.7.



Figura 3.7. Nombre del titular que aparece al exponer la credencial en una lámpara de luz negra.

Fuente: http://www.ife.org.mx/documentos/DERFE/RFE2/cred/CredencialVotar_anverso.swf

3.9.2 Parte posterior.

La parte posterior incluye las siguientes características y elementos de seguridad:

1. Los cuatro primeros números, que aparecen en el reverso, deben corresponder con los cuatro dígitos de la “sección”. Los ocho restantes forman el OCR, como se observa en la Figura 3.8.



Figura 3.8. Números que sirven para verificar si la credencial es genuina.

Fuente: <http://www.ife.org.mx/documentos/DERFE/RFE2/cred/trasera.swf>

2. El rectángulo donde aparece la firma del titular lleva una impresión de micro línea, con su nombre completo, como se expone en la Figura 3.9.



Figura 3.9. Impresión micro línea, con el nombre del titular de la credencial.

Fuente: <http://www.ife.org.mx/documentos/DERFE/RFE2/cred/trasera.swf>

3. La sección para marcar cuando el votante participa, en las elecciones federales y locales, tiene un espesor compatible con la norma internacional (0.76 milímetros más delgada, flexible), como se muestra en la Figura 3.10.



Figura 3.10. Secciones para marcar la participación del votante, en elecciones federales y locales.

Fuente: <http://www.ife.org.mx/documentos/DERFE/RFE2/cred/trasera.swf>

3.10 Instituto Electoral del Estado de Colima.

Para la creación de leyes, organismos electorales y demás autoridades electorales, se debe tener en claro que la autoridad con esta facultad es el Gobernador y el Congreso del Estado de Colima, de acuerdo con la Constitución del Estado.

De acuerdo a la XX Legislatura del Estado de Colima (2011), se indica:

- Título I,
 - Capítulo I de los derechos del hombre
 - VIII. Por el carácter plural de la sociedad colimense, las autoridades están obligadas a fortalecerla, alentando la participación democrática de individuos, organizaciones y partidos políticos en el desarrollo del Estado.

- Título III,
 - Capítulo III facultades del Congreso. Artículo 33.- Son facultades del Congreso:
 - II--Reformar esta Constitución, previos los requisitos que ella misma establece. Legislar sobre todos los ramos de la administración o gobierno interiores que sean de la competencia del Estado, conforme a la Constitución Federal. Así como también; reformar, abrogar y derogar las leyes que expidiere;
 - VI. Expedir leyes sobre planeación del desarrollo económico o social del Estado;
 - IX. Expedir leyes electorales conforme a la presente Constitución, así como los Estatutos Laborales del Instituto y Tribunal (sic) Electorales.
 - Capítulo V De la Iniciativa y Formación de las Leyes, el Artículo 37.- El derecho de iniciar Leyes corresponde:
 - (REFORMADA, P. O. 11 DE DICIEMBRE DE 1999) I A los Diputados.

- (REFORMADA, P. O. 11 DE DICIEMBRE DE 1999) II. Al Gobernador.
 - (REFORMADA, P. O. 11 DE DICIEMBRE DE 1999) III. Al Supremo Tribunal de Justicia en asuntos del Ramo de Justicia.
 - XXXIX. Organizar y conducir la planeación democrática del desarrollo del Estado. Establecer los medios para la participación ciudadana y la consulta popular;
- Título IV. (REFORMADA SU DENOMINACIÓN, P.O. 26 DE MARZO DE 1994)
 - Capítulo I. Artículo 58.- Son facultades y obligaciones del Ejecutivo:
 - I En el orden Federal, las que determine la Constitución y las leyes federales. (REFORMADA, P.O. 23 DE ENERO DE 1954)
 - II. Promulgar, ejecutar y hacer que se ejecuten las Leyes y Decretos haciendo uso en su caso, de todas las facultades que le concede esta Constitución.
 - III Formar los reglamentos y dictar las providencias que demande la mejor ejecución de las leyes.
 - XXXIX. Organizar y conducir la planeación democrática del desarrollo del Estado y establecer los medios para la participación ciudadana y la consulta popular.

Así mismo, el órgano encargado de organizar las elecciones, en el Estado de Colima, es el Instituto Electoral del Estado de Colima, de acuerdo con la XX Legislatura del Estado de Colima (2011).

- TÍTULO VI (ADICIÓN Y REFORMA DENOMINACIÓN, P.O. 26/ MARZO/1994)
 - CAPÍTULO ÚNICO De los Partidos Políticos y Organismos Electorales
 - III La organización de las elecciones locales es una función estatal que se realiza a través de un organismo público, de carácter permanente, denominado Instituto Electoral del Estado. Dotado de personalidad

jurídica y patrimonio propio, en cuya integración participan; el Poder Legislativo del Estado, los partidos políticos y los ciudadanos, en los términos que ordene la ley. En el ejercicio de esta función estatal, la certeza, legalidad, independencia, imparcialidad y objetividad, serán principios rectores.

El Instituto Electoral del Estado será autoridad en la materia, profesional en su desempeño, autónomo e independiente en sus decisiones y funcionamiento. Contará en su estructura con órganos de dirección, ejecutivos, técnicos, y se organizará de acuerdo con las siguientes bases:

a) El Consejo General será su órgano superior de dirección y se integrará por siete Consejeros Electorales propietarios. Designados por el Congreso del Estado, por mayoría calificada de sus integrantes, a propuesta de los grupos parlamentarios. Previa convocatoria pública, mediante la realización de una amplia consulta a la sociedad y con la aplicación de una evaluación a los aspirantes. Durarán en su encargo siete años, sus requisitos y mecanismos de elección serán determinados en la ley de la materia. Uno de los Consejeros será Presidente, electo por un mínimo de cinco votos de los Consejeros. Tendrá un Secretario Ejecutivo, que deberá ser también Consejero y será electo por cinco votos de los Consejeros, a propuesta en terna de su Presidente.

Ambos funcionarios durarán en su cargo 4 años, pudiendo ser reelectos para completar el resto del período. Los Consejeros Electorales estarán sujetos al régimen de responsabilidades, establecido en el Título XI de esta Constitución.

Por otro lado, la participación de los partidos políticos y ciudadanos, mayores de 18 años con credencial para votar vigente en las elecciones locales, está regulada por la normatividad del Código Electoral del Estado de Colima.

Por lo anterior, el Instituto Electoral del Estado de Colima (IEEC), es un “organismo público autónomo, de carácter permanente, con personalidad jurídica y patrimonio propio. Depositario de la autoridad electoral y responsable del ejercicio de la función estatal de organizar las elecciones”. Este proceso lo realiza con la participación de los partidos políticos y la sociedad, conforme a lo estipulado en el Código Electoral del Estado de Colima.

3.10.1 Fines.

El IEEC tiene como fines:

- Preservar y fortalecer, promover y fomentar el desarrollo de la democracia en la entidad.
- Preservar y fortalecer el régimen de partidos políticos.
- Garantizar a los ciudadanos el ejercicio de los derechos políticos-electorales y vigilar el cumplimiento de sus obligaciones.
- Organizar y vigilar la realización periódica y pacífica de las elecciones, para renovar al titular del poder Ejecutivo, a los integrantes del poder Legislativo y de los Ayuntamientos.
- Velar por la autenticidad y efectividad del sufragio.
- Coadyuvar en la promoción y difusión de la cultura cívica, política democrática.

3.10.2 Consejo General.

El Consejo General del IEEC está integrado de la siguiente forma, como lo muestra el organigrama de la Figura 3.11 y que se describe a continuación:

- Consejero Presidente. Lic. Mario Hernández Briceño.
- Secretario Ejecutivo y Consejero General. Lic. José Luis Puente Anguiano.
- Consejero Electoral. Lic. Daniel Fierros Pérez.
- Consejero Electoral. Lic. Federico Sinué Ramírez Vargas.
- Consejera Electoral. Licda. María de los Ángeles Tintos Magaña.
- Consejera Electoral. Licda. Ana Francis Santana Verduzco.
- Consejera Electoral. Licda. Rosa Esther Valenzuela Verduzco.

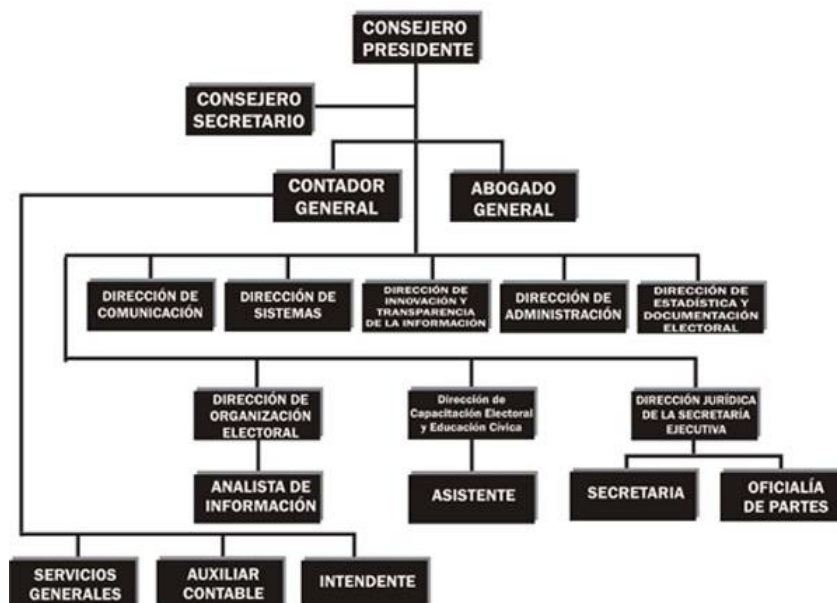


Figura 3.11. Órganos Ejecutivos del IEEC.

Fuente: IEEC, 2009.

3.10.3 Consejos Municipales Electorales.

Los Consejos Municipales Electorales están conformados como se señala en la Tabla 3.1:

Tabla 3.1 Consejos Municipales Electorales del Estado de Colima.

| Municipio | Distrito | Secciones Electorales | Domicilio | Integrantes |
|------------------|--|---|--|---|
| Armería | Noveno | 0170-0190 | Sonora No. 70 Colonia Centro Teléfono: 3133221158 | Profr. Elías García García. Presidente. Lic. José Filemón Ruelas Morales. Secretario. Lic. Miguel Ángel Espíritu Macías. Consejero. Profr. Genaro Palomera Ramírez. Consejero. Profr. Druso Alfonso Escalante Petra. Consejero. C.P. Briceida Arceo Rodríguez. Suplente. C.P. Rosa Elva Valdovinos Reyes. Suplente. Angelina Núñez Manzo. Aux. Admvo. |
| Colima | Primer (Nor-Este) • Urbano • Rural Segundo (Colima Centro). • Urbano Tercer (Colima | 0001-0013, 0015, 0016, 0018-0024, 0034-0037 077 El Chanal (cabecera), 0078 La Capacha (cabecera), 0079 El Diezmo (cabecera), 0080 Colonia El Porvenir, 0082 Colonia La Estancia Nor-Este (cabecera) y localidad de Cardona 0014, 0017, 0025- 0033, 0038-0041, 0043-0048, 0052, | Constitución No. 191 C.P. 28000 Colonia Centro Teléfono: 3123149312 | C.P. Eliseo Corona Gómez. Presidente. Lic. Gerardo Alva Rodríguez. Secretario. Licda. Adela Cortez Ramírez. Consejera. Mtra. Angélica Yedit Prado Rebolledo. Consejera. Lic. José Manuel López Araujo. Consejero. Mtra. Rosalva Covarrubias Gómez. Suplente. Licda. Verónica Valdez Adaya. Suplente. Suplente. Carmen Karina Aguilar Orozco. Aux. |

| | | | | |
|--------|--|--|--|--|
| | <p>Sur).</p> <ul style="list-style-type: none"> • Urbano • Rural | <p>0054, 0055, 0058, 0063 y 0064</p> <p>0042, 0049-0051, 0053, 0056, 0057, 0059, 0060-0062, 0065-0076</p> <p>0081 Lo de Villa, 0083 Colonia Juana de Asbaje (cabecera), 0084 Piscila (cabecera), 0085 Astillero de Abajo (cabecera), 0086 Los Asmoles (cabecera), 0087 Los Ortices (cabecera), 0088 Los Tepames (Norte), 0089 Los Tepames (Sur), 0090 Tinajas (cabecera) y 0091 Estapilla (cabecera)</p> | | Admvo. |
| Comala | Cuarto | 0092-0104 | <p>Guillermo Prieto No. 94</p> <p>Teléfono: 3123156587</p> | <p>Lic. Víctor Aviña Solís. Presidente.</p> <p>Profr. Rubén Jaime Valencia Salazar. Secretario Ejecutivo.</p> <p>Licda. Marlene Valencia Madrigal. Consejero.</p> <p>Profr. Armando Montes Amezcua. Consejero.</p> <p>Lic. Juan Maximino Ramírez. Consejero.</p> <p>Licda. Gladia Fabiola Mendoza Quintero. Suplente.</p> <p>Profr. Mario González. Suplente.</p> <p>Claudia Liliana López</p> |

| | | | | |
|-----------------|--------|-----------|--|--|
| | | | | Ramírez. Aux. Admvo. |
| Coquima tlán | Quinto | 0105-0119 | Reforma, esquina con Victoria 3123230114 | Licda. María Esperanza Toscano Cerna. Presidente. Profra. Carmen Silvia Brizuela Benavides. Secretario. Profr. Sergio Cobián Hernández. Consejero. C.P. Ramón Preciado Brizuela. Consejero. Profr. Rafael Pérez George. Consejero. Lic. Sergio Anaín Dueñas Manzo. Suplente. Licda. Ana María Alcalá Ceja. Suplente. Rosalba Flores Rosales. Aux. Admvo. |
| Cuauhté moc | Sexto | 0120-0137 | 16 de Septiembre No. 10, esquina Venustiano Carranza Teléfono: 3123280888 | Profr. Raúl Leonel Aguirre Campos. Presidente. Licda. Delma Alejandra Alcaraz Díaz. Secretario. T.S. Ma. Leticia Torres Ahumada. Consejero. Profr. Nicolás Chávez Armenta. Consejero. Profr. Gustavo Silva Cobián. Consejero. Profr. José Juan Campos Preciado. Suplente. LAE. Dámaso Valencia Cruz. Suplente. Rafaela Álvarez Torres. Aux. Admvo. |
| Ixtlahua cán | Décimo | 0191-0199 | Nicolás Bravo No. 10 | Lic. Antonio Partida Haro. Presidente. |

| | | | | |
|------------|-------------------------------------|--|---|--|
| | Décimo Tercer (Centro). • Urbano | las Garzas (cabecera), 0253-0256 Las Brisas (cabecera), 0257-0258 Tapeixtles (cabecera), 0259-0263 El Colomo (cabecera), 0264 Las Juntas de Abajo (cabecera), 0265 San Buenaventura (cabecera), 0266-0267 Venustiano Carranza (cabecera), 0268-0269 Campos (cabecera). 0200-0216, 0218, 0220-0221 | | |
| Minatitlán | Décimo Cuarto | 0270-0276 | 27 de Octubre No. 16 C.P. 28750 Teléfono: 3143360251 | Profr. Rafael Barajas Pizano. Presidente. Lic. Ramón Pascacio Arciniega Pedraza. Secretario. Profra. María Hilda Murguía Castañeda. Consejero. Profra. María de los Ángeles Figueroa Arias. Consejero. Profr. Gabriel Quezada Franco. Consejero. Licda. Elva Yadira Figueroa Michel. Suplente. C.P. Clemente Mendoza Martínez. Suplente. Alma Edith Rodríguez Barragán. Aux. Admvo. |
| Tecomá | Décimo | | Mercurio y | Lic. J. Jesús Guillén |

| | | | | |
|------------------|--|--|---|---|
| n | <p>Quinto (Norte).</p> <ul style="list-style-type: none"> • Urbano • Rural <p>Décimo Sexto (Sur-Este).</p> <ul style="list-style-type: none"> • Urbano • Rural | <p>0277-0295, 0298-0299</p> <p>0317-0319 Madrid (cabecera), 0320 Tecolapa (cabecera), 0321 Caleras (cabecera), 0325 Poblado La Estación (cabecera), 0326 Colonia María Esther Zuno de Echeverría (cabecera), 0327 Cofradía de Hidalgo (cabecera).</p> <p>0296-0297, 0300-0316</p> <p>0322 Adolfo Ruiz Cortínez (cabecera), 0323 Colonia Antonio Salazar Salazar (cabecera), 0324 Colonia Bayardo (cabecera), 0328 Colonia L. Moreno (cabecera), 0329 Cofradía de Morelos (cabecera), 0330 El Saucito, 0331 Chanchopa, 0332 San Miguel del ojo de Agua (cabecera), 0333 Callejones, 0334-0336 Cerro de Ortega (cabecera).</p> | <p>Ejército Nacional (a un lado de la unidad deportiva). Teléfono: 3133252666</p> | <p>Cruz. Presidente. Profr. Javier Mesina Escamilla. Secretario. C.P. Miguel García Ávila. Consejero. Mtra. Adelina del Carmen García Morales. Consejero. Licda. Artemisa González Guerrero. Consejero. Licda. Ada Carina Cuevas Palacios. Suplente. Lic. Sergio Arturo Skokanic Briceño. Suplente. Celia Candelaria Reyes Velázquez. Aux. Admvo.</p> |
| Villa de Álvarez | <p>Séptimo (Nor-Este).</p> <ul style="list-style-type: none"> • Urbano | <p>0138-0145, 0147-</p> | <p>Morelos No. 74 Zona Centro</p> | <p>Lic. Héctor René Cabezud. Presidente. Lic. José Llerenas</p> |

| | | | | |
|--|--|--|---------------------------------|--|
| | <ul style="list-style-type: none"> • Rural <p>Octavo (Sur-Este)</p> <ul style="list-style-type: none"> • Urbano • Rural | <p>0151, 0158-0159</p> <p>0166 El Nuevo Naranjal (cabecera) y 0169 El Chivato (cabecera)</p> <p>0146, 0152-0157, 0160-0165</p> <p>0167 Pueblo Nuevo (cabecera) y 0168 Juluapan (cabecera).</p> | <p>Teléfono: 3123114343</p> | <p>Macías. Secretario. Licda. Alma Cecilia Meza Romero. Consejero. M.C. Arturo González Larios. Consejero. Licda. Sandra Elizabeth Campos Gómez. Consejero. Lic. Alejandro Javier Rodríguez Ramírez. Suplente. Ing. Víctor Hugo Chávez Ventura. Suplente. Josefina Vargas Contreras. Aux. Admvo.</p> |
|--|--|--|---------------------------------|--|

Fuente: IEEC, 2009.

3.11 Seguridad del voto electrónico.

3.11.1 Planeación de la Seguridad Informática.

Una de las reflexiones que se deben tener, al momento de establecer un modelo de seguridad para realizar transacciones empresariales, gubernamentales o de cualquier otra índole, es el organigrama corporativo o institucional. De tal suerte que se pueda ubicar perfectamente quiénes son los responsables de una área específica y sus funciones en particular. Con lo anterior, la entidad tendrá un rumbo claramente definido, teniendo sus repercusiones al corto, mediano y largo plazo.

La planeación estratégica, junto a la dirección de tecnología de la organización, es de vital importancia para que las entidades tengan rumbo. Después de realizar su planeación corporativa, deben bajarlo a las divisiones o departamentos más pequeños, para tener una definición más clara del impacto en particular, que habrá de tener esa área menor de la entidad o corporación, como se muestra en la Figura 3.12.



Figura 3.12. Planeación Top-Down para la Seguridad de la Información.

Fuente: Withman y Mattord. Administración de la Seguridad de la Información (p.44).

Por otro lado, se requiere una Planeación Estratégica, para poder determinar y establecer los riesgos de la operación de la Institución indicada, como se determina en el estandar ISO 17799-2005 (ISO, 2007).

Es esencial que una organización identifique sus requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad. Una fuente se deriva al evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos. Se evalúa la vulnerabilidad, la probabilidad de ocurrencia y se calcula el impacto potencial.

De acuerdo con Withman y Mattord (2010): “Para ejecutar esta amplia estrategia y transformar las declaraciones en acciones, el equipo ejecutivo debe, primero, definir sus responsabilidades en lo individual”.

Este aspecto debe ser cubierto desde las altas esferas de la organización, donde se están ejecutando las estrategias. Lo anterior se indica en la Figura 3.13.

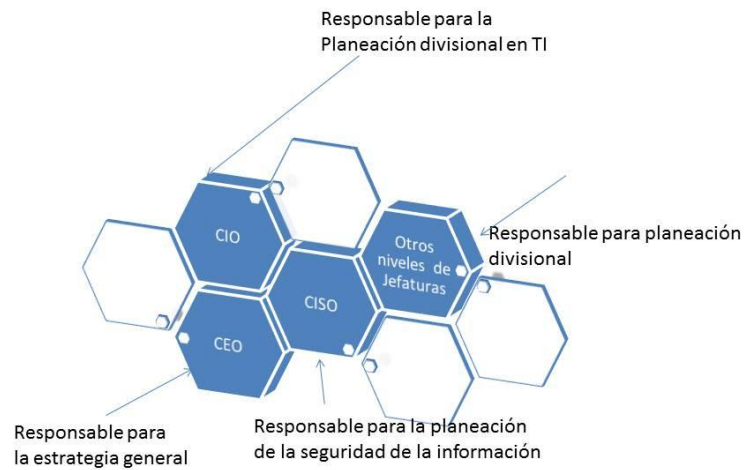


Figura 3.13. Planeación de la Organización.

Fuente: Withman y Mattord. Administración de la Seguridad de la Información (p.44).

3.11.2 Niveles del Plan Operacional.

Una vez que el plan estratégico es trasladado en metas estratégicas, para cada división o departamento, siendo una de estas divisiones el grupo de Seguridad de Información Electrónica, el siguiente paso a dar es trasladar estas estrategias en tareas específicas que sean medibles, alcanzables y delimitadas por objetivos en un tiempo específico.

Hecho lo anterior, se ponen en marcha los planes tácticos, los cuales tienen una duración más corta que el plan estratégico, por lo regular de uno a tres años.

Enseguida se tienen los planes operacionales, los cuales se derivan de los planes tácticos, para organizar el comportamiento y el desempeño diario de las tareas. Un ejemplo de la separación de los niveles de planeación, se presenta en la Figura 3.14.

Administradores y empleados usan el plan operacional, el cual se deriva de los planes tácticos, para organizar el curso y el desempeño diario de las tareas. El plan operacional debe incluir la identificación plena, la coordinación de actividades, a través de los límites departamentales, requerimientos de comunicación, reuniones semanales, resúmenes, reportes de avances y tareas asociadas.



Figura 3.14. Niveles de Planeación.

Fuente: Withman y Mattord. Administración de la Seguridad de la Información (p. 45).

Como lo mencionan Withman y Mattord (2010): “La primera prioridad del Oficial Jefe de Seguridad de la Información (Chief Information Security Officer, CISO) y el administrador de la seguridad, debe ser la estructura de un plan estratégico”.

Mientras que cada organización puede tener su propio formato para el diseño y distribución de un plan estratégico, los elementos básicos de la planeación son los mismos. Como lo afirman Withman y Mattord (2010).

Dichos elementos son:

- Introducción por el Presidente de la Junta o CEO
- Resumen ejecutivo.
- Declaración de la misión y visión.

- Perfil organizacional e historia.
- Cuestiones estratégicas y valores centrales.
- Metas programadas y objetivos.
- Administración/Metas operacionales y objetivos.
- Apéndices (opcional; análisis de fortalezas, debilidades, oportunidades y amenazas, FODA, encuestas, presupuestos, etc.)

3.11.3 Planeación Previa de los Sistemas de Seguridad.

Para la empresa, la planeación previa de los esquemas de seguridad es muy importante, ya que se deben visualizar todos los escenarios posibles. Desde la seguridad interna, políticas de acceso y control, hasta una posible intrusión externa, o en extremo, un hackeo completo del sistema. Todo lo anterior es un escenario mínimo, si se considera el mal uso que se puede hacer a los datos que son extraídos o manipulados por los intrusos.

Los altos ejecutivos de la empresa juegan un rol muy importante, para trasladar la planeación estratégica en un plan táctico y operacional de la seguridad de la información. En este caso el CIO y el CISO.

En el caso particular del CISO, su rol toma una peculiar importancia, ya que él tiene sobre sus hombros la seguridad empresarial. La descripción del trabajo, para el Administrador del Departamento de Seguridad de Información, partiendo de los roles de seguridad y su responsabilidad, lo mencionan Withman y Mattord (2010):

- Deben crear una estrategia de seguridad de la información, con una visión al futuro de la Seguridad de la Información de la Empresa.
- Comprender las actividades fundamentales desarrolladas por la empresa, y con base en ello, sugerir el portafolio de soluciones apropiados para proteger las actividades.

- Desarrollar el plan de acción, calendario, presupuestos, estado de reportes, y algunas otras comunicaciones de alta dirección, destinadas a mejorar el estatus de la seguridad de la información de la empresa.

Una vez que el plan estratégico de la empresa ha sido trasladado, dentro de las Tecnologías de la Información y los objetivos del departamento de seguridad de información por el CIO, entonces es traducido a los planes tácticos y operativos por el CISO. Sólo entonces, la aplicación de seguridad de la información puede comenzar. La aplicación de seguridad de la información se puede lograr de dos maneras: de abajo hacia arriba o de arriba hacia abajo, como se muestra en la Figura 3.15.

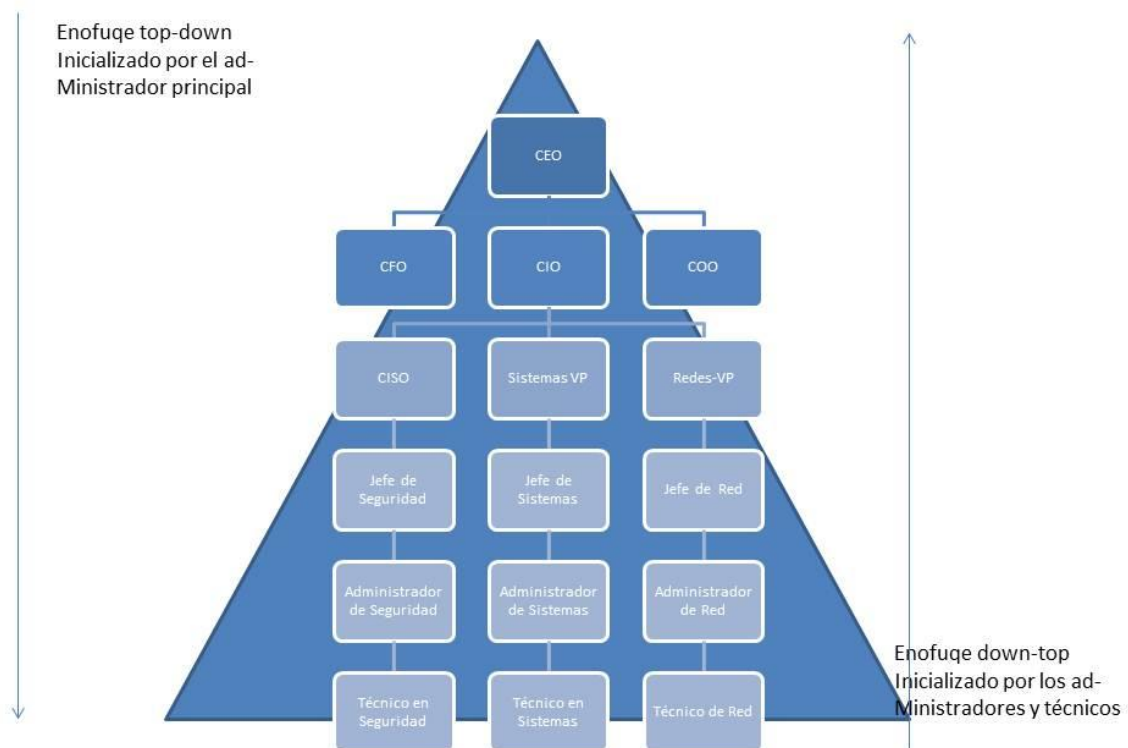


Figura 3.15. Enfoques para la Implementación de la Seguridad.

Fuente: Withman y Mattord. Administración de la Seguridad de la Información (p. 54).

3.11.4 Ciclo de Vida al Desarrollo de Sistemas.

El ciclo de vida de desarrollo de sistemas, en general, es una metodología para el diseño y la puesta en práctica de un sistema de información. En una institución es ampliamente utilizada en TI por las organizaciones, de acuerdo con Senn (2002). En la Figura 3.16 se muestra la relación entre los sistemas de información y los niveles de una organización.



Figura 3.16. Relación entre los sistemas de información y los niveles de una organización.

Fuente: Senn. Introducción al Desarrollo de Sistemas de Información (p. 26).

Una metodología es un acercamiento formal para resolver problemas, basados en una secuencia estructurada de procedimientos. Usando una metodología, asegura un riguroso proceso e incrementa la probabilidad de alcanzar el objetivo final deseado.

De acuerdo con Senn (2002), para iniciar un proyecto basado en esta metodología, puede ser manejado por eventos. Comenzado, en respuesta a un cierto acontecimiento, en la comunidad empresarial, dentro de la organización, o dentro de las filas de los empleados, de clientes u otros interesados o afectados en el proyecto. Otra opción podría ser un plan conducido, que es resultado de una estrategia de planificación cuidadosamente desarrollada.

Al final de cada fase, se realiza una revisión a la estructura. Se confronta con los resultados esperados. Durante esta revisión, el equipo de desarrollo determina si el proyecto debe continuar, posponerse o definitivamente pararlo. De manera alternativa se puede endosar su desarrollo a empresas externas, como se muestra en la Figura 3.17.

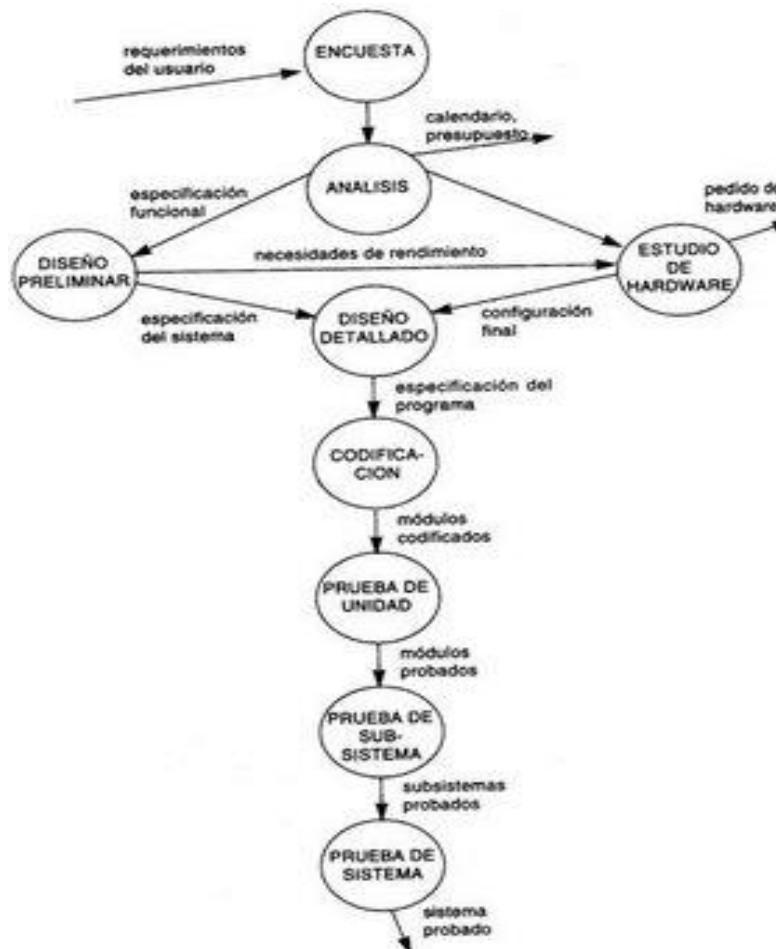


Figura 3.17. Actividades del Ciclo de Vida Clásico de Desarrollo de Sistemas.

Fuente: Con apoyo del libro Senn. Introducción al Desarrollo de Sistemas de Información (p.

Así pues, las fases son las siguientes.

- **Investigación Preliminar.** Esta fase identifica el problema que se intenta resolver, a través del sistema que se desarrolla. Comenzando con una evaluación del evento, o plan inicial de los procesos, donde los objetivos, limitantes y ámbito del proyecto, son especificados.
- **Un análisis costo/beneficio** es desarrollado para evaluar los beneficios percibidos y la apropiación de esos beneficios que se persiguen.
- **Determinación de los Requerimientos del Sistema.** Esta fase de análisis comienza con la información que se aprende durante la fase de investigación. En esta fase se evalúa la disposición de la organización, el estado de los sistemas actuales, más su capacidad para aplicar y apoyar los sistemas propuestos.
El análisis determina lo que se espera realicen los nuevos sistemas y cómo se desempeñen, a la par de cómo han de interactuar con los sistemas actuales.
- **Diseño del Sistema.** En el diseño lógico, la información obtenida durante la fase de análisis es usada para crear una solución, basada en el sistema para el problema que se desea resolver.
- **Por último**, sobre la base de todo lo anterior, el equipo selecciona los **tipos específicos de los controles técnicos**, que pueden resultar útiles cuando se implementa como una solución física.
- **El diseño lógico** es la implementación independiente del proyecto, para la solución deseada.
- **Diseño físico o de software.** Durante el diseño físico, el equipo selecciona la tecnología para soportar las alternativas identificadas y la evaluación del diseño lógico.
- **La selección de los componentes es evaluado** más para hacer la evaluación de compra. Entonces un diseño final es seleccionado para integrar los diferentes requerimientos y tecnologías.

- **Implementación.** En la fase de implementación, los ingenieros de software desarrollan cualquier programa que no se compra y toman las decisiones de integración para los módulos. Lo anterior, como esquema, es customizado, evaluado y documentado.

Todos y cada uno de los componentes se han de evaluar en lo individual e instalarse.

- **Mantenimiento.** Esta fase consiste en las actividades necesarias para dar soporte, modificar y añadir funcionalidad al sistema, para el resto de la vida útil.

En el caso muy particular del desarrollo de software, se puede tomar en cuenta el siguiente diagrama, que se observa en la Figura 3.18, el cual detalla las fases del ciclo de vida de software. Caben resaltar cuatro funciones básicas que deben ser manejadas:

- **Requisitos=** Se debe tener en cuenta qué debe hacer el software.
- **Diseño=** En esta segunda fase se considera el modelo de la arquitectura, las interfaces y las funciones del sistema.
- **Implementación=** El sistema en si mismo es montado o se deja ejecutándose.
- **Prueba=** y por último, su evaluación y desempeño.

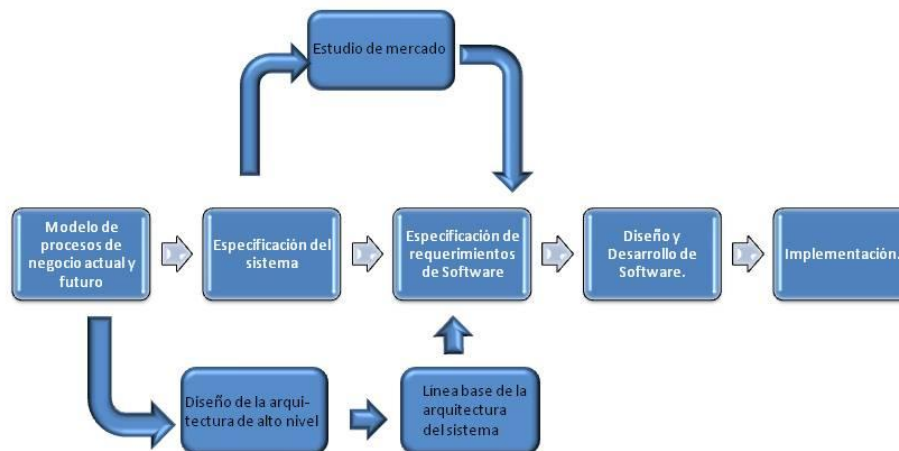


Figura 3.18. Ciclo de vida de Software.

Fuente: <http://www.swri.org/4org/d10/ised/fulllife.htm>

Contando con el modelo arriba señalado, se puede planificar de manera ordenada y coordinada, teniendo como apoyo los siguientes modelos conceptuales:

- Cascada
- Espiral.
- Iterativo
- Prototipo.

3.11.5 El Ciclo de Vida del desarrollo de los Sistemas de Seguridad (SecSDLC).

El Ciclo de Vida del Desarrollo de los Sistemas de Seguridad, puede ser diferente en algunas actividades en específico, pero básicamente cubre la misma metodología.

El proceso de SecSDLC implica la identificación de las amenazas específicas y los riesgos que representan. También el diseño, más la puesta en prácticas subsecuentes de controles específicos, para contrarrestar esas amenazas y para asistir a la administración del riesgo.

Investigación en el SecSDLC.

La fase de la investigación del SecSDLC comienza con una directiva de la alta gerencia, que especifica el proceso, los resultados, las metas del proyecto, así como su presupuesto y otras limitantes.

Frecuentemente, esta fase inicia con la afirmación o creación de políticas de seguridad, en las cuales el programa de seguridad de la organización es, o en su defecto, será fundada.

El equipo de administradores, empleados y contratistas se reúnen para analizar problemas. Definen su ámbito, metas y objetivos específicos. Identifican cualquier limitante adicional, no cubierta en las políticas de seguridad empresarial.

Finalmente, un análisis de viabilidad de organización determina si la organización tiene los recursos, incluyendo la comisión para conducir un análisis y un diseño acertados de seguridad.

Este modelo se expone en la Figura 3.19.



Figura 3.19. Ciclo de Vida del Desarrollo de los Sistemas de Seguridad.

Fuente: <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

Análisis en el SecSDLC.

El equipo de desarrollo, creado durante la fase de la investigación, conduce a un análisis preliminar de políticas de seguridad, o de programas existentes, junto con amenazas actuales documentadas y controles asociados.

Esta fase también incluye un análisis de las cuestiones legales relevantes, que podrían afectar al diseño de la solución de la seguridad. La tarea de la gestión de riesgos también comienza en esta etapa:

a) Gestión de riesgos.

La gestión de riesgos es el proceso para; identificar, determinar, y evaluar los niveles de riesgo que hacen frente a la organización. Específicamente las amenazas a la seguridad de la organización, a la información almacenada y procesada por la organización.

Para entender mejor la fase de análisis del SecSDLC, debemos saber algo sobre las clases de amenazas, que hacen frente a organizaciones en el mundo de la tecnología de la información. En este contexto, una amenaza es el objeto, la persona, o la otra entidad que representa un peligro constante a un activo, como se señala en la Tabla 3.2.

Tabla 3.2. Amenazas a la seguridad de la información.

| Categorías de las amenazas | Ejemplos |
|---|---|
| Actos de errores humanos o fallas | Accidentes de empleados, errores. |
| Compromisos con la propiedad intelectual | Piratería, infracciones a los derechos de autor. |
| Actos deliberados de espionaje o violación | Acceso no autorizado y recolección de datos |
| Actos deliberados de extorsión de información. | Chantaje de divulgación de información. |
| Actos deliberados de sabotaje y vandalismo | Dstrucción de sistemas de información |
| Actos deliberados de robo. | Confiscación ilegal de equipo o información. |
| Ataques deliberados de software | Virus, gusanos, macros, denegación de servicio. |
| Las desviaciones en la calidad de servicio de los proveedores de servicio. | Problemas de potencia y de servicios WAN. |
| Fuerzas de la naturaleza | Fuego, terremotos, tormentas electromagnéticas. |
| Fallas técnicas de Hw | Falla de equipo. |
| Fallas técnicas de Sw | Bugs, problemas de código, fallas desconocidas. |
| Problemas técnicos de obsolescencia | Tecnología vieja o fuera de tiempo. |

Fuente: Withman y Mattord. Administración de la Seguridad de la Información (p. 57).

Un ataque es un acto deliberado que aprovecha una vulnerabilidad. Esto se logra por un agente que la amenaza, daña o roba información de una organización, o de activos físicos.

Un exploit es una técnica o mecanismo, utilizado para comprometer un sistema y así establecer o buscar una vulnerabilidad, la cual es identificada de un sistema controlado, en el que los controles necesarios no están presentes o ya no son eficaces.

Así mismo, un ataque es el uso de un exploit para lograr comprometer un sistema controlado.

Los ataques más comunes son:

- El código malicioso.
- Bromas.
- Puertas traseras.
- Craqueo de Contraseña.
- Ataque de fuerza bruta.
- Ataque a Diccionario.
- Negación de servicio (DoS) y la negación distribuida de servicio (DDoS).
- Spoofing.
- Man-in-the-middle
- Spam.
- Bombardeo de Correo.
- Sniffer.
- Ingeniería social.
- Desbordamiento de búfer
- Timing.

El último paso en el conocimiento del enemigo, es encontrar algún método para priorizar el riesgo planteado por cada categoría de amenaza y sus correspondientes métodos de ataque. Esto puede hacerse mediante la adopción de los niveles de peligro de un estudio de las amenazas existentes, o creando su propia clasificación de las amenazas para su entorno, basado en análisis de escenarios.

b) Identificación y evaluación de las vulnerabilidades.

Este proceso iterativo debe incluir una clasificación y categorización de todos los elementos de los sistemas de una organización; las personas, los procedimientos de datos y la información, software, hardware y elementos de red. El próximo reto en la fase de análisis consiste en revisar cada uno de los activos de información, para cada amenaza que se enfrenta y crear una lista de las vulnerabilidades, como se ilustra en la Figura 3.20.

En la fase de análisis se continúa el proceso. La siguiente tarea es evaluar el riesgo relativo de cada uno de los activos de información.

Esto lo lograremos mediante un proceso llamado evaluación de riesgos o análisis de riesgos. La evaluación de riesgos asigna una calificación de riesgos comparativos, o puntaje, a cada activo de información específica. Concretamente, aquí se pueden adaptar herramientas como el Balanced Score Card.

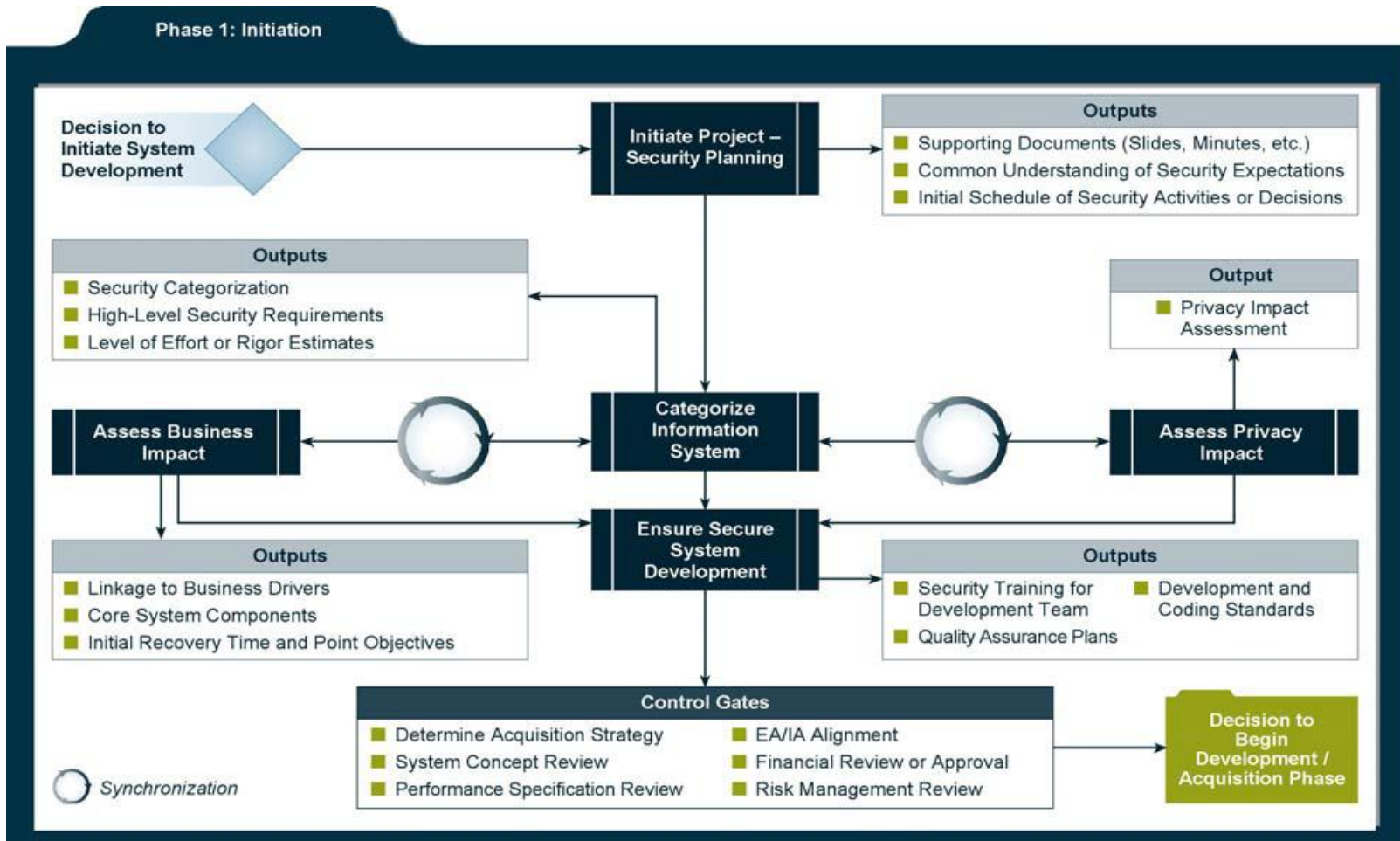


Figura 3.20. Fase de Iniciación del SecSDLC.

Fuente: <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

La gestión de riesgos es la parte, en la fase de análisis, que identifica las vulnerabilidades en los sistemas de información de una organización. Toma cuidadosamente medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de todos los componentes, en el sistema de información de la organización.

Diseño en el SecSDLC.

La fase de diseño se compone de dos partes distintas; el diseño lógico y diseño físico.

En la fase de diseño lógico, los miembros del equipo crean y desarrollan el plan de seguridad. Examinan y aplican políticas clave, que influyen en las decisiones posteriores. En la fase de diseño físico, los miembros del equipo de evaluación seleccionan la tecnología necesaria, para apoyar el plan de seguridad, generar soluciones alternativas y acordar el diseño final.

Entre las fases de diseño lógico y físico, un administrador de seguridad puede tratar de utilizar los modelos de seguridad, establecidos para guiar el proceso de diseño. Los modelos de seguridad proporcionan marcos para garantizar que todas las áreas de la seguridad sean incluidas. Las organizaciones pueden adaptar, o adoptar, un marco para satisfacer sus propias necesidades de seguridad de la información.

Uno de los elementos de diseño del programa de seguridad de la información, es la política de seguridad de la información de la organización.

El administrador debe definir tres tipos de políticas de seguridad:

1. General o política del programa de seguridad.
2. Tema específico de las políticas de seguridad y
3. Sistemas específicos de las políticas de seguridad.

Otra parte integral del programa de seguridad de información, que se debe considerar para ser diseñado, es el programa de la educación de la seguridad y formación (SETA). Como mencionan Withman y Mattord (2010): “Es responsabilidad del CISO, el programa SETA, que es una medida de control diseñado para reducir las violaciones accidentales por los empleados”. Como se describe en la Tabla 3.1, en el ranking de errores se encuentra el ocasionado por el personal, por lo que el programa SETA se compone de tres elementos; la educación sobre seguridad, formación en seguridad y la conciencia de seguridad. El propósito de SETA es mejorar la seguridad en las siguientes áreas, como lo mencionan Withman y Mattord (2010):

1. Mejorar la conciencia de la necesidad de proteger los recursos del sistema.
2. Desarrollar habilidades y conocimientos para usuarios de computadoras, que puedan desarrollar su trabajo más seguro.
3. La construcción del conocimiento en profundidad, según sea necesario, para diseñar, implementar, operar programas de seguridad para las organizaciones y sistemas.

En la fase de diseño continuo, la atención se enfoca en el diseño de los controles y salvaguardias, para proteger la información de los ataques de amenazas. Hay tres categorías de controles, de acuerdo con los documentos del Temple University (2009):

- Controles de gestión de dirección en el diseño e implementación del proceso de planificación de la seguridad y la gestión de los programas de seguridad. La gestión de los controles también se ocupa de la gestión de riesgos y revisiones de controles de seguridad.
- Controles operativos que cubran las funciones de gestión y planificación de menor nivel, como; la recuperación de desastres y la planificación de respuesta a incidentes. Controles operacionales también se ocupan de la seguridad personal, seguridad física, más la protección de los insumos y productos.

- Controles técnicos que aborden esas cuestiones tácticas y técnicas, relacionadas con el diseño y la implementación de la seguridad en la organización. Aquí, las tecnologías necesarias para proteger la información, son examinados y seleccionados.

Otro elemento en la fase de diseño es la creación de los documentos esenciales de la preparación:

- Planeación de la contingencia. Es la planeación completa, conducida por la organización, para prepararse y reaccionar en caso de eventos que amenacen la seguridad de la información, así como los activos de información en la organización. Incluye la posterior restauración de las operaciones comerciales normales.
- Planeación de las respuestas a los incidentes (IRP). Es el proceso asociado con la identificación, clasificación, respuesta y recuperación desde un incidente.
- Planeación de la recuperación de desastres (DRP). Es el proceso de planeación asociado con la preparación y recuperación, desde que ocurrió un desastre, sin importar que sea natural o artificial.
- La planificación de la continuidad del negocio (BCP). Es el proceso de planificación asociados con la garantía de que las funciones críticas del negocio, continúen, si un incidente catastrófico o desastre se presentan.

3.11.6 Elementos que integran una Urna Electrónica Segura.

El impacto que tienen las TIC's en todas las áreas de la dinámica social, en general, es muy alto. Sabemos que desde un modesto celular, hasta el más sofisticado sistema electrónico, empotrado en el automóvil, ha llegado a formar parte del entorno y necesidades del ser humano. Los bancos, las universidades, los supermercados, el gobierno, el hogar... en fin, todas las aristas del ser humano, tienen en su entorno diario una referencia electrónica. La cual es difícil imaginarse, no tenerla al alcance, sin que llegue a perturbar la economía y la toma de

decisiones en todos los niveles. Del mismo modo que las TIC's afectan el quehacer diario de todas las entidades y las personas, así mismo se ve afectado en los elementos para integrar un sistema sofisticado de urna electrónica. Los elementos, tanto en software como en hardware, que se integren a la urna, deben ser evaluados y llevados a los estándares internacionales en; operación, seguridad, ergonomía, compatibilidad, estabilidad, entre otros. Con lo anterior se tiene que, dependiendo del tipo de diseño, se usa una determinada tecnología. Por consecuencia, el uso y las propiedades que ofrece la urna. Así mismo, se pueden agregar gadgets muy específicos para el servicio y confort, tanto de los electores como de quienes llevan a cabo la administración del sistema. A continuación se enumeran los sistemas de voto electrónico, en la Tabla 3.3.

Tabla 3.3. Resumen de los sistemas voto electrónico.

| IMPLEMENTO | DEFINICIÓN | DESCRIPCIÓN | FUNCIONES GENERALES |
|--------------------|---|--|--|
| Urnas electrónicas | Dispositivo electrónico que permite el registro y escrutinio de los votos emitidos. Así como la transmisión de los resultados del cómputo de la elección en la casilla. | <ul style="list-style-type: none"> • Carcasa metálica. • Cuenta con un teclado numérico en la parte frontal, con aplicaciones Brille. • Pantalla monocromática de 9.4”. • Controlador de luminosidad. • Microterminal con teclado y lector magnético. • Tarjeta de memoria externa. • Procesador interno. • Impresora térmica. • Capacidad para trabajar con corriente alterna y/o corriente directa. • Batería de respaldo. • Procesador de datos. • Memoria interna de | <ul style="list-style-type: none"> • Registra el voto. • Contabiliza el voto. • Guarda la información. • Transmite los resultados. |

| | | | |
|------------------------------------|---|--|--|
| | | respaldo. <ul style="list-style-type: none"> • Módem para la transmisión de datos vía telefónica. | |
| Pantalla sensitiva (Touch screen). | Dispositivo digital que permite el registro y escrutinio de los votos emitidos. Así como la transmisión de los resultados del cómputo de la elección en la casilla, a través de la utilización de un teclado sensitivo que está contenido en la pantalla del monitor. | <ul style="list-style-type: none"> • Carcasa plástica. • Pantalla digital sensible al tacto. • Tarjeta de memoria extraíble. • Tarjeta de memoria interna. • Procesador interno. • Impresora interna. • Batería de respaldo. • Lector magnético e infrarrojo. • Módem interno para la transmisión de datos vía telefónica o microondas. • Aplicaciones braille en los costados de la pantalla. • Instrucciones en audio para personas con debilidad visual. | <ul style="list-style-type: none"> • Registra el voto. • Contabiliza el voto. • Guarda la información. • Transmite los resultados. |
| Contador de votos (Scanner). | Dispositivo electrónico que permite el conteo y escrutinio de votos, a través de un lector óptico. | <ul style="list-style-type: none"> • Carcasa plástica o metálica. • Lector óptico. • Depósito de boletas (urna). • Teclado de operación remoto. • Impresora. • Procesador interno | <ul style="list-style-type: none"> • Contabiliza el voto. • Transmite los resultados. |
| Voto por teléfono | Sistema informático que opera a través de los aparatos telefónicos que permite el registro y escrutinio de los votos emitidos. | <ul style="list-style-type: none"> • Sistema informático residente en un servidor. • Funciona a través de la red telefónica. • Se opera a través de marcación por tonos. | <ul style="list-style-type: none"> • Registra el voto. • Guarda la información para posteriormente emitir los resultados. |

| | | | |
|--|--|--|--|
| | Así como la emisión de los resultados del cómputo de una elección. | | |
|--|--|--|--|

| | | | |
|-------------------|--|---|---|
| Voto por Internet | Sistema informático que opera a través de un procesador personal, conectado a Internet, que permite el registro y escrutinio de los votos emitidos. Así como la emisión de los resultados del cómputo de una elección. | <ul style="list-style-type: none"> • Sistema informático residente en un servidor. • Funciona a través del Internet. • Requiere de un procesador personal. | <ul style="list-style-type: none"> • Registra el voto. • Contabiliza el voto. • Guarda la información. • Presenta los resultados. |
|-------------------|--|---|---|

Fuente: <http://www.iedf.org.mx/de/deoyge/EstudioComparativo2008.pdf>.

Software requerido para la Urna Electrónica. El software que puede ser usado es variado. Desde los programas de corte comercial, hasta los de tipo software libre. En el mercado se encuentran diferentes tipos de licencia, a las cuales se pueden acudir dependiendo de las necesidades que se tengan. Mencionamos las siguientes, como se enlista en la página informática HOY (2010).

Software Libre o Free Software: es un software disponible para cualquiera que desee utilizarlo, copiarlo y distribuirlo, ya sea en su forma original o con modificaciones. La posibilidad de modificaciones implica que el código fuente está disponible. Si un programa es libre, puede ser potencialmente incluido en un sistema operativo, también de corte libre. Es importante no confundir software libre con software gratis, porque la libertad asociada al software libre, de copiar, modificar y redistribuir, no significa gratuidad. Existen programas gratuitos que no pueden ser modificados ni redistribuidos. Ejemplos;

Copyleft: es donde la mayoría de las licencias usadas, en la publicación de software libre, se permite que los programas sean modificados y redistribuidos. Estas prácticas están generalmente prohibidas por la legislación internacional de copyright, que intenta impedir que alteraciones y copias sean efectuadas sin la autorización del o los autores. Las licencias que acompañan al software libre, hacen uso de la legislación de copyright, para impedir la utilización no autorizada. Pero estas licencias definen, clara y explícitamente, las condiciones bajo las cuales pueden realizarse copias, modificaciones y redistribuciones. Esto, con el fin de garantizar las libertades de modificar y redistribuir el software registrado. A esta versión de copyright, se le da el nombre de copyleft.

GPL: la Licencia Pública General GNU (GNU General Public License GPL) es la licencia que acompaña los paquetes distribuidos por el Proyecto GNU, más una gran variedad de software que incluye el núcleo del sistema operativo Linux. La formulación de GPL es tal, que en vez de limitar la distribución del software que protege, llega hasta impedir que este software sea integrado en software propietario. La GPL se basa en la legislación internacional de copyright, lo que debe garantizar cobertura legal para el software licenciado con GPL.

Debian: la licencia Debian es parte del contrato realizado entre Debian y la comunidad de usuarios de software libre. Se denomina Debian Free Software Guidelines (DFSG). En esencia, esta licencia contiene criterios para la distribución que incluyen, además de la exigencia de publicación del código fuente; (a) la redistribución libre, (b) el código fuente debe ser incluido y debe poder ser redistribuido, (c) todo trabajo derivado debe poder ser redistribuido bajo la misma licencia del original, (d) puede haber restricciones en cuanto a la redistribución del código fuente, si el original fue modificado, (e) la licencia no puede discriminar a ninguna persona o grupo de personas, así como tampoco ninguna forma de utilización del software, (f) los derechos otorgados no dependen del sitio en el que el software se encuentra, y (g) la licencia no puede 'contaminar' a otro software.

Open Source: la licencia de Open Source Initiative, deriva de Debian.

BSD: la licencia BSD cubre las distribuciones de software de Berkeley Software Distribution, además de otros programas. Es una licencia considerada 'permisiva', ya que impone pocas restricciones sobre la forma de uso, alteraciones y redistribución del software. El software puede ser vendido y no hay obligaciones de incluir el código fuente. Esta licencia garantiza el crédito a los autores del software, pero no intenta garantizar que las modificaciones futuras permanezcan siendo software libre.

X.org: el Consorcio X distribuye X Window System, bajo una licencia que lo hace software libre, aunque sin adherirse al copyleft. Existen distribuciones bajo la licencia de X.org que son software libre, con otras distribuciones que no lo son. Hay algunas versiones no-libres del sistema de ventanas X11, para estaciones de trabajo y ciertos dispositivos de IBM-PC, que son las únicas funciones disponibles, sin otros similares que sean distribuidos como software libre.

Software con Dominio Público: el Software con dominio público es software sin copyright. Algunos tipos de copia o versiones modificadas pueden no ser libres, si el autor impone restricciones adicionales en la redistribución del original o de trabajos derivados.

Software Semi-libre: el Software semi-libre es un software que no es libre, pero permite que otros individuos lo usen, lo copien, lo distribuyan y hasta lo modifiquen. Ejemplos de software semi-libre son las primeras versiones de Internet Explorer, de Microsoft, o algunas versiones de browsers de Netscape, y Star Office.

Freeware: el término freeware no posee una definición ampliamente aceptada, pero es utilizada para programas que permiten la redistribución, pero no la modificación, y que incluyen su código fuente. Estos programas no son software libre.

Shareware: Shareware es el software disponible con el permiso para que sea redistribuido, pero su utilización implica el pago. Generalmente, el código fuente no se encuentra disponible, y por lo tanto es imposible realizar modificaciones.

Software Propietario: el Software propietario es aquel cuya copia, redistribución o modificación están, en alguna medida, prohibidos por su propietario. Para usar, copiar o redistribuir, se debe solicitar permiso al propietario, o pagar.

Software Comercial: el Software comercial es el software desarrollado por una empresa, con el objetivo de lucrar con su utilización. Nótese que "comercial" y "propietario" no son lo mismo. La mayor parte del software comercial es propietario, pero existe software libre que es comercial, y existe software no-libre que no es comercial.

Por lo anterior, en el mercado existen plataformas de urnas electrónicas desarrolladas en diferentes tipos de licencias, lo cual arroja características diferentes de desempeño y costo.

Manejadores de Base de Datos: los manejadores de base de datos son los programas que administran la información. Entre sus características encontramos las siguientes:

- Control de redundancia
- Control de usuarios
- Seguridad de acceso a datos
- Multiusuario.
- Integridad de información.
- Soporte para control de transacciones y transacciones fallidas.

En la Tabla 3.4 se muestra el tipo de manejador de base de datos disponible y el tipo de licencia de que dispone.

Tabla 3.4. Manejadores de Base de Datos.

| Manejador | Tipo de Licencia. |
|---|-------------------|
| Mysql, msql. | Libre |
| Sybase, Oracle, MSSQL Server, Informix, DB2 | Comercial |

Fuente: Sitios Web de los programas mencionados.

Lenguaje de programación base: los lenguajes de programación son una parte importante para el desarrollo de las aplicaciones. En el caso de la urna electrónica no es menos su importancia de elección, a lo cual se muestra una lista compacta de los lenguajes que se pueden usar y su principal orientación por tipo de licencia. A continuación, en la Tabla 3.5, encontrará una breve lista de los lenguajes de programación actuales:

Tabla 3.5. Lenguajes de Programación.

| Lenguaje | Principal área de aplicación | Tipo |
|---------------------|--|-----------------|
| Visual Basic NET | Uso general para aplicaciones locales y web | Comercial. |
| C, C++ | Programación de sistema | Libre/Comercial |
| Java | Programación de sistema orientado a objetos | Libre/Comercial |
| PHP | Programación orientada a Internet, desarrollo de sitios web dinámicos. | Libre |
| Perl | Procesamiento de cadenas de caracteres | Libre |

Fuente: Páginas web de los lenguajes citados.

Sistema operativo: los Sistemas Operativos (SO), al igual que los programas mencionados anteriormente, tienen un tipo de licenciamiento muy particular. Aunado a lo anterior, poseen características muy particulares que permiten, a un SO, tener ventaja competitiva de uno sobre otro, dependiendo del uso que se le vaya a dar. En la Tabla 3.6 se muestra un resumen de los tipos de SO y sus principales características.

Tabla 3.6. Tipos de SO y características.

| Sistema Operativo | Tipo de Licencia | Características |
|-------------------|---------------------------------|--|
| Windows | Comercial | <ul style="list-style-type: none"> • Son muy estables y amigables. • Su interfaz gráfica es buena. • Conexión de red especial. • Su navegador no es tan rápido como firefox, pero es seguro (IE 7 y 8). • La mayoría de los programas que se crean son para Windows. • Es uno de los más atacados por los creadores de virus, de 10 computadoras 9 lo usan. • Firewall muy aceptable. • La mayoría de los fabricantes de PC basan su drivers para Windows. • Soporte multitarea. |
| Linux | Licencia Pública General (GPL). | <ul style="list-style-type: none"> • Libre de virus. • Multiusuario. • Multiproceso. • Multiplataforma • Gran administrador de memoria y de recursos en general. • Gran estabilidad. • Sus actualizaciones tienen menos frecuencia, a comparación con Windows. • Compatibilidad con otros SO. • Interfaz de usuario amable. • Gran soporte en internet. • Ha tomado gran parte del mercado y en la actualidad existe mucho soporte por profesionales de la informática. |
| SUN | Sun Community Source. | <ul style="list-style-type: none"> • Libre de Virus. • Multiusuario. • Multiproceso • Multiplataforma. • Gran administrador de memoria y de recursos en general. • Gran estabilidad. • Sus actualizaciones tienen menos |

| | | |
|--------|-----------|---|
| | | <p>frecuencia a comparación con Windows.</p> <ul style="list-style-type: none"> • Compatibilidad con otros SO. • Interfaz de usuario amable. • Gran soporte en internet. El soporte lo integra ORACLE, empresa de mucho prestigio. • Proporciona una gran seguridad por los sistemas cerrados que posee. |
| NOVELL | Comercial | <ul style="list-style-type: none"> • Soporte de la empresa NOVELL y su prestigio de servicio. • NOVELL íntegro en su núcleo de servicio a Linux, lo cual hereda sus propiedades. |
| Mac OS | Comercial | <ul style="list-style-type: none"> • Los pioneros en la interfaz gráfica de usuario. • Gran prestigio en la actualidad. • No existen virus en este SO. • Gran estabilidad. • Costoso. • Existe poco software para él, aunque existen compatibilidades con software abierto. • Poco soporte regional. |

Fuente: Sitios Web de los SO.

Con lo expuesto anteriormente y de acuerdo a los alcances del proyecto, la presente implementación tendrá el uso de software libre, en plataformas de hardware basadas en Intel.

3.11.7 Entorno de seguridad.

Una de las reflexiones preliminares que se deben tener presentes, es la seguridad física de las instalaciones y los protocolos referentes a la seguridad del entorno lógico de desarrollo.

El control que se debe tener en las instalaciones debe ser, si no paranóico, sí muy alto, para que sólo el personal que requiera estar en sitio acceda a él, con un alto control de acceso.

Por otro lado; las reglas, control y plantillas de usuarios, grupos y staff que acceden al servidor, red y servicios que se proporcionan, debe estar perfectamente planeado para

minimizar el efecto de accesos no deseados. Como lo refiere Instituto Nacional de Estándares y Tecnología (*NIST* 1995), tanto dentro como fuera del perímetro lógico de seguridad. El control de las bitácoras, seguimiento y revisión, es otro tema que debe ser cubierto, por demás, en forma exhaustiva.

Así mismo, los servicios deben ser controlados; por su tipo, acceso remoto, protocolo de acceso, tipo de encriptación, etcétera. Siguiendo estándares que ya se han implementado y seguido, quizá el error humano es, con mucho, el culpable de intromisiones que, al tiempo, tiene que ver con pérdidas que terminan siendo costosas.

Con lo antes señalado, se debe considerar que existen tres elementos clave en todo entorno de seguridad:

- 1) Personas.
- 2) Equipo.
- 3) Procesos.

A continuación se expone más en los temas arriba introducidos.

Seguridad del sitio.

La seguridad del sitio, donde se instalan los servidores, equipo de comunicación, servidores de base de datos, desde el propio acceso, debe ser restringido, por dos razones. La primera es por seguridad misma del sitio. La segunda es porque en ocasiones se tiene instalado equipo que pudiera representar peligro para quienes acceden y se quieren evitar accidentes, como ejemplo: algún equipo de transmisión que maneje láseres o alto voltaje.

Entre lo que se debe considerar, se tiene:

- a. Control de acceso físico a las instalaciones.

El control efectivo de acceso físico a las instalaciones debe ser la máxima preocupación, ya que si tienen acceso a los equipos y con conocimientos avanzados de informática, prácticamente la información está al desnudo. La mayoría de las organizaciones utilizan uno de los tres mecanismos, que a continuación se enumeran para implementar la seguridad física (en orden creciente de seguridad):

- Bloqueo y acceso de teclado, Lock-and-key Access (ver Figura 3.21).

Es el control de seguridad física más común en las organizaciones pequeñas. El acceso funciona como en los hoteles. Se le proporciona un acceso que es habilitado para ingresar a un determinado cuarto. Entre las ventajas que tiene es que no requiere experiencia técnica para su manejo.

Uno de los inconvenientes que presenta es que los trabajadores podrían “perder” la llave y quedar expuestos a “accidentes” que resultarían costosos. Además que fácilmente se pueden hacer duplicados, si se tiene acceso al hardware. A menos que, junto con un sistema de alarma que aumenta la seguridad del acceso a la cerradura y llave, no hay ningún mecanismo para determinar cuando los empleados, con acceso a las claves de una ubicación física determinada, acceden o no a ellas.

La autenticación de clave es de un solo factor.



Figura 3.21. Control de acceso por teclado.

Fuente : Mathias Lock and Key, 2011.

- Clave de acceso con tarjeta (ver Figura 3.22).

En la mayoría de las organizaciones grandes, este tipo de control puede ayudar con algunos problemas de administración, asociado con el primer esquema de seguridad y puede incrementar las medidas de seguridad. El acceso con tarjetas puede ser por bandas magnéticas, o por tarjetas inteligentes. Como todos los sistemas, tiene sus pros y contras que pueden ser eliminados con el uso de tecnología complementaria. A continuación, algunos beneficios de este sistema.

- I. Acceso a múltiples lugares que pueden ser controlados por una solo tarjeta.
- II. Si un empleado deja la compañía, la tarjeta del empleado puede ser deshabilitada rápidamente, en caso de que no la regrese.
- III. Facilita instalaciones con múltiples entradas.
- IV. Los bloqueos nunca son reingresados.
- V. Puede reportar cuántas personas han ingreso a un determinado lugar.

Inconvenientes del sistema.

- I. Al igual que con el sistema anterior, este tiene el inconveniente que cualquier tarjeta válida da entrada a sitio.
- II. Este sistema puede ser caro y una falla en el sistema de autenticación puede causar que el usuario no logre acceder al sitio.
- III. El principal problema con este sistema es un acceso llamado Tailgating. Tailgating es un acceso no autorizado, porque siguen a un individuo con acceso válido.



Figura 3.22. Lector de tarjeta

Fuente: Mathias Lock and Key, 2011.

- Tarjeta de acceso con rehilete (ver Figura 3.23).

Este tipo de tecnología lo encontramos en los estadios. La tarjeta de acceso es el boleto de entrada y el rehilete sólo permite el acceso para una persona. Es un método más seguro que el anterior, además de que toma los beneficios del sistema anterior.

Inconvenientes del sistema.

- I. Este método, generalmente, requiere de un guardia de seguridad para verificar que las personas no están saltando el rehilete, o el acceso especial para personas con discapacidades físicas, que no pasa por el rehilete.
- II. Los rehiletes no son estéticos.
- III. El rehilete puede ser incómodo para personas que llevan acompañantes, por alguna disposición especial como acompañantes o que requieren usar equipo especial.
- IV. Es caro.
- V. Una falla puede ocasionar que no se ingrese al sitio.



Figura 3.23. Acceso con rehilete o torniquete.

Fuente: Mathias Lock and Key, 2011.

- Escáner de huellas digitales (ver Figura 3.24).

El escáner de huellas digitales usa el mapa de las huellas que prácticamente es imposible duplicar. Son ideales para uso masivo en el control de asistencia y acceso.



Figura 3.24. Escáner de huellas digitales.

Fuente: Mathias Lock and Key, 2011.

- Escáner de retina (ver Figura 3.25).

Los lectores de retina analizan los capilares que están situados en el fondo del globo ocular. El usuario debe acercar el ojo al lector y fijar su mirada en un punto. Una luz examina los patrones de los capilares en la retina.



Figura 3.25. Escáner de retina.

Fuente: Mathias Lock and Key, 2011.

- Reconocimiento de cara (ver Figura 3.26).

Esta tecnología analiza las características faciales. Una cámara digital captura una imagen de la cara. Se crea, a partir de aquí, una plantilla.

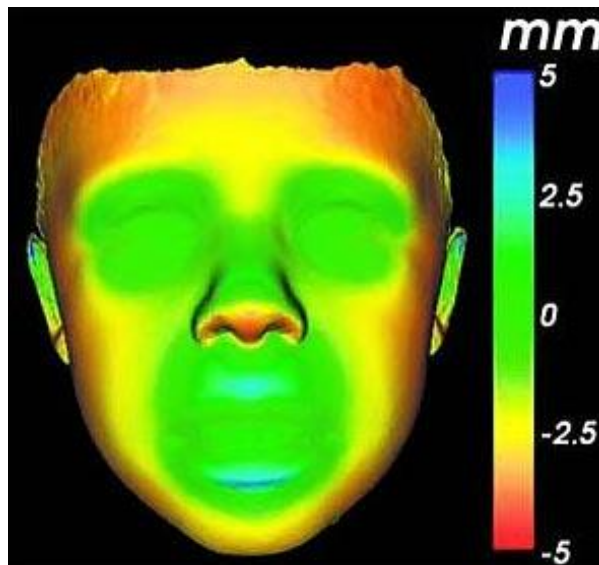


Figura 3.26. Escáner de rostro.

Fuente: Mathias Lock and Key, 2011

Se puede llevar a cabo la implementación de alguno de los mecanismos arriba mencionados, la combinación de dos, o más de ellos.

b. Control de acceso físico a los centros de datos.

En la mayoría de las ocasiones se tiene, para el acceso al centro de datos y servidores, un doble candado, integrado por lo menos por dos tipos de tecnologías de seguridad, de las que se mencionaron arriba. Por lo regular, respaldado por personal de seguridad. Integrado con protocolos de seguridad y control de emergencias, muy bien planeado, tanto en su logística como legal.

Otro de los problemas que se deben considerar, es la ubicación geográfica. Ya que de acuerdo con las necesidades del entorno, se deben construir edificios que soporten temblores, con protección de incendios y maremotos. Considerar si se está expuesto a tormentas eléctricas, para su correspondiente protección, entre otras previsiones. En lo particular, se pueden contratar estudios hechos por la unidad de protección civil de la entidad, o de empresas especialistas en este rubro.

De manera alternativa se tiene el entorno social, ya que la cultura y concientización de los colaboradores, referente a la importancia que implica la conciencia de saber que maneja información, que de acuerdo al nivel operativo de cada uno de ellos, es importante para la empresa.

La seguridad básica del BIOS, para cada dispositivo, es imprescindible. Ya que, por ejemplo, los servidores deben tener una clave de arranque, al igual que los equipos de comunicación, entre otros.

Los sistemas personales como PC, PDA's y móviles en general, deberán contar con algún esquema biométrico, que asegure su correcto uso y apropiación de servicio.

Seguridad del servidor.

La seguridad del servidor es una parte medular de cualquier sistema de control de usuarios. Que debe ser planificada a partir de los usuarios, aplicaciones y niveles de acceso. Tomar en cuenta si están dentro o fuera de la organización (intranet o extranet).

Entre los sistemas operativos que más destacan en el mercado, existen los siguientes, con su respectivo porcentaje (Awio Web Services LLC, 2011):

- Windows 83.63%
- Apple 8.75%
- Linux 1.44%
- Sun 0.1%
- CPM 0.1%
- Otros 6.15%

De acuerdo con lo anterior, la expectativa de seguridad se puede abordar por la tecnología Windows y Unix; Linux, Sun, Aix, incluso Apple. Lo anterior, para plantear la seguridad del servidor y explotar sus ventajas operativas.

Ruest y Ruest (2008) sugieren que se debe aplicar el sistema de defensa del castillo, como se observa en la Figura 3.27.

- **Capa 1 información crítica.** El corazón de su sistema de información que busca proteger. Se trata de la bóveda de información.
- **Capa 2 Protección física.** Las medidas de seguridad siempre deben empezar con un nivel de protección física de sistemas de información. Se compara con el propio castillo.

- **Capa 3 Endurecimiento del sistema operativo.** Una vez que se han colocado las defensas, necesita “endurecer” el sistema operativo de cada equipo, para limitar lo más que se pueda la superficie de ataque. Este es el patio.
- **Capa 4 Acceso a la información.** Cuando da acceso a sus datos, necesita asegurar que todo esté autenticado, autorizado y auditado. Se trata de los muros del castillo y las puertas que abre en ellos.
- **Capa 5 Acceso externo.** La capa final de protección trata con el mundo exterior. Incluye la red perimetral y todas sus defensas. Es el foso de su castillo.

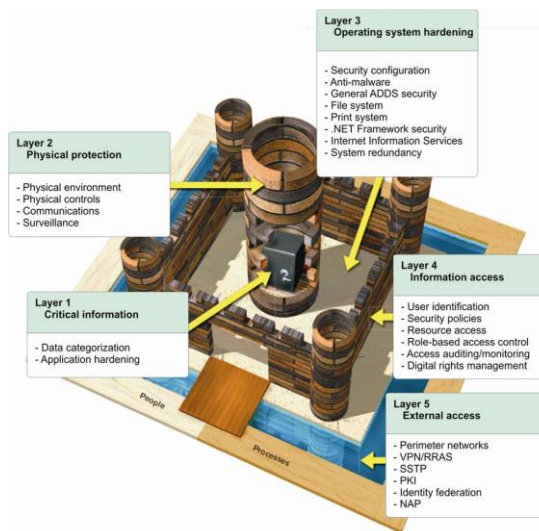


Figura 3.27. Sistema de defensa del castillo.

Fuente: Ruest y Ruest, 2008.

- I. **Brecha de seguridad accidental.** La gran mayoría de los usuarios, tanto noveles como expertos, suelen causarlos de manera accidental. Por lo regular no se dimensionan los peligros que tiene el realizar determinadas acciones, o entrar a ciertas áreas no autorizadas y exploran el contenido. Esto último, por una mala planeación del administrador, porque se tiene o solicita acceso estando habilitado, pero no se tienen las habilidades técnicas para operar.

- II. Ataques internos.** Por lo regular, es falta de vigilancia de los administradores, en referencia a las políticas y procesos de seguimiento. En otras ocasiones se da por usuarios noveles, que quieren experimentar con el sistema.

Teniendo como precedente lo anterior, es una de las principales fuentes de ataque. En realidad, solía ser la principal fuente de ataque, pero con la proliferación de ataques, basados en Internet, su importancia, en proporción a otros ataques, ha venido a la baja. Por lo regular provienen de la red interna.

- III. Ingeniería Social.** La Ingeniería Social puede definirse como una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema. Es el arte de conseguir, de un tercero, aquellos datos de interés para el atacante, por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos.

Estos ataques surgen de la falta de conciencia. Son causados por fuentes externas que toman la personalidad del staff interno y hacen que los usuarios divulguen información comprometedoras. Es una práctica común que este personal les pida a los usuarios su contraseña. Este comportamiento es completamente inaceptable hoy en día. No hay razón para que el personal de soporte técnico tenga, siquiera, acceso a la contraseña de usuario.

- IV. Ataque a la organización.** Este tipo de ataques, por lo regular, son de empresas desleales que quieren causar daño a su competencia. Su principal intención es debilitar su capital de TI, para poder vulnerarlo, tratar de acceder a secretos y patentes empresariales.

- V. Ataques automatizados.** Ahora son los tipos de ataques más comunes. En esencia se rastrea la red, host y vulnerabilidades que tiene la red. Por lo regular, este tipo de ataques son complejos, por el tipo de herramientas que se usan.

- VI. Negación de servicio distribuida.** Estos ataques están diseñados para sobrecargar la operación de un servicio en la red, por ende estresarlo. A menudo surgen de varias fuentes a la vez. De ahí el nombre de distribuida.
- VII. Ataques de virus.** Los ataques por virus, por lo regular gusanos, caballos de troya, virus en general, están diseñados para infiltrar su sistema para que realice alguna forma de daño a servicios o datos.
- VIII. Correos electrónicos maliciosos o suplantación de identidad.** Es muy similar al ataque de ingeniería social, con sus variantes electrónicas, ya que toman desprevenido a la víctima, al engañarla para que realice una acción que otorgará al atacante acceso al sistema. La educación de los usuarios es una de las mejores maneras de evitar estos ataques.

Roles de los usuarios y seguridad lógica. Una de las principales acciones que se deben planear de manera adecuada y exhaustiva, es la forma de administrar a los usuarios, grupos y asociados al sistema. Ya que de esto depende, en gran manera, la forma de llevar a cabo la administración de usuarios, plantillas y grupos a los que pertenece.

De acuerdo al sistema que se use, se determinan las acciones a realizar, pero en esencia es básicamente lo mismo. Es decir, la administración de usuarios y tomas de decisiones, en caso de alguna contingencia, sin que el servicio de red se vea afectado.

O sea, que la "Seguridad Lógica" consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos, a las personas autorizadas para hacerlo".

Los objetivos que se plantean son:

1. Restringir el acceso a los programas y archivos.

2. Asegurar que los operadores puedan trabajar, sin una supervisión minuciosa y no puedan modificar los programas, ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos, en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia, para la transmisión de información.

Controles de Acceso.

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software, de la utilización o modificaciones no autorizadas. Para mantener la integridad de la información, restringiendo la cantidad de usuarios y procesos con acceso permitido, y para resguardar la información confidencial de accesos no autorizados.

Así mismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo; las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso, solicitado por un usuario, a un determinado recurso. Al respecto, el NIST (2008) ha resumido los siguientes estándares de seguridad, que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

- **Identificación y Autenticación.** Firma y acceso relacionado.
- **Roles.** El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes; programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, entre otros. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

- **Transacciones.** También pueden implementarse controles a través de las transacciones. Por ejemplo, solicitando una clave al requerir el procesamiento de una transacción determinada.
- **Limitaciones a los Servicios.** Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software, para cinco personas, en donde exista un control a nivel sistema, que no permita la utilización del producto a un sexto usuario.
- **Modalidad de Acceso.** Temporal, por zona, privilegiado, etcétera.
- **Ubicación y Horario.** El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios, a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso. Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.
- **Control de Acceso Interno.** Tipos de acceso, manejo de la intranet, como acceso privilegiado.
- **Control de Acceso Externo.** Relaciones de confianza para accesos externos; por empleado, por compañía y zonas de exclusión.
- **Administración.** La administración es la que lleva las políticas, estrategias de cómo se han de llevar todos los controles señalados, manejo de riesgos, entre otras acciones vinculadas.

Servicios.

Los servicios que ofrecen en los servidores, así como los usuarios, deben ser planificados con detenimiento. De acuerdo con Ruest y Ruest (2000), la planeación formal de los esquemas, entre los usuarios, servicios e infraestructura, debe ser el 80% del tiempo. El 20% debe ser la implementación.

En el caso de los servidores, de acuerdo con Ruest y Ruest (2008), sugiere seguir la planeación, como se muestra en la Figura 3.28.

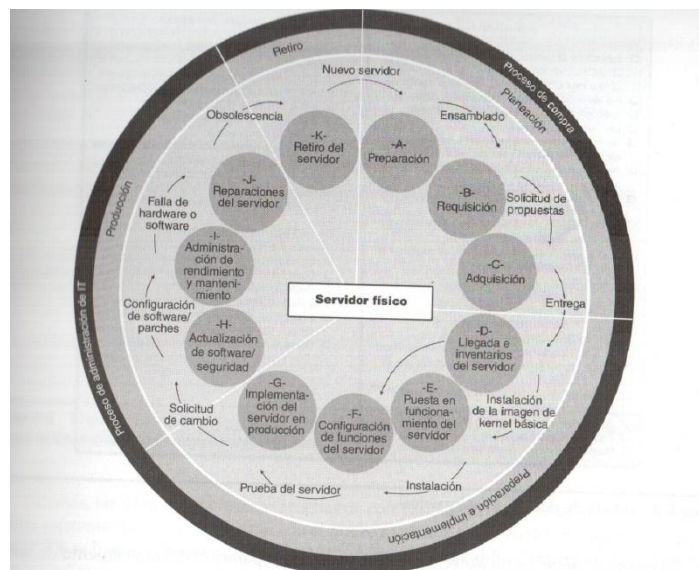


Figura 3.28. El ciclo de vida del servidor físico.

Fuente: Ruest y Ruest (2008, pág. 83)

- **Proceso de compra.** Durante esta fase se deben considerar los requerimientos de los usuarios, para que los procesos en el ámbito empresarial se desarrollen con eficiencia y calidad. Más allá de compromisos económicos o débitos empresariales, para otorgar la compra a un tercero comprometido. Por otro lado se debe considerar la marca, o en su defecto; el ensamblado del equipo, garantía, servicio, el tipo de licitación y claro, su entrega en tiempo y forma.
- **Preparación e implementación.** Aquí se tiene el equipo en sitio, y por supuesto, que debe iniciar la revisión de los componentes; software, controladores que integran el

equipo, sistema operativo, antivirus (en su caso), la instalación, puesta en marcha con algunos usuarios base, configuración de las funciones del servidor e implementación del servidor en producción. Se debe señalar que en esta fase se debe pasar por la prueba de estrés del servidor, para que veamos cómo reacciona a:

- a) Ataques.
 - b) Manejo de peticiones.
 - c) Desempeño de los servicios (www, correo, dns, ftp etc).
- **Producción.** Durante la etapa de producción, el servidor ya está en la etapa final donde se integra a los servicios de la empresa. Por lo regular se debe contemplar la migración de los datos anteriores y montarlos en el servidor nuevo. Por otro lado, se debe considerar la instalación de parches al vuelo, actualización de software, así como los servicios de mantenimiento correctivo y preventivo.
 - **Retiro.** Cuando un servidor pasa a la etapa de retiro, es porque la empresa ya tiene el cálculo de su retiro y próximo reemplazo.

Revisión. Dentro del mismo esquema del servidor se encuentra el ciclo de vida de los servicios, como lo señala Ruest y Ruest (2008), quien indica que se debe contemplar:

- Planeación, identificación y preparación de soluciones para la implementación.
- Implementación. Adquisición, empaquetado, configuración, instalación y prueba de estrategias de implementación.
- Producción. Administración de problemas, cambios, optimización y manejo dentro de la red de producción.
- Retiro. Planeación del reemplazo o la actualización y eliminación de tecnologías y procesos obsoletos.

Seguridad de la comunicación.

Uno de los aspectos más relevantes, para la seguridad del voto electrónico, es la seguridad en la transferencia de la información. Teniendo como antecedente los entornos agresivos que existen en internet y los diferentes intereses que existen alrededor de una elección, como lo ha sido históricamente en México.

Dentro de los esquemas que se deben considerar, para la planeación de la seguridad en la transferencia, se contemplan:

- a) Protección primaria mediante; Firewall, Routers, Switches y en general equipos de comunicación. El primer cinturón de seguridad en la comunicación y traslado de información, vía red, se debe planear en los equipos de comunicación. Ya que de ello depende por mucho la seguridad perimetral. Los equipos de ruteo pueden especificar las listas de acceso de frontera, tanto en el lado de la LAN (Local Area Network), como en la WAN (Wide Area Network).
- b) Autenticación en el sistema operativo.
Se refiere a la autenticación de los usuarios y los privilegios dentro del sistema; tipo de autenticación, manejo de bitácoras, hora de ingreso, hora de salida, operaciones realizadas, accesos no válidos a zonas no autorizadas, por mencionar algunos.
- c) Autenticación en el Sistema Gestor de Base de Datos.
Acceso a bases de datos autorizadas, así como las operaciones permitidas. Igualmente, el manejo de bitácoras y políticas dentro del manejador de datos.
- d) Seguridad en la VPN, la cual básicamente viene dada por los equipos de comunicación, aunque se puede dar por medio de software comercial o libre. Este último punto cobra vital importancia, pues es donde se llevará a cabo la conexión entre los clientes y el servidor. Por lo que impactará de manera directa en la planeación del voto electrónico.

Todo lo anterior se puede manejar mediante un diagrama de flujo, para los puntos de acción de manejo de riesgos, de acuerdo con Withman y Mattord (2010), como se observa en la Figura 3.29:

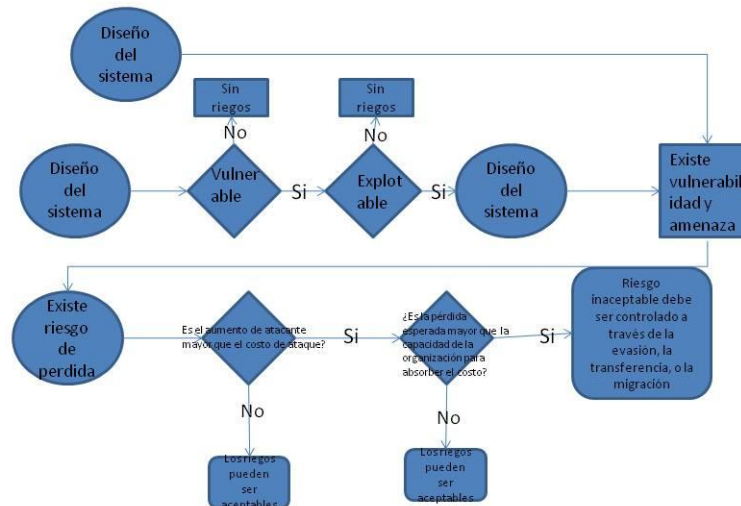


Figura 3.29. Puntos de acción para el manejo de riesgos.

Fuente: Withman y Mattord (2010, pág. 314).

Por otro lado, se debe tener en cuenta un ciclo de control de riesgos. Pues este ciclo debe ser dinámico, ya que las amenazas son latentes mientras el sistema esté en funcionamiento. Por lo cual el ciclo debe tener presente la constante actualización de los métodos, esquemas y formas de defender el sistema, para que este sea autosustentable. Por lo tanto, viable, tal y como se muestra en la Figura 3.30:

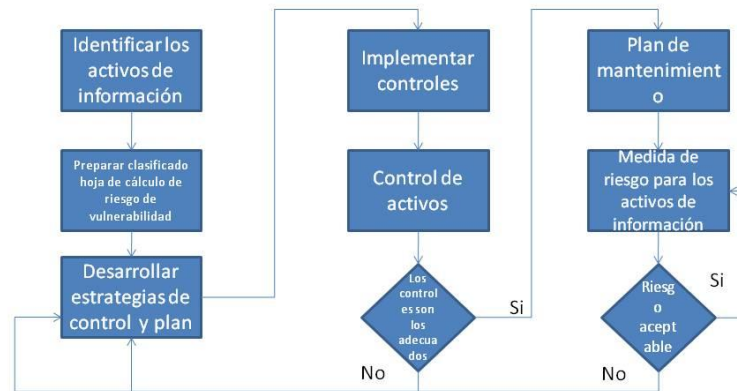


Figura 3.30. Ciclo de control de riesgos.

Fuente: Withman y Mattord (2010, pág. 315).

Análisis costo beneficio.

El costo, exactamente como tal, es la dificultad para determinar el valor de la información. Es tan difícil como determinar el costo de protegerlo. Entre los elementos que pueden afectar el costo de un control, o una garantía, están los que siguen:

- El costo de desarrollar o adquirir software, hardware o servicios.
- Entrenamiento.
- Costo de implementación.
- Costo del servicio
- Costo del mantenimiento.

Para llevar a cabo, mediante una fórmula, el cálculo del análisis costo beneficio, se muestra a continuación (Qingkai, 2010) el proceso:

Fórmula 1. Análisis Costo Beneficio.

$$ACB = EPA(\text{pre-control}) - EPA(\text{pos-control}) - CAS$$

Fuente: Qingkai(2010).

ACB= Análisis costo beneficio.

EPA=Expectativa anualizada de pérdida.

CAS=Costo anual de la seguridad.

Al día de hoy existen algunas gráficas que ayuden a planificar los factores de riesgo. Como la que se describe en la Figura 3.31, la cual, por medio de un árbol de decisiones, señala el análisis del factor de riesgo de la información.

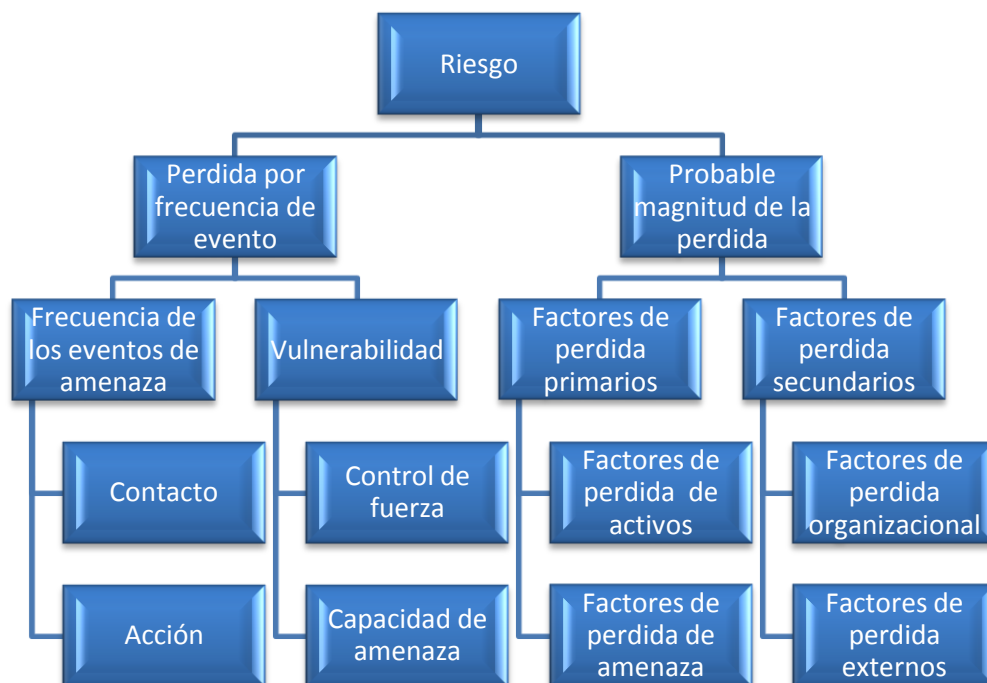


Figura 3.31. Análisis del factor de riesgo de la información.

Fuente: Withman y Mattord (2010, pág. 327).

Gestión de Sistemas.

Es muy posible que una de las partes que más inquietud genera, sea la administración de usuarios. En este caso especial, funge un tema por demás importante, ya que por lo general es donde se puede caer en contradicciones y suspicacias, en caso de no tener la gestión adecuada de los usuarios que pudieran operar el sistema, incluyendo a los mismos electores, como usuarios base del sistema. En el caso particular de Windows y Linux, que son de los sistemas que más proliferan en el mercado, serán analizados para esta situación.

a) Gestión de sistemas Windows.

El sistema operativo Windows tiene un poderoso administrador, el cual permite gestionar los diferentes objetos y recursos de la red corporativa. Como resultado de esta herramienta, para quienes son asiduos usuarios de Windows Server, se han facilitado las tareas redundantes, así como han mejorado las tareas de gestión, minimizando las pérdidas de tiempo y más riesgos de seguridad debido a errores.

Las soluciones Microsoft Identity y Access conforman un conjunto de tecnologías y productos diseñados, para que las organizaciones puedan usar identidades y privilegios de acceso asociados, como lo muestra la Figura 3.32. Concentradas en temas de seguridad y de facilidad de uso, estas soluciones ayudan a que los negocios aumenten su productividad, reduzcan sus costos TI, además de que eliminen la complejidad de identidades y de accesos. Las soluciones Microsoft Identity y Access se aplican a las cinco áreas siguientes:

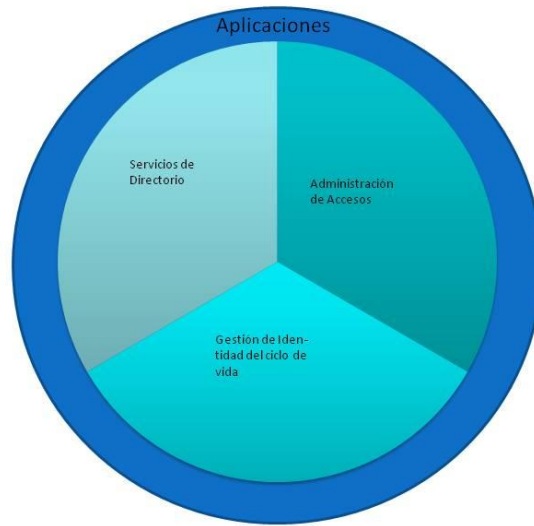


Figura 3.32. Microsoft Identity y Access.

Fuente: Microsoft Corp., 2011.

- Servicios de Directorio: Simplifica la administración de usuarios y dispositivos.
- Sólida Autenticación: Acceso seguro, más allá de los nombres de usuario y las claves.
- Identidades Federadas: Colabora en forma segura, más allá de los límites de la organización.
- Protección de Información: Protege los datos confidenciales, sin importar dónde vayan.
- Administración del Ciclo de Vida de las Identidades: Automatiza la administración de identidades y accesos.

Las ventajas que se resaltan, como lo menciona Microsoft Corp. (2011), en su sitio, son las siguientes:

Controladores de Dominio de Sólo Lectura. En Windows Server 2008, una de las funciones más significativas de los Servicios de Dominio de Active Directory,

conocida como Active Directory Domain Services (AD DS), es el Controlador de Dominio de Sólo Lectura, identificado como Read-Only Domain Controller (RODC). Un RODC permite instalar fácilmente un controlador de dominio, que hospeda una réplica de sólo lectura de su base de datos. Esto favorece a las ubicaciones, donde no puede garantizarse la seguridad física del controlador de dominio. Donde la conectividad de la red puede causar un impacto negativo en la productividad, o donde otras aplicaciones deben ejecutarse en el controlador de dominio y mantenerse bajo la responsabilidad de un administrador del servidor que, en teoría, no es miembro del grupo de Administradores de Dominio.

Servicios de Federación de Active Directory. Los Servicios de Federación de Active Directory, conocida como Active Directory Federation Services (AD FS), son otro rol de servidor perteneciente al sistema operativo de Windows Server 2008. Se puede recurrir a los AD FS para crear una solución de acceso de identidades segura, altamente extensible, y escalable en Internet. Capaz de operar en distintas plataformas, incluyendo entornos con y sin Windows. Ahora AD FS posee una función que permite importar/exportar políticas, y que facilita el establecimiento de una relación confiable, entre socios federados. Existe un proveedor de membrecías que otorga una autorización basada en roles para WSS (Windows SharePoint Services) y RMS (Rights Management Services), para usuarios socios federados. Ahora los administradores pueden limitar la instalación del servicio de federación a través de las Políticas de Grupo. El sistema también ofrece una configuración capaz de verificar la revocación de distintos tipos de certificados.

Auditoría de los Servicios de Directorio. Los administradores cuentan con capacidades de auditoría, gracias a la nueva subcategoría de política de auditoría, denominada Directory Service Changes o Cambios del Servicio de Directorio. Esta política captura los valores viejos y nuevos, de cambios aplicados a los objetos y a los atributos del Servicio de Directorio. Los administradores sabrán exactamente quién realizó algún cambio, cuándo lo hizo, qué objeto y/o atributo cambió, cuáles fueron los valores primeros y últimos. La auditoría del Servicio de Directorio se captura en el

Windows Event Log. Puede consolidarse a través del Microsoft Operations Manager o de herramientas creadas por terceros. Este nivel detallado de ingreso ayuda a simplificar el registro de la administración del Servicio de Directorio. Permite manejar la conformidad regulatoria de la organización.

Rol de Server Core. AD DS y AD LDS, identificados como Active Directory Lightweight Directory Services, son roles admitidos por las instalaciones de Server Core en Windows Server 2008. Server Core es una nueva opción de instalación, que crea un entorno de bajo mantenimiento, ideal para servicios específicos basados en roles. Server Core fue pensado para reducir los requisitos de administración y servicio, así como para limitar las áreas vulnerables de la instalación de Windows Server 2008.

Cryptography API. Next Generation: Criptografía API. En Windows Server 2008, la Nueva Generación (CNG) es una interfaz de programación de aplicaciones o Application Programming Interface (API), completamente nueva, que implementa la recomendación de protocolos Suite B de la National Security Agency. Los Active Directory Certificate Services (AD CS), recurren a la CNG en función de sus necesidades criptográficas. La CNG efectúa un reemplazo, a largo plazo, para la CryptoAPI de versiones anteriores de Windows.

En AD CS, los algoritmos criptográficos clásicos todavía encuentran soporte en los proveedores de servicios certificados, conocidos como Certificate Service Providers (CSPs). Mientras los algoritmos criptográficos nuevos, como la criptografía curva elíptica, o Elliptic Curve Cryptography (ECC), encuentran soporte en los proveedores clave de CNG. Una de las funciones únicas de CNG, ofrece la posibilidad de recurrir a algoritmos criptográficos personalizados, tal como se los necesita.

Modelo de Administración Granular. AD CS utiliza nuevas funciones de seguridad, que permiten controlar quién se registra para obtener certificados, qué tipo de certificados y quién puede otorgar los certificados. Estas funciones de administración

integran los grupos de seguridad de AD DS, a las tareas de administración, llevadas a cabo por los agentes de inscripción y por los Administradores de Certificados.

Plantillas de certificado V3. En AD CS, las plantillas correspondientes al certificado V3 reemplazan a las plantillas de los certificados V1 y V2, incluidas en versiones anteriores de Windows. Admiten los últimos algoritmos criptográficos de la CNG de Windows Server 2008. Las plantillas V3 también ofrecen un método más seguro para la validación de controladores de dominios. Puede encriptar comunicaciones cliente y servidor, relacionados con AD CS.

Administración de la Infraestructura de Public Key Infrastructure (PKI). PKIView, disponible como parte del Kit de Recursos de Windows Server 2003, ahora forma parte como snap-in de MMC, con la instalación de AD CS en Windows Server 2008.

PKIView simplifica la administración del PKI de una empresa, combinando las tareas de administración de Certificados de Autoridad (CA), en una interfaz administrativa única. Esta visión consolidada elimina los límites geográficos, al ofrecer un soporte globalizado a través de Unicode. Lo anterior, por medio de la interfaz consolidada. Así, los administradores cuentan con:

- Una visión única y jerarquizada de la infraestructura del PKI que se registra con, y participa en, una topología AD DS.
- Una vista con relación padre/hijo. Cuando se elige una raíz CA en particular, todos los CAs aparecen detallados en el árbol de la raíz.
- La posibilidad de administrar directamente cada nodo dentro de la interfaz.
- Indicadores con códigos a color, que señalan el estado general de los CAs, de los árboles o del PKI corporativo, como una totalidad.

Soporte para los últimos estándares. En Windows Server 2008, AD CS le ofrece soporte a los últimos estándares, incluyendo el OCSP (Online Certificate Status

Protocol), la IDP CRL (Issuing Distribution Point Extension) y el SCEP (Simple Certificate Enrollment Protocol).

Colaboración Federada. Windows Server 2008 ofrece la primera implementación de la solución completamente integrada, conocida como Federated Rights Management Services. Esta integración combina los aspectos de AD FS (Active Directory Federation Services), con los de AD RMS (Active Directory Rights Management Services) y ofrece un marco de colaboración externo, fácilmente instalable.

Antes de Windows Server 2008, la colaboración con derechos protegidos, que se establece con organizaciones externas, exigía que los administradores TI mantuvieran, de manera interna, un conjunto secundario de credenciales que pudieran ser utilizadas por usuarios externos. Estas eran cuentas de dominio típicas, o alguna forma de integración de passport. Ahora, con la integración entre funciones de AD RMS y AD FS, los usuarios externos que pretendan acceder a contenido protegido por una organización, serán inicialmente autenticados por su "controlador de dominios". Por lo tanto, se eliminará la necesidad de mantener un conjunto redundante de credenciales.

Windows BitLocker Drive Encryption. Windows BitLocker Drive Encryption es una función protectora de datos, disponible en Windows Vista Enterprise y Windows Vista Ultimate. Es para computadoras cliente, y está en todas las versiones de Windows Server 2008. Windows BitLocker Drive Encryption enfrenta las amenazas más concretas de robo o pérdida de datos.

Windows BitLocker Drive Encryption evita la irrupción de hackers en los archivos, así como en el sistema operativo de Windows Server 2008. También impide que agentes externos, no autorizados, vean de manera offline los archivos almacenados en cualquier ubicación protegida. En principio, la función utiliza Trusted Platform Module (TPM) 1.2, para proteger los datos comprometidos y para asegurar que nadie haya ingresado a una computadora con Windows Server 2008, mientras el sistema se encontraba offline. Windows BitLocker Drive Encryption mejora la protección de

datos, al combinar dos subfunciones sumamente importantes: la encriptación total de los discos y la verificación de la integridad de los componentes de inicio temprano.

b) **Gestión de sistemas Linux (Sistemas clones de Unix).**

En el caso muy particular de Linux, son mucho más sencillos los términos y manejo de las entidades, objetos y usuarios, ya que todo sigue un patrón lógico, pues el orden de manejo gestión es:

- Instalar el servicio que se desea.
- Añadir los grupos y usuarios al servicio del que se va a disponer.
- Habilitar.
- Administración y control de los objetos.

En el sistema operativo Unix los servicios se sustentan básicamente en permisos, como sigue:

`[d]rwx rwx rwx`

- *r* permiso de lectura
- *w* permiso de escritura
- *x* permiso de ejecutar.
- *d* ó *l* *d* significa que el objeto en cuestión es un directorio y si aparece una *l*, significa que es una liga similar a los accesos rápidos de Windows.

La primer entrada [d] nos indica si el archivo, al que se hace referencia, es un directorio. En Unix; directorios, archivos, dispositivos y cada uno de los objetos, son tratados como archivos, por lo que sigue el mismo patrón para todas las entidades.

El primer bloque rwx nos hace referencia a los permisos del dueño, es decir, la persona que se registró en el sistema.

El segundo bloque rwx hace referencia al grupo al que pertenece el usuario registrado.

El tercer bloque rwx se usa para otros usuarios.

NIS+.

Para esquemas distribuidos se puede considerar el servicio NIS+.

El diseño de uso del servicio NIS+ (Network Information Service), tiene su base en el servicio NFS (Network File System), para esquemas distribuidos. Es nativo de los sistemas Unix y clones de Unix, ya que forman parte del paquete de servicios con que cuenta.

Básicamente, el NIS+ convierte los archivos convencionales de Unix en un mapa, distribuido en la red, integrada con equipos soportados en el mismo Unix. Aplica tanto para equipos servidores como clientes. No sólo es una administración lineal. Es una administración jerárquica similar al de un DNS.

Adicionalmente, NIS+ soporta llamadas RPC seguras y encriptadas, que ayudan mucho a resolver los problemas de seguridad del viejo NIS.

Por lo regular, cuando se tienen que hacer operaciones administrativas, se realizan desde el servidor principal. En caso de no existir, se toma uno secundario y cuando entra en operación el servidor principal, se actualiza la información sin mayor problema.

Así, cuando hay la ausencia de algún permiso, simplemente esa entidad no puede hacer uso de dicho recurso, en ese modo de operación.

Si se observa, es mucho más fácil la administración, además de la operación de los usuarios y permisos en Unix (Linux) que en Windows. Ya que en este último se deben tener una serie de consideraciones adicionales, para no alterar el orden de los objetos y por ende, quedar en vacíos de seguridad.

Para el caso de ambos sistemas operativos, se cuenta con plantillas administrativas que pueden ser usadas a mejor conveniencia del administrador, por lo que requiere previa experiencia en administración de servidores.

Protocolo Ligero de Acceso a Directorios. Conocido como *Lightweight Directory Access Protocol* (LDAP), es un servicio de administración de “páginas blancas”, similar al X.500, el cual se soporta en la parte superior del TCP/IP, lo que nos permite una administración centralizada.

La implementación de LDAP nos ahorra la gestión de diferentes sistemas de administración de usuarios y permisos. Cuando se tiene en el servidor LDAP una base de datos de usuarios y máquinas, cada usuario o máquina tiene un nombre único, distinto al resto, como una clave primaria de una base de datos. Y después, tiene una serie de campos con su valor correspondiente. Se puede especificar a qué grupo pertenece (usuarios, administradores, etc.), más su nombre de pila, su correo, entre otros aspectos.

Los servicios que se pretende autenticar por LDAP, de acuerdo al manual de solaris de Watters (2003): “tienen un patrón de búsqueda en la BD. Buscarán un campo y un valor determinados en los usuarios, y los que cumplan con el requisito, podrán ser utilizados a través de ese servicio”.

Cabe resaltar que LDAP, como tal, no es un Gestor de Base de Datos, como Oracle o Sql Server. Un directorio es una base de datos, pero en general contiene información más descriptiva y más basada en atributos. La información contenida en un directorio, normalmente se lee mucho más de lo que se escribe, como se ilustra en la Figura 3.33:

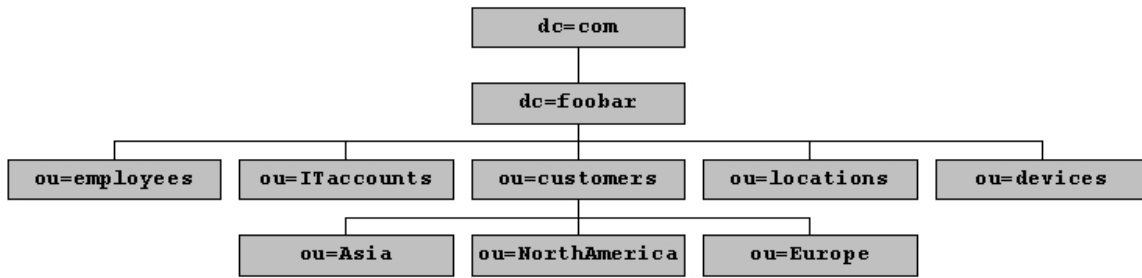


Figura 3.33. Estructura de LDAP.

Fuente: LDAP man home page, 2000.

Como consecuencia, los directorios no implementan normalmente los complicados esquemas para transacciones, o esquemas de reducción, que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos. Las actualizaciones, en un directorio, son usualmente cambios sencillos: de todo o nada.

Una de las ventajas operativas de LDAP es que los sistemas, como Microsoft Windows Server, Novell y el mismo Unix, soportan este esquema, por lo que lo hace muy versátil. Además de ofrecer mucho más ventajas operativas que los esquemas propios, como; Active Directory y NIS+.

3.12 “Fallas” en el voto electrónico.

Una de las principales causas de que el voto electrónico no sea implementado en el Estado de Colima, ni a nivel nacional, es por el poco conocimiento que tiene la población acerca del funcionamiento de las TIC’s. Así como de la confianza que se tiene, en general, de cualquier órgano de gobierno, ya que se pueden enumerar cualquier tipo de tropelías que hacen, por acción o por omisión, los funcionarios en todos los niveles de gobierno.

Un caso sería la venta de información confidencial, como lo menciona *El Universal* (2010), ya que se pueden encontrar; las bases de datos del IFE, el número de casetas telefónicas públicas

de telmex, nombre, adscripción y número de placas de los policías a todos los niveles, entre otros aspectos.

La venta de la base de datos del IFE, de acuerdo con la reportera Carmen Aristegui, en su matutino *MVS* (2010), apoyada con información del periodico *El Universal* (2010), se realiza por medio de sitios web públicos y se hace con la complacencia de las autoridades.

Por otro lado, se tiene el antecedente de las trampas, fraudes y poca ética de los políticos. También por sus propios partidos políticos, para perpetuarse en el poder, a cualquier costo. De esto se pueden citar cualquier cantidad de referencias.

Otro hecho que ha provocado enconos, es la colación de espurios (PAN) y legítimos (PRD) en la actualidad, cuando en su momento más álgido las relaciones, entre estos partidos políticos, estaban por demás polarizadas. Así mismo, la relación prostituida de pequeños partidos, haciendo coalición con partidos de más representación, pero que, por intereses mezquinos y de posicionamiento, se realiza. Tenemos ejemplos en el PRI - PVEM y otros.

La población, en general, ve con tristeza este tipo de tropelías. En lo particular, la ciudadanía ve la poca altura política que se tiene, sintiéndose rebasadas las instituciones políticas por los electores. A nivel internacional los eventos no son nada alentadores y se presentan diversos escenarios, como lo describe Harris B. (2003):

Dallas, Texas: Más de 41,000 votos no fueron contados durante la elección general en 1998, por un error de programación. El recuento fue hecho y la empresa ES&S al mismo tiempo asumió el error. Los Demócratas obtuvieron más de 1000 votos, todo esto no fue suficiente para anular la elección.

Caracas, Venezuela. Mayo, 2000: Las altas cortes de Venezuela suspendieron las elecciones por problemas con la tabulación de las elecciones nacionales. Venezuela envió un jet de la fuerza aérea a Omaha, en busca de expertos de ES&S, de última

hora, en un esfuerzo por resolver el problema. Docenas de protestes reclamaban: “Gringos fuera”, lo anterior a los técnicos de la empresa ES&S. Con este escenario, el presidente Chávez acusó a la empresa ES&S de querer desestabilizar al país.

Como lo señala la página votersunite (s.f.), en el Condado de Pima, Arizona: “Por tercera vez en las elecciones, el Condado de Pima, Arizona, las computadoras no registraron votos por 24 distritos electorales, en las elecciones generales de 1998, pero mostró muchas listas de votantes que habían y estaban usando máquinas World Election Systems, que ahora se venden bajo el nombre de la empresa Diebold”.

Del mismo modo, Harris B. (2004) cita el caso en el Condado de Orange, California:

En el equipo electoral se incurrió en un error del 100 por ciento, durante abril de 1998, en torno al referéndum de bonos escolares. El registro de votantes, inicialmente anunció que la emisión de bonos había perdido por un amplio margen. De hecho, fue apoyada por la mayoría de los votos emitidos. El error se atribuyó a un programador, por revertir el "Sí" y el "No", en el software utilizado para contar los votos.

Un dato interesante es el que presenta Kassab B. (2001), quien relata, entre los problemas expuestos por el Partido Demócrata, en la infame elección de la Florida, el año 2000, lo siguiente:

Cuando una máquina de votación, de la que el candidato presidencial Al Gore tuvo 16.022 votos negativos, el vendedor lo atribuyó a una “tarjeta de memoria defectuosa”. El conteo de votos computarizado dio al candidato del Partido Socialista de los Trabajadores casi 10.000 votos. Casi la mitad del número que recibió en todo el país.

En Florida, en el año 2000, se suscitaron sospechas porque en 47 de 67 condados, Bush recibió más votos, en comparación con los republicanos que estaban registrados. En 15

condados recibió el doble de votos y en 4 más, el triple, como lo señala la página wired.com (2004).

Los anteriores señalamientos se indican, como una manera de mostrar que no existe sistema seguro y confiable, sino se tiene:

- a) Un sistema adecuado que esté probado adecuadamente y por supuesto, certificado ante instancias internacionales. No sólo en esquemas administrativos. Se deben incluir esquemas de seguridad de datos, como lo menciona el NIST, el ITIL, entre otros.
- b) Que exista una adecuada planeación en metodos, procedimientos y logística.
- c) Contar con un sistema transparente de rendición de cuentas, por parte de los órganos de gobierno.
- d) Confiabilidad en las personas que manejan los sistemas, de tal suerte que esté certificado el proceso de selección de personal.

3.12.1 Elementos de seguridad para el voto electrónico.

Los elementos más importantes, para asegurar la información en el voto electrónico, son sin duda la forma de encriptar los datos a la hora de:

- Verificar la referencia del elector en físico (tarjeta, id, o algún elemento similar).
- Certificar el emisor de la información.
- Dar fe de quien se dice ser el elector, sea quien emite el voto.

Para lograr lo anterior, se pretende integrar protocolos criptográficos que nos aseguren que la información es la correcta. Desde saber quién la emite, hasta el receptor que hará uso de la misma (Maiorano, 2009). Esto nos ayudará a solucionar las contrariedades de autenticación, no rechazo, integridad y confidencialidad.

Para lograr lo anterior (Vega Lebrún, Arvizu Gutiérrez, & García Santillán, 2008), los elementos que han de integrar el voto electrónico, independientemente de la plataforma tecnológica, para asegurar la referencia del elector son los siguientes:

- Protocolo de criptografía asimétrica.

El protocolo de firma asimétrica nos permite resolver los problemas de autenticación y no rechazo. Este protocolo se desarrolla usando un algoritmo de clave pública.

- Firma o certificado digital.

La integración de la firma digital se aplica de archivos básicamente a archivos. Pero se extiende a muchas entidades. Funciona de manera similar a la firma autógrafa. El procedimiento que sigue se divide en dos secciones: la primera es el procedimiento de la firma y el segundo la revisión de la misma. Se acepta cuando es auténtica.

Otros elementos a considerar, en el aseguramiento del procedimiento, es el uso de dispositivos biométricos, para elevar el nivel de complejidad y evitar el robo electoral.

3.13 Cuadro de Mando Integral (*Balanced Score Card, BSC*).

Históricamente, las empresas privadas, gubernamentales o paraestatales, hacían su análisis de gestión y planeación, basados en los estados financieros. Lo que al final no permitía hacer ajustes al “vuelo”, para corregir los posibles daños, antes de que estos fueran a impactar a la empresa de manera negativa.

En la actualidad, para evitar estos impactos negativos, que sólo podrían verse al final, muchas empresas en el orbe usan el Cuadro de Mando Integral o BSC. Esta herramienta fue diseñada por Kaplan y Norton (2009), en donde a partir del diseño de la planeación estratégica, se generan los diferentes indicadores que han de ser evaluados por los diferentes departamentos que integran la compañía. Lo que al final se verá reflejado en los indicadores financieros de la

misma. En algunos casos, suele existir un poco de ajuste a esta herramienta, ya que prácticamente, en cualquier parte donde se requiera la gestión y su evaluación, puede usarse.

Básicamente, el BSC requiere de cuatro perspectivas, que a continuación se señalan en la Figura 3.34:

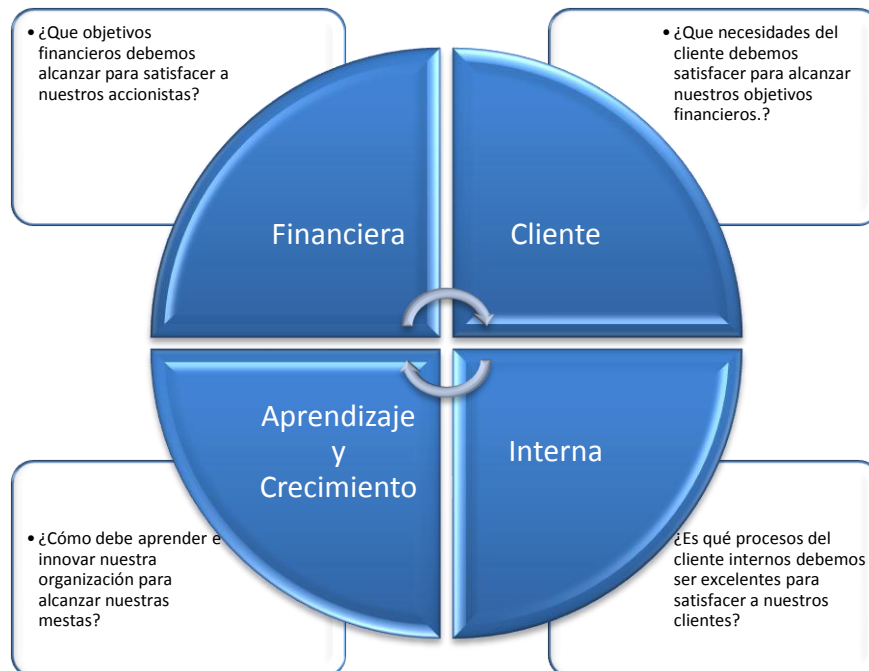


Figura 3.34. Cuadro perspectiva del BSC.

Fuente: Diseño propio, a partir del resumen Kaplan y Norton (2009).

Por medio de esta herramienta se ofrece una visión integrada y equilibrada, de la entidad en evaluación, que permite desarrollar la estrategia de forma clara. Para lograr esto, se ponen sobre la planeación las cuatro perspectivas señaladas en la Figura 3.34; Financiera, Cliente, Interna, Aprendizaje y Crecimiento. Todas enlazadas entre sí, en un sistema de causa/efecto, en un claro alineamiento de los objetivos, trazados con sus respectivos indicadores.

Para la implementación del BSC, deben estar inmersos los altos directivos de la entidad. De preferencia, uno de ellos será el responsable de su implementación, puesta en marcha, desarrollo y seguimiento.

De acuerdo con Keyes (2005), la Junta de Trabajo de los Directores de Empresas (2003), hizo una extensa revisión de cuadros de mando de TI. Se encontró que los cuadros de mando, más avanzados, compartían las siguientes seis características estructurales:

1. Simplicidad de la presentación. Los mejores cuadros de mando se limitan a una sola página, de 10 a 20 indicadores, escrito en léxico no técnico.
2. Vínculos explícitos con la estrategia de TI. El cuadro de mando debe estar bien acoplado al proceso de planificación estratégica de TI. Debe ayudar en el seguimiento del progreso, a salvo de las metas y objetivos clave.
3. Compromiso ejecutivo amplio. Tanto el IT superior, así como altos gerentes de negocios, deben estar involucrados en el proceso de puntuación, tanto en la creación como en su curso.
4. Definición de métricas empresariales estandar. El consenso debe ser alcanzado rápidamente en las definiciones de parámetros. Las reuniones de revisión deben centrarse en las decisiones, en lugar del debate sobre las mediciones.
5. Capacidad drill-down¹ y el contexto disponible. El alto nivel de cuadro de mando de TI, debe permitir la revisión detallada de las tendencias, o sus variaciones, proporcionando una mayor perspectiva en los elementos componentes.
6. La compensación individual del gerente debe estar vinculada a la tarjeta de puntuación y el rendimiento.

Para implementar el BSC, se puede hacer por medio de Excel TM o en programas especializados, como el BSC Designer TM. Para efectos de este proyecto, se debe desarrollar en este último, ya que permite dar un seguimiento pormenorizado. Porque posee una interfaz

¹ En tecnología de la información, para pasar de la información de resumen de los datos detallados por centrarse en algo. Para profundizar a través de una serie de carpetas.

gráfica, muy intuitiva para los diferentes indicadores y seguimientos; por tiempo, por porcentaje, por indicadores, por nivel de riesgo, entre otros. En fin, ofrece tantos indicadores como se requiera evaluar a la empresa (Ver Figura 3.35).

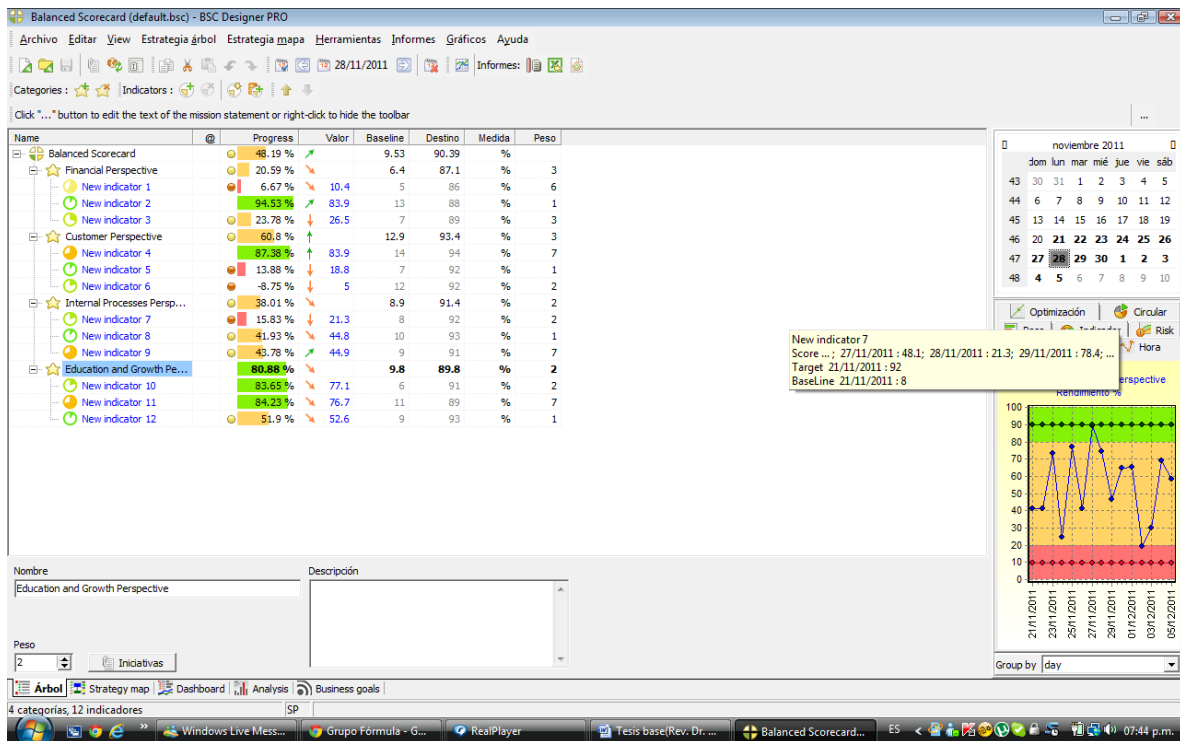


Figura 3.35. Interfaz del BSC Designer.

Fuente: Propia, tomada de Impresión de Pantalla de MS Windows.

3.14 Conclusiones.

La correcta planeación en toda institución debe iniciar desde las altas esferas. Permea en cada uno de los departamentos y grupos de trabajo. Tener muy claro; la misión, visión y objetivos. Por lo anterior, se deben establecer los objetivos generales de la institución, para seguir con los objetivos particulares a cada grupo o departamento, añadiendo a cada uno de ellos la forma de ser evaluados.

Las TIC's siguen este mismo orden, haciendo una adaptación al proceso informático. La planeación de este grupo tecnológico quedaría como se citó en la Figura 3.13:

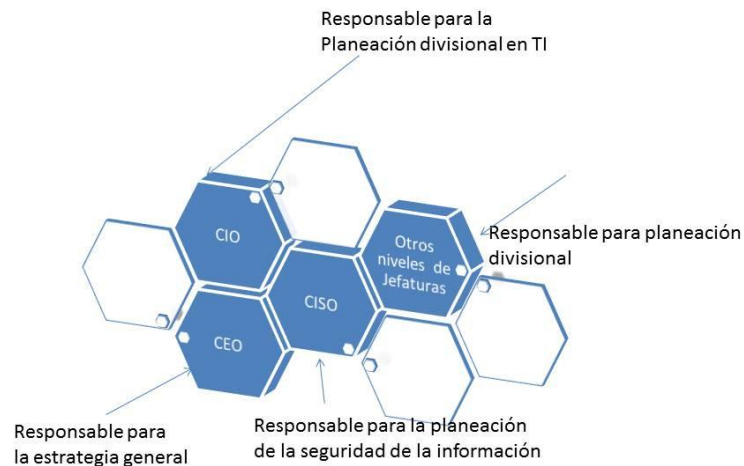


Figura 3.13. Planeación de la Organización.

Fuente: Withman y Mattord. Administración de la Seguridad de la Información (p.44).

Y ya en lo particular, cada grupo tendría su propia planeación estratégica y forma de evaluarse.

Como todo esquema informático y tecnológico, se tienen ciclos de vida que inician en una proyección, prueba, desarrollo, implementación y cierre. Cada una de estas fases tiene su propia forma de evaluación y retroalimentación. De acuerdo a las diferentes metodologías de desarrollo en cada área en particular.

Así, la seguridad de los procesos informáticos han establecido diferentes estándares para su diseño. Los cuales componen dos fases: el diseño físico y el diseño lógico.

En la fase de diseño lógico, los miembros del equipo crean y desarrollan el plan de seguridad. Examinan y aplican políticas claves, que influyen en las decisiones posteriores. En la fase de

diseño físico, los miembros del equipo de evaluación seleccionan la tecnología necesaria, para apoyar el plan de seguridad, generar soluciones alternativas y acordar el diseño final.

Con lo anterior, las urnas electrónicas se apoyan en estos estándares tecnológicos (National Institute of Standards and Technology, 2008), que cada democracia trata de adaptar a las condiciones de su entorno. Procuran respetar los estándares mencionados, así como las normas internacionales que soportan dicha tecnología y que cada vez más países se suman a ello (Aceproject, 2008).

Dentro de los estándares que se deben considerar, están los siguientes puntos:

- Sistemas Operativos.
- Lenguajes de programación.
- Integración del entorno de red.
- Hardware base.
- Sistemas manejadores de Base de Datos.
- Tipo de licenciamiento; libre, comercial, etc.
- Certificación del software.
- Seguridad.
- Controles biométricos.
- Seguridad del sitio.
- Suministro eléctrico.
- Comunicaciones.

A partir de la implementación del sistema, es relevante para su correcto funcionar, la transparencia y confianza, que dé a todos el entorno sociopolítico. Esto se logrará partiendo de que sólo existen CERO errores en su funcionamiento, considerando que un sistema electoral debe contener las siguientes propiedades:

Tabla 3.7. Propiedades del voto electrónico.

| Propiedad | Definición |
|------------------|--|
| Democracia | Sólo los electores elegibles pueden participar en la elección. |
| Conveniencia | Los electores pueden emitir su voto fácil y rápidamente. |
| Movilidad | No hay restricciones impuestas a la ubicación donde los votantes pueden emitir su voto. |
| Eficiencia | Los electores deben emitir su voto en una cantidad razonable de tiempo y no es necesario esperar a otros, para completar el proceso. |
| Robustez | Nadie puede alterar o perturbar las elecciones a causa de la independencia de los procesos de votación. |
| Anonimato | Nadie puede rastrear la identidad de los votantes de las urnas. |
| Autenticación | Las autoridades y los electores deben verificar, uno al otro, durante el proceso de votación. |
| Validación | Las autoridades son capaces de comprobar si los votos son válidos o no. |
| Unicidad | Los electores no pueden votar más de una vez. |
| Completo | Un elector elegible siempre es aceptado por las autoridades. |
| Justicia | Las autoridades tienen prohibido engañar, incluso si intentan colusión. |

Fuente: Chou-Chen, Ching-Ying, y Hung-Wen (2004)

Estas propiedades permitirán que no se cometan errores, como los señalados en el capítulo.

Capítulo IV.- Metodología de la Investigación.

4.1 Introducción.

En la presente investigación se realizará una comparación entre los países de primer mundo y algunos en vía de desarrollo. Lo anterior para observar de manera clara y precisa cómo estos países, de acuerdo a los indicadores de la OCDE, IER y UNTAD, han venido evolucionando en la implementación del voto electrónico.

Es importante que se tenga en cuenta que la tecnología avanza día a día. Razón por la cual ha de tomarse en cuenta que una correcta planeación estratégica, alineada con la tecnología, tiene un papel preponderante para que llegue a buen puerto esta investigación.

Del mismo modo, es importante la revisión que se realizará de manera puntual a los sistemas; en las diferentes latitudes, el tipo de tecnología que se usó y cómo la gente se empoderó de los sistemas. Debemos tener en cuenta que en algunos países existen; dos, tres y hasta cuatro esquemas diferentes de voto electrónico. Al mismo tiempo que se revisará la literatura a nivel internacional, se observarán algunos sistemas que ya se han venido implementando a nivel nacional. Tenemos el caso concreto de Coahuila, donde se entrevistará a los funcionarios y se grabará una elección vinculante para un partido político.

Así mismo, se realizó una encuesta hacia la sociedad, de donde se obtuvo un análisis estadístico descriptivo. Lo anterior, para formar una estrategia en su implementación, ya que la población, de acuerdo a su percepción, dictaminará las formas en cómo aceptará la manera de hacer democracia. Tomará en cuenta la confianza que los actores políticos y la sociedad tengan hacia estos sistemas electrónicos.

Por otro lado, tan importante es el medio como su evaluación. Así se generó una implementación de varias plantillas del Balanced Score Card (BSC), para que una vez puesto en marcha, se evalúe el desempeño y el alcance, con indicadores precisos.

A continuación en la Figura 4.1 se muestra el diagrama de actividades realizado para la presente investigación:



Figura 4.1. Diagrama de actividades.

Fuente: Propia.

4.2 Alcance y enfoque de la investigación.

El alcance del presente proyecto es explicativo, ya que se ha de diseñar un modelo de seguridad para voto electrónico presencial. Tomando como referencia estándares internacionales de seguridad y mejores prácticas en TI. Aplicando herramientas de planeación estratégica para el análisis y evaluación de su desempeño. Lo anterior, considerando principalmente la opinión en el Estado de Colima, de sectores como:

- a) Sociedad.

- b) Partidos políticos.
- c) Gobierno

Se mencionan estos actores como los principales del proyecto, por la sinergia que existe en la triada, pues la democracia no existe sin que sea validada por:

- a) La sociedad, a quien se debe todo el proceso en sí mismo, para saber quién lo va a gobernar en un Estado de derecho.
- b) Los partidos políticos, quienes son los que compiten en la justa para llegar al poder y finalmente...
- c) El gobierno, quien necesita la legitimidad de todos los participantes, para generar un Estado democrático y legal.

Igualmente, el desarrollo de un sistema seguro de voto electrónico debe ir acompañado de la certeza, que debe brindar a todos los involucrado en un proceso electoral, principalmente a la sociedad. Esto se debe lograr con la transparencia del proceso, desde que inicie hasta que termine. Pudiendo éste ser auditado en cualquier evento que sugiera alguna irregularidad, pues sólo con transparencia se da confianza y certidumbre.

4.3 Preguntas de investigación.

Las siguientes preguntas de investigación se demostrarán con los resultados de la encuesta:

- ¿El Estado de Colima cuenta con la infraestructura; tecnológica, logística, legal y política necesaria, para desarrollar un modelo estratégico de votaciones electrónicas presenciales seguras, e implantarlo a mediano plazo?
- ¿Qué tan informada está la sociedad colimense con respecto a las votaciones electrónicas seguras?

- ¿Qué tecnologías de hardware y software se requieren para desarrollar un modelo estratégico de seguridad para votaciones electrónicas presenciales, que apoyen al proceso democrático en el que participa la sociedad?

La primera pregunta de investigación se ha de resolver al obtener los datos del mapa de distribución de la red de datos de la Universidad de Colima. Así como el tipo de servicios que brinda. Por otro lado, existe una estrecha relación entre las preguntas del cuestionario, en el bloque de los datos generales del encuestado, pues se ha de comprobar si existe relación entre; la edad, grado de estudios, el lugar donde vive, su sexo, estado civil y su relación con las TIC's. Ya que de esto dependerá el tipo de estrategia a seguir para la introducción de la democracia digital.

La pregunta número uno de la encuesta ha de establecer la afinidad política. Nos permitirá relacionarla con el bloque de datos generales y analizar el impacto en el uso de TIC's, que existe por estratos.

En cuanto al bloque número 3 (confianza) de la encuesta, nos indicará los parámetros de seguridad que existen en el entorno y su sentir en la población. Esto, para manejar una estrategia política a seguir por parte de los partidos políticos y los órganos encargados de organizar las contiendas electorales. Asimismo, la relación de confianza que existe entre los proveedores de comunicación y seleccionar el esquema que más convenza a la población, para que los datos sean transportados en un entorno de red. También, en la pregunta número 19 de la encuesta se obtendrá el nivel de confianza que se tiene en el gobierno en turno, al cuestionarlo acerca de la apreciación del RENAULT.

Además de lo anterior, se ha de obtener información relativa a qué tan informada está la sociedad colimense, referente al uso de TIC's en otras democracias. Por medio de la pregunta de investigación 2, se han de resolver estas incertidumbres. Sobre todo al obtener información por medio de las preguntas que van de la 40 a la 50. Ya que en ello observaremos si la

sociedad se ha mantenido informada. Si ha visualizado el impacto que ha tenido en el entorno internacional y nacional.

En cuanto a la pregunta de investigación número 3, nos ha de proporcionar información para resolverla a partir de la pregunta 21 y hasta la pregunta 39 del cuestionario. Lo anterior, al visualizar el uso de diferentes tecnologías. Igual, cómo las personas se han identificado con ellas. Así nos darán un parámetro de familiaridad, de confianza, en lo que hacen y usan con cierta frecuencia.

4.4 Diseño de la investigación.

Para el diseño de la investigación se realizaron búsquedas de información en sitios de Internet. Entre los más importantes destacan:

- Sitio del Instituto Nacional de Estándares y Tecnología en Estados Unidos (NIST).
- Los sitios de las democracias que se citan en capítulos anteriores, así como de los diferentes partidos que lo componen.
- El sitio de la Biblioteca de Infraestructura de Tecnologías de Información (ITIL).
- Del sitio del IFE y de los institutos de electorales de; Coahuila, Jalisco, Colima, Yucatán y Distrito Federal.

También se consultaron diferentes textos sobre temas de; seguridad informática, criptografía, sistemas operativos Unix, Windows Server 2003 y 2008, implementación de redes cableadas e inalámbricas. Además de enciclopedias de seguridad informática.

Por otro lado, se realizó una búsqueda exhaustiva de documentos sobre; planeación estratégica, estrategias electrónicas, balanced score card y su implementación.

En cuestión de la elaboración de las estadísticas, el estudio se apoyó en bibliografía de spss y algunos libros del área.

Para la investigación de campo se asistió al Instituto de Participación Ciudadana del Estado de Coahuila, donde se llevó a cabo una entrevista con funcionarios. Así como la filmación de un evento electoral, que ellos coordinaron para el Partido Acción Nacional, en el Estado de Nuevo León, con el apoyo de urnas electrónicas.

4.5 Selección de la muestra.

La determinación del tamaño de la muestra es un factor por demás importante, para que el estudio tenga relevancia e impacto. Al mismo tiempo se debe considerar, para efectos del tiempo, el cual se tiene contemplado para el proyecto, más la inversión en recurso humano y monetario.

Para obtener el tamaño de la muestra, se pueden considerar dos fórmulas. La fórmula 2 (Lind & Mason, 2000, pág. 257) es para cuando no se conoce el tamaño del universo a considerar. La fórmula 3 (Montesinos López et al, 2009, pág. 51) cuando sí se tiene considerado el universo:

Fórmula 2. Cuando no se considera el tamaño del Universo.

$$n = \frac{(Z_{95})^2 (p * q)}{m^2}$$

Fuente: Lind & Mason (2000, pág. 257)

Donde:

n es el tamaño de muestra, obtenido a partir de la fórmula.

Z es el valor estandarizado, con su correspondiente grado de confiabilidad de la muestra calculada.

p es la probabilidad que tiene la muestra, en poseer las mismas propiedades de la población (homogeneidad).

q es la probabilidad que la muestra no esté en el mismo espacio de homogeneidad.

Fórmula 3. Cuando se considera el tamaño del Universo.

$$n = \frac{NZ_{95}^2 pq}{d^2(N - 1) + Z_{95}^2 pq}$$

Fuente: Montesinos López et al (2009, pág 51)

Donde:

n es el tamaño de muestra obtenido a partir de la fórmula.

Z es el valor estandarizado, con su correspondiente grado de confiabilidad de la muestra calculada.

p es la probabilidad que tiene la muestra, en poseer las mismas propiedades de la población (homogeneidad).

q es la probabilidad que la muestra no esté en el mismo espacio de homogeneidad.

d es la precisión y confiabilidad fijada por el investigador.

N es el tamaño del universo a considerar.

Citando como soporte, para obtener el espacio que se va a lograr, se toma como base el conteo del Instituto Nacional de Estadística y Geografía (INEGI, 2005).

Así pues, tomando como base la primera fórmula, se obtienen 295.6 personas. Lo cual redondeamos al valor superior de 296. Si se considera el tamaño del universo $N = 416772$, se obtienen 295.4, el cual se redondea al valor superior de 296. Con lo anterior, para este caso, cualquiera de los dos valores son factibles para la muestra.

Por otro lado se determinó que se tomarían encuestas en dos estratos con tendencia citadina y otro con tendencia rural. Pues las condiciones económicas, demográficas y por nivel educativo, son homogéneas, de acuerdo al estrato al que pertenece, sin tomar en cuenta el municipio. Al mismo tiempo, se respetó la proporción demográfica por género, para que la muestra sea lo más representativa del universo.

4.6 Recolección de datos.

Para la primera parte de la recolección de datos, se realizó una prueba piloto con 50 encuestas. En esta primera etapa se contó con el apoyo de expertos en el área. Los cuales intervinieron en el proceso del diseño de la encuesta, pilotaje, levantamiento y cierre de las mismas. En el proceso, la encuesta piloto fue aplicada de manera equilibrada, como se menciona en el apartado anterior. Este primer levantamiento nos arrojó resultados muy prometedores, en cuanto a los que se obtuvieron. También permitió corregir algunos detalles menores, en cuanto a la redacción de la entrevista y la dirección que debía darse.

Para la aplicación de la encuesta, se tomó en consideración el total de las encuestas, menos las cincuenta iniciales, para así poder completar la muestra y determinar los resultados buscados.

La aplicación de todas las encuestas se llevó a cabo en los municipios siguientes:

- a) Armería.
- b) Colima
- c) Comala.
- d) Coquimatlán.
- e) Cuauhtémoc.
- f) Ixtlahuacán.
- g) Manzanillo.
- h) Minatitlán.
- i) Tecomán.
- j) Villa de Álvarez.

Durante el tiempo que duró la encuesta, se apreció que las personas, en lo general, al tocar el tema democrático, desconfiaban o se mostraban temerosas de la información que pudiera ser comprometedor. A lo cual se les insistía, que el objetivo era una investigación sin fines de lucro y que lejos de perjudicar a la población, se pretendía hacer mejoras en el sistema electoral actual.

En general, para todos los encuestados se observó que era familiar el uso de tecnología celular. También alguna similar al cajero automático o teléfono de casa, por lo que la relación con este tipo de tecnología no era mayor problema.

Referente a los legisladores, se les preparó un instrumento. A pesar de que en repetidas ocasiones se les solicitó cita, para levantar la encuesta, no existió disponibilidad por parte de ellos para llevarla a cabo. Por lo que esa información no se verá reflejada en esta investigación.

La investigación de campo, en el Estado de Coahuila y Nuevo León, fue fructífera. Ya que al estar presentes y observar cómo se prepara una elección, usando estos medios tecnológicos, la logística y el tipo de personal que se debe contemplar, para que todo llegue a buen término, resultó por demás constructivo.

Al regreso de los estados, arriba mencionados, se levantó de nueva cuenta una encuesta. Con un espacio muestral de 30 individuos, para comparar los primeros 50, pues se suscitaron eventos poco alentadores, como el asesinato del ex gobernador Silverio Cavazos Ceballos. Lo que nada ayudó a mejorar los índices de confianza que existían en el entorno.

4.6.1 Selección del instrumento.

Encuesta a la Sociedad en el Estado de Colima.

A continuación se explican, de manera puntual, cada una de las preguntas de la encuesta. La cual está conformada por seis bloques y 41 preguntas:

- 1) Datos generales del encuestado; edad, último grado de estudios, municipio, sexo y estado civil.
- 2) Participación electoral; 3 preguntas.
- 3) Confianza; 16 preguntas.

- 4) Banca electrónica; 3 preguntas.
- 5) Uso de las TIC's; 14 preguntas.
- 6) Voto electrónico; 5 preguntas.

1) Datos generales del encuestado.

Los datos de este bloque (edad, último grado de estudios, municipio, sexo y estado civil), servirán para combinarlos con las opiniones de los encuestados. También para hacer un análisis estadístico por grupos, con la finalidad de revisar si las opiniones, a favor o en contra, dependen de la edad de la gente, de su preparación académica, del municipio en que viven, del sexo, o de su estado civil.

Edad. Con el rango de edad se podrá analizar si existe, o no, alguna relación entre la pirámide generacional y el uso de las TIC's.

Último grado de estudios. Este parámetro servirá para analizar si la experiencia que se tiene, con el uso de las TIC's, depende del perfil académico del encuestado, o si también influye la edad de las personas.

Municipio. Servirá para analizar si la vocación de los municipios (turística, agrícola, ganadera, industrial o servicios) influye en la aceptación, o rechazo, del voto electrónico. Igualmente, si favorece o limita el acceso de la población para el manejo de las TIC's.

Sexo. Servirá para analizar qué género tiene mayor contacto con las TIC's y quiénes coinciden en la incorporación de la tecnología en procesos democráticos. Así mismo, con el rango de edad y el grado de estudios, se determinará hacia qué población se puede dirigir el proyecto.

Estado Civil. Con este parámetro se analizará si el estado civil de las persona propicia un mayor acercamiento con el uso de las TIC's.

2) Participación electoral.

Servirá para conocer el porcentaje de participación electoral en el último proceso estatal (2009).

Pregunta 1. ¿Con qué ideología política simpatiza usted?

Objetivo: Conocer la ideología política de los encuestados.

Justificación: Al identificarse la ideología política de los encuestados, se pueden realizar conexiones con otros parámetros, como; la edad, último grado de estudios, municipio, sexo y estado civil. Luego puede hacerse un análisis estadístico y comparar las magnitudes representadas en cada intervalo de clase. Esto ayudará a que el modelo diseñado cumpla con las expectativas de la población.

Pregunta 2. ¿Votó usted en las últimas elecciones estatales (2009)?

Objetivo: Saber si los encuestados ejercieron su derecho al voto en las últimas elecciones estatales.

Justificación: Este parámetro servirá para tener una perspectiva de la participación electoral que se tuvo en el último ejercicio electoral del Estado.

Pregunta 3. Indique la razón por la cual no votó.

Objetivo: Conocer las razones que tuvieron aquellos encuestados para no participar en el último proceso electoral estatal.

Justificación: Esta pregunta servirá para identificar áreas de oportunidad, que contribuyan a mejorar el porcentaje de participación de los votantes en un proceso electoral.

3) Confianza.

Esta sección servirá para conocer el nivel de confianza que tienen los encuestados, en diferentes rubros; vecinos, compañeros de trabajo, asociaciones religiosas, cuerpos policiacos, medios de información local, detectores de metales instalados en las centrales de autobuses, aeropuertos u oficinas de gobierno. Igualmente en; las compañías que ofrecen servicios de telefonía fija, proveedores de Internet, servicios de telefonía celular y veracidad de los datos almacenados en el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT). Considera el manejo que hará con ellos la Secretaría de Gobernación. De esta manera, se podrá vislumbrar si existe un ambiente propicio en el Estado de Colima, para que la gente confíe en un modelo estratégico para votaciones electrónicas presenciales seguras, o qué aspectos se deben mejorar.

Pregunta 4. ¿Confía en sus vecinos?

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en la gente que vive cerca de él.

Justificación: Esta pregunta servirá para tener una perspectiva de la confianza que tiene la gente, en sus vecinos. En caso de que las respuestas sean negativas, será interesante analizar las razones del por qué los encuestados no confían en sus semejantes, para reforzar este aspecto cuando se diseñe el modelo y lograr que confíen en él.

Pregunta 5. ¿Confía en sus compañeros de trabajo?

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en sus compañeros de trabajo.

Justificación: Esta pregunta ayudará a conocer si los encuestados confían, o no, en sus compañeros de trabajo. En caso de que las respuestas sean negativas, será interesante analizar las razones del por qué los encuestados no confían en sus semejantes, para reforzar este aspecto cuando se diseñe el modelo y lograr que confíen en él.

Pregunta 6. ¿Confía en la gente que acude a rendir culto en la iglesia de su preferencia?

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en la gente que acude a rendir culto a la misma iglesia que él.

Justificación: Esta pregunta ayudará a conocer si los encuestados confían en la gente que comparte las mismas creencias religiosas que ellos. En caso de que las respuestas sean negativas, será interesante analizar las razones del por qué los encuestados no confían en sus semejantes, para reforzar este aspecto cuando se diseñe el modelo y lograr que confíen en él.

Pregunta 7. ¿Confía en los cuerpos policiacos del Estado de Colima?

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en los cuerpos policiacos del Estado de Colima.

Justificación: Esta pregunta ayudará a conocer si los encuestados confían en los cuerpos policiacos de la entidad. Además, servirá para confirmar o refutar las afirmaciones que hacen el Gobierno Estatal y los Gobiernos Municipales, con respecto a la honestidad de quienes se encargan de brindar seguridad a la población. En caso de que las respuestas sean negativas, será interesante analizar las razones del por qué los encuestados no confían en sus cuerpos de seguridad, para reforzar este aspecto cuando se diseñe el modelo y lograr que confíen en él.

Pregunta 8. ¿Confía en los medios de información local; radio, televisión, prensa?

Objetivo: Conocer el nivel de confianza que tienen los encuestados en los medios de información local; radio, televisión, prensa.

Justificación: Esta pregunta ayudará a conocer el nivel de confianza que tienen los encuestados, en los medios locales encargados de informar sobre los diferentes acontecimientos que se suscitan en la entidad. En caso de que las respuestas sean negativas, será interesante analizar las razones del por qué los encuestados no confían en ellos, para reforzar este aspecto cuando se diseñe el modelo y lograr que confíen en él.

Pregunta 9. ¿Confía en la información que proporcionan los detectores de rayos-x, instalados en las terminales de autobuses, aeropuertos u oficinas de gobierno?

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en la información que proporcionan los dispositivos instalados en las terminales de autobuses, aeropuertos u oficinas de gobierno, para detectar metales, explosivos, drogas, etc.

Justificación: Esta pregunta servirá para conocer el nivel de confianza que tienen los encuestados, en los detectores de rayos-x, así como en las personas que los operan. En caso de que las respuestas sean negativas, será interesante analizar las razones del por qué los encuestados no confían en ellos, para reforzar este aspecto cuando se diseñe el modelo y lograr que confíen en él.

Pregunta 10. ¿Confía en la veracidad de los datos almacenados en el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT)?

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en la veracidad de los datos almacenados en el RENAUT.

Justificación: El uso de las TIC's y el conocimiento en los procesos gubernamentales, así como el otorgamiento de productos y servicios a la población, por parte de las autoridades federales, estatales y municipales. Deben estar precedidos por una meticulosa planeación estratégica, que les permita obtener un vínculo estrecho y ganarse la confianza de sus gobernados. Por tal motivo, es importante conocer lo que la gente opina al respecto.

Pregunta 11. ¿Confía en que la Secretaría de Gobernación hará un manejo responsable de los datos almacenados en el RENAUT?.

Objetivo: Conocer si los encuestados confían en que la Secretaría de Gobernación hará un manejo responsable de los datos almacenados en el RENAUT.

Justificación: Para legitimar las diversas acciones que realizan nuestros gobernantes, es primordial que garanticen la transparencia e integridad de sus funciones, como servidores públicos, evitando caer en actos de corrupción. Los datos que en fecha reciente proporcionaron al RENAUT, los usuarios de teléfonos celulares, son confidenciales. De ahí la importancia de un manejo responsable por parte de la autoridad federal. Por tal motivo, es importante conocer lo que la gente opina al respecto.

Pregunta 12. ¿Su proveedor de telefonía fija es:

Objetivo: Conocer el proveedor de servicio de telefonía de los encuestados y su impacto en la región.

Justificación: Esta pregunta servirá para conocer el nivel de penetración que tienen las compañías de telefonía en la región

Pregunta 13. ¿Confía en su proveedor de telefonía fija?

Objetivo: Conocer el nivel de confianza en el proveedor de telefonía fija.

Justificación: Con la información recabada de esta pregunta nos proporcionará una visión clara del nivel de confianza de los usuarios hacia su compañía de telefonía fija.

Pregunta 14. Su proveedor de telefonía celular es:

Objetivo: Conocer el nivel de penetración de las compañías de telefonía celular y su preferencia.

Justificación: Esta pregunta servirá para conocer cómo se encuentra la distribución y preferencia de los usuarios entre las compañías de telefonía celular.

Pregunta 15. ¿Confía en su proveedor de telefonía celular?

Objetivo: Conocer el nivel de confianza en el proveedor de telefonía celular.

Justificación: Con la información recabada de esta pregunta nos proporcionará una visión clara del nivel de confianza de los usuarios hacia su compañía de telefonía celular.

Pregunta 16. ¿Su proveedor de televisión por cable es?

Objetivo: Conocer quien es el proveedor de televisión por cable.

Justificación: Esta pregunta nos servira para recabar información de la penetración de los serivicos de cable y la compañía dominante.

Pregunta 17. ¿Confía en su proveedor de televisión por cable?

Objetivo. Conocer el nivel de confianza en el proveedor de televisión por cable.

Justificación. Con la información recabada de esta pregunta nos proporcionara una visión clara del nivel de confianza de los usuarios hacía su compañía de televisión por cable.

Pregunta 18. Su proveedor de Internet es:

Objetivo. Conocer quien es el proveedor dominante de los servicio de conectividad.

Justificación. Con esta información se obtendra quien es el proveedor de servicio de Internet dominante en la entidad y su impacto.

Pregunta 19. ¿Confía en su proveedor de Internet?

Objetivo. Medir el nivel de confianza entre usuarios y su proveedor.

Justificación. Medir el impacto que tiene el nivel de confianza entre la compañía de internet y el entorno del usuario.

4) Banca electrónica.

Esta sección, servirá para tener un panorama de la frecuencia con que la población utiliza los cajeros automáticos, la banca electrónica, así como el grado de confiabilidad que se tiene en las operaciones bancarias que se realizan a través de los cajeros automáticos. Por ejemplo; retiro de dinero en efectivo, depósitos, consulta de saldos, actualización de contraseña, etc.

Pregunta 20. ¿Utiliza los cajeros automáticos?

Objetivo: Conocer la periodicidad con que los encuestados utilizan los cajeros automáticos.

Justificación: Esta pregunta servirá para conocer la frecuencia con que los encuestados utilizan los cajeros automáticos y si están familiarizados con este tipo de tecnología, que tiene bastante similitud con la que se utiliza para el voto electrónico.

Pregunta 21. ¿Utiliza la banca en línea?

Objetivo: Conocer la periodicidad con que los encuestados utilizan la banca en línea.

Justificación: Esta pregunta servirá para conocer la frecuencia con que los encuestados, utilizan la banca en línea y si están familiarizados con la tecnología que utilizan los bancos en sus sitios Web.

Pregunta 22. Indique el grado de confiabilidad que tiene usted en las operaciones bancarias que se realizan a través de los cajeros automáticos.

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en las operaciones bancarias que se realizan a través de los cajeros automáticos.

Justificación: El funcionamiento de un cajero automático también se parece a la manera en que trabaja la urna electrónica. Lo que implica, entre otros aspectos, conexiones seguras a través de las líneas de comunicación. La interacción que el usuario realiza, con un cajero automático, es muy parecida a la que realizan las personas en procesos electorales mediante voto electrónico. En caso de que los encuestados evidencien un grado de confiabilidad elevado, será de gran ayuda para el diseño del modelo y facilitará su aceptación por parte de la sociedad colimense.

5) Uso de las TIC'S.

Esta sección servirá para tener una idea del nivel en que está la población, con respecto al uso de la tecnología, en aspectos como; enviar mensajes SMS (*Short Message Service*, Servicio de Mensajes Cortos) desde su celular, trabajar con motores de búsqueda para localizar información en Internet, enviar correos electrónicos, enviar información confidencial a través de Internet, utilizar los kioscos turísticos cuando sale de vacaciones o los kioscos de servicios del Gobierno del Estado de Colima, para realizar algún trámite. También considera los servicios que están disponibles en sus hogares, como; telefonía fija, teléfono celular, acceso a una computadora y acceso a Internet.

Pregunta 23. ¿Sabe cómo se envían mensajes SMS (Servicio de Mensajes Cortos) desde su celular?

Objetivo: Conocer si los encuestados saben cómo interactuar con un teléfono celular para enviar mensajes de texto.

Justificación: Las interfaces disponibles, actualmente, en los teléfonos celulares, son llamativas e intuitivas. Lo que facilita la interacción, sin embargo, todavía hay personas a las que se les dificulta operarlos correctamente. Es importante conocer si las generaciones adultas están preparadas para usar esta herramienta tecnológica. Esta pregunta, junto con las demás que integran la sección “Uso de las TIC’s”, servirá para tener un panorama de la brecha digital que existe en el Estado de Colima.

Pregunta 24. ¿Acostumbra enviar mensajes SMS para comunicarse con los demás?

Objetivo: Conocer si los encuestados acostumbran comunicarse con los demás, a través de mensajes SMS.

Justificación: Es importante conocer el porcentaje de encuestados que acostumbran enviar mensajes de texto, para comunicarse con los demás. Y es que algunas personas prefieren usar cadenas alfanuméricas, en lugar de hacer una llamada. Principalmente por el costo que esto representa, o por las diversas aplicaciones que se le pueden adjuntar al

mensaje, como; fotografías, video, animaciones, entre otras. También es común que la gente use los mensajes de texto para participar en concursos y sorteos. Esta pregunta, junto con las demás que integran la sección “Uso de las TIC’s”, servirá para tener un panorama de la brecha digital que existe en el Estado de Colima.

Pregunta 25. ¿Cuántos mensajes SMS acostumbra enviar semanalmente?

Objetivo: Conocer el número aproximado de mensajes de texto que acostumbran enviar, los encuestados, cada semana.

Justificación: Es importante conocer el promedio de mensajes de texto que envían semanalmente los encuestados, ya que se trata de un fenómeno social y cultural que involucra principalmente a los jóvenes. Con las respuestas obtenidas, se analizará la viabilidad de incluir esta herramienta, como parte del modelo que se desarrollará. Esta pregunta, junto con las demás que integran la sección “Uso de las TIC’s”, servirá para tener un panorama de la brecha digital que existe en el Estado de Colima.

Pregunta 26. ¿Tiene acceso a una computadora?

Objetivo: Conocer el porcentaje de personas que tienen acceso a una computadora.

Justificación: Es importante conocer el promedio de personas que tienen acceso a una computadora. Así como el lugar donde se encuentra físicamente el equipo, ya sea en el hogar, en el trabajo, con un amigo, en un ciber café, en la Universidad, o en otro sitio. Esta pregunta, junto con las demás que integran la sección “Uso de las TIC’s”, servirá para tener un panorama de la brecha digital que existe en el Estado de Colima.

Pregunta 27. ¿Ha utilizado algún motor de búsqueda, como; Google, Bing, Hotbot y Yahoo para buscar información en Internet?

Objetivo: Conocer si los encuestados han utilizado algún motor de búsqueda, para localizar información en Internet.

Justificación: Esta pregunta servirá para conocer qué motores de búsqueda utilizan, con mayor frecuencia, los encuestados que necesitan información de Internet. Esta pregunta,

junto con las demás que integran la sección “Uso de las TIC’s”, servirá para tener un panorama de la brecha digital que existe en el Estado de Colima.

Pregunta 28. ¿Confía usted en la seguridad de la información que proporcionan los motores de búsqueda en Internet?

Objetivo: Conocer el nivel de confianza que tienen los encuestados, en la seguridad de la información proporcionada por los motores de búsqueda en Internet.

Justificación: En Internet existe información que proviene de una fuente poco fiable, que puede ser falsa. En ocasiones atenta a la moral y seguridad de las personas. Por eso es importante conocer la opinión de los encuestados, con respecto a la percepción que tienen de la seguridad de la información proporcionada por los motores de búsqueda.

Pregunta 29. Cuando almacena información en la computadora, ¿Confía en que no será modificada o leída por alguien, sin su consentimiento?

Objetivo: Conocer el nivel de confianza que tienen los encuestados que almacenan información en la computadora, de que no será modificada o revisada por alguien, sin su consentimiento.

Justificación: Para muchas personas, la información representa el activo más valioso que poseen. Por lo que es primordial que prevalezca la seguridad en el manejo de la misma. Es importante conocer el nivel de confianza que tienen los encuestados, en el entorno donde realizan sus labores cotidianas. Sobre todo cuando se comparte la misma computadora.

Pregunta 30. ¿Utiliza alguna cuenta de correo electrónico?

Objetivo: Conocer el promedio de encuestados que utilizan alguna cuenta de correo electrónico.

Justificación: El correo electrónico se ha convertido en una herramienta imprescindible para aquellas personas que se encuentran geográficamente distantes y que necesitan comunicarse con frecuencia. Es importante conocer el número de encuestados que poseen

una cuenta de correo electrónico, para tener un panorama de la brecha digital que existe en el Estado de Colima.

Pregunta 31. ¿Con qué frecuencia utiliza su cuenta de correo electrónico?

Objetivo: Conocer la frecuencia con que los encuestados utilizan su cuenta de correo electrónico.

Justificación: Al conocer la frecuencia con que los encuestados utilizan sus cuentas de correo electrónico, se podrá apreciar el acercamiento que tienen con esta herramienta y qué tan importante es para ellos.

Pregunta 32. ¿Ha enviado información confidencial a través de Internet?

Objetivo: Conocer si los encuestados han enviado información confidencial a través de Internet.

Justificación: Es importante conocer si los encuestados acostumbran enviar información confidencial, a través de Internet. La manera en que lo han hecho, así como las razones de aquellos que no lo han hecho, para valorar la confianza que tienen en esta tecnología.

Pregunta 33. ¿Con qué frecuencia envía información confidencial a través de Internet?

Objetivo: Conocer la periodicidad con que los encuestados envían información confidencial a través de Internet.

Justificación: En base a las respuestas de esta pregunta, se determinará el nivel de confianza que tienen los encuestados en esta tecnología. Así como la periodicidad en que datos confidenciales viajan a través de las redes de comunicación.

Pregunta 34. ¿Acostumbra usar los kioscos turísticos cuando viaja?

Objetivo: Conocer si los encuestados acostumbran usar los kioscos turísticos cuando viajan.

Justificación: Esta pregunta servirá para tener una idea de la cultura informática que poseen los encuestados, a partir de la frecuencia con que utilizan los kioscos turísticos en sus viajes.

Pregunta 35. ¿Ha usado los kioscos del Gobierno del Estado de Colima, para realizar algún trámite?

Objetivo: Conocer el promedio de encuestados que han usado los kioscos del Gobierno del Estado de Colima, para realizar algún trámite.

Justificación: Esta pregunta permitirá conocer si los encuestados acostumbran utilizar los kioscos del Gobierno del Estado de Colima, para realizar algún trámite. Los cuales forman parte del programa de Gobierno Electrónico del Estado de Colima. También se podrán conocer los trámites o servicios que más solicitan, así como las razones de aquellas personas que no acostumbran utilizarlos. Todo lo anterior, ayudará a tener un referente de la cultura informática que prevalece en Colima.

Pregunta 36. ¿Con qué frecuencia utiliza los kioscos del Gobierno del Estado de Colima, para realizar algún trámite?

Objetivo: Conocer la frecuencia con que se utilizan los kioscos del Gobierno del Estado de Colima, para realizar algún trámite.

Justificación: Continuando con el aspecto de la cultura informática que prevalece en Colima, es relevante conocer la periodicidad en que son demandados los servicios que ofrecen los kioscos del Gobierno del Estado, para determinar la importancia que éstos representan en el entorno y lo habitados que están los ciudadanos en el manejo y aprovechamiento de las TIC's.

6) Voto electrónico.

Esta sección ayudará a conocer qué tan informada está la población, acerca del voto electrónico. También permitirá conocer su opinión sobre el uso del voto electrónico, en

futuros procesos electorales de Colima. Ya sea a través de un teléfono fijo, un teléfono celular o a través de medios electrónicos, similares a los de un cajero automático. De igual manera, servirá para conocer si los ciudadanos confiarían en los resultados electorales, en caso de que la gente votara a través de medios electrónicos, parecidos a los de un cajero automático y el tipo de proceso (elección vinculante y/o consulta ciudadana) en el que le gustaría que se implementara el voto electrónico en el Estado.

Después de analizar las preguntas de esta sección y de las anteriores, se tendrán elementos contundentes para determinar la pertinencia del proyecto.

Pregunta 37. ¿Le gustaría que en futuros procesos electorales de Colima, se utilizara el voto electrónico a través de un teléfono fijo?

Objetivo: Conocer si a los encuestados les gustaría que en futuros procesos electorales de Colima, se utilizara el voto electrónico a través de un teléfono fijo.

Justificación: Es importante conocer la opinión de la gente e involucrarlos, desde las etapas previas del proyecto que se está desarrollando. Las opiniones que ellos emitan servirán de base para diseñar el modelo estratégico de votaciones electrónicas presenciales seguras, en el Estado de Colima.

Pregunta 38. ¿Le gustaría que en futuros procesos electorales de Colima, se utilizara el voto electrónico a través de un teléfono celular?

Objetivo: Conocer si a los encuestados les gustaría que en futuros procesos electorales de Colima, se utilizara el voto electrónico a través de un teléfono fijo.

Justificación: Es importante conocer la opinión de la gente e involucrarlos, desde las etapas previas del proyecto que se está desarrollando. Las opiniones que ellos emitan servirán de base para diseñar el modelo estratégico de votaciones electrónicas presenciales seguras, en el Estado de Colima.

Pregunta 39. ¿Le gustaría que las elecciones en Colima se llevaran a cabo a través de medios electrónicos, similares a un cajero automático?

Objetivo: Conocer si a los encuestados les gustaría que las elecciones en Colima se llevaran a cabo a través de medios electrónicos, similares a un cajero automático.

Justificación: Es importante conocer la opinión de la gente e involucrarlos, desde las etapas previas del proyecto que se está desarrollando. Las opiniones que ellos emitan servirán de base para diseñar el modelo estratégico de votaciones electrónicas presenciales seguras, en el Estado de Colima.

Pregunta 40. ¿Confiaría en los resultados electorales, si la gente votara a través de medios electrónicos, similares a los de un cajero automático?

Objetivo: Conocer si los encuestados confiarían en los resultados electorales, en caso de que la gente votara a través de medios electrónicos, similares a los de un cajero automático.

Justificación: Es importante conocer la opinión de la gente e involucrarlos, desde las etapas previas del proyecto que se está desarrollando. Las opiniones que ellos emitan servirán de base para diseñar el modelo estratégico de votaciones electrónicas presenciales seguras, en el Estado de Colima.

Pregunta 41. En caso de que el voto electrónico sea permitido en Colima... ¿en qué tipo de proceso le gustaría que se utilizara?

Objetivo: Conocer en qué tipo de proceso les gustaría a los encuestados que se utilizara el voto electrónico, en caso de permitirse en Colima.

Justificación: Es importante conocer la opinión de la gente e involucrarlos, desde las etapas previas del proyecto que se está desarrollando. Las opiniones que ellos emitan servirán de base para diseñar el modelo estratégico de votaciones electrónicas presenciales seguras, en el Estado de Colima.

4.6.2 Aplicación del instrumento.

El desarrollo de este apartado se divide en dos secciones que se describen a continuación.

a) Encuesta.

La encuesta fue realizada con base en el conteo de vivienda 2005, realizada por el INEGI en el 2005. El estado de Colima contaba con una población total de 567996. De este total, la población que estaba en posibilidad de ejercer el voto era de 416772.

Primero se tomaron como base dos estratos. El primero con tendencia citadina, donde se consideran; Colima, Manzanillo y Villa de Álvarez. El segundo estrato es con tendencia rural, que agrupa los municipios de; Armería, Comala, Coquimatlán, Cuauhtémoc, Ixtlahuacán, Minatitlán y Tecomán.

Seguido de esto, se dividió en estratos, por edades, para respetar la proporcionalidad de las personas de acuerdo al género y edad, quedando la distribución como se muestra en las Tablas 4.1 y 4.2:

Tabla 4.1. Distribución de la población en los 10 municipios de Colima.

| Municipio | Población Total | Hombres | Mujeres |
|-------------------|-----------------|-------------------|-------------------|
| Armería | 24,939 | 12,326 | 12,613 |
| Colima | 132,273 | 64,136 | 68,137 |
| Comala | 19,495 | 9,660 | 9,835 |
| Coquimatlán | 17,363 | 8,618 | 8,745 |
| Cuauhtémoc | 25,576 | 12,615 | 12,961 |
| Ixtlahuacán | 4,759 | 2,333 | 2,426 |
| Manzanillo | 137,842 | 68,955 | 68,887 |
| Minatitlán | 7,478 | 3,825 | 3,653 |
| Tecomán | 98,150 | 49,002 | 49,148 |
| Villa de Álvarez. | 100,121 | 48,535 | 51,586 |
| TOTAL | 567,996 | 280,005 | 287,991 |
| Porcentaje | | 49.2970021 | 50.7029979 |

Fuente: Elaboración propia, con apoyo del censo de población y vivienda 2005 (INEGI).

Tabla 4.2. Distribución de la población, en edad de votar, en los 10 municipios de Colima.

| Municipio | Pob. en edad de votar. | Total | Menores de edad. | Personas a encuestar por estrato. | %Hombre | %Mujeres |
|-------------------|------------------------|--------|------------------|-----------------------------------|---------|----------|
| Armería | 15451 | 24939 | 9488 | 21.13 | 22 | 9.72 |
| Colima | 59210 | 132273 | 73063 | 80.96 | 81 | 37.24 |
| Comala | 6505 | 19495 | 12990 | 8.89 | 9 | 4.09 |
| Coquimatlán | 5902 | 17363 | 11461 | 8.07 | 9 | 3.71 |
| Cuauhtémoc | 9772 | 25576 | 15804 | 13.36 | 14 | 6.15 |
| Ixtlahuacán | 1616 | 4759 | 3143 | 2.21 | 3 | 1.02 |
| Manzanillo | 49770 | 137842 | 88072 | 68.05 | 69 | 31.30 |
| Minatitlán | 2119 | 7478 | 5359 | 2.90 | 3 | 1.33 |
| Tecomán | 29577 | 98150 | 68573 | 40.44 | 41 | 18.60 |
| Villa de Álvarez. | 36304 | 100121 | 63817 | 49.64 | 50 | 22.83 |
| | 216226 | | | 295.65 | 301 | |

Fuente: Elaboración propia, con apoyo del censo de población y vivienda 2005 (INEGI).

Tabla 4.3. Distribución final por estratos, de acuerdo a la proporción de las edades.

| Tipo de Población/Estrato por Edad. | 18-20 | 21-25 | 26-30 | 31-35 | 36-40 | 41-45 | 46-50 | 51+ |
|-------------------------------------|-------|-------|-------|-------|-------|-------|-------|-----|
| Rural Mujeres | 12 | 11 | 11 | 4 | 7 | 5 | 3 | 0 |
| Rural Hombres | 10 | 14 | 2 | 4 | 9 | 3 | 4 | 0 |
| Ciudad Mujeres | 20 | 25 | 14 | 17 | 17 | 11 | 10 | 0 |
| Ciudad Hombres | 21 | 17 | 15 | 12 | 14 | 16 | 11 | 0 |
| Total por estrato | 63 | 67 | 42 | 37 | 47 | 35 | 28 | 0 |

Fuente: Elaboración propia, con apoyo del censo de población y vivienda 2005 (INEGI).

4.7 Interpretación de los resultados.

Para el proceso de interpretación de los datos, se considera el uso de estadística descriptiva, acorde con las recomendaciones del comité de expertos que apoyó en el proceso. Las gráficas que a continuación se muestran, nos revelan el comportamiento y sentir social, referente al uso, o no, de este tipo de tecnología. Esto se ha de considerar para la estrategia que debe seguirse en un futuro, para su implementación.

El Grafico 4.1 nos muestra el balance que se respetó, en cuanto a la representatividad de género, en el Estado y en los estratos que se cuidó fueran balanceados en cada uno de ellos.

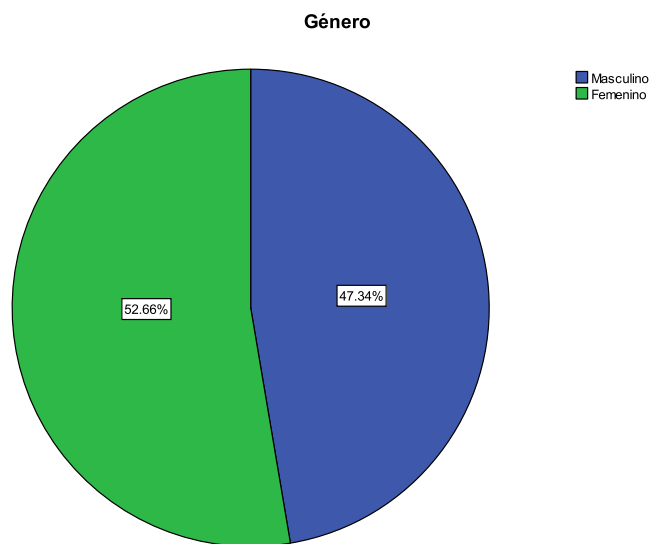


Gráfico 4.1. Género del encuestado.

Fuente: Propia, con apoyo del SPSS.

Así mismo, en el Estado de Colima se puede observar que la pirámide generacional es muy apta para la implementación del voto electrónico, ya que el 80.3 % acumulado son personas menores de 40 años, como se observa en el Gráfico 4.2.

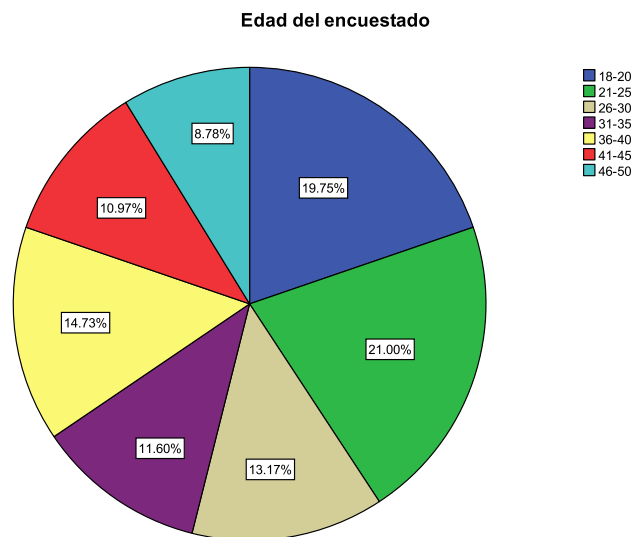


Gráfico 4.2. Edad del encuestado.

Fuente: Propia, con apoyo del SPSS.

Por otro lado, se obtuvo un dato interesante en cuanto al nivel escolar, ya que en la entidad se posee un nivel de preparación académica por demás apto. Pues si consideramos el porcentaje acumulado, de nivel medio superior a postgrado, es de 79.9.% como se aprecia en el Gráfico 4.3. Este dato es fundamental, ya que en la mayoría de las escuelas, a estos niveles, la penetración y el manejo de TIC's es muy alto.

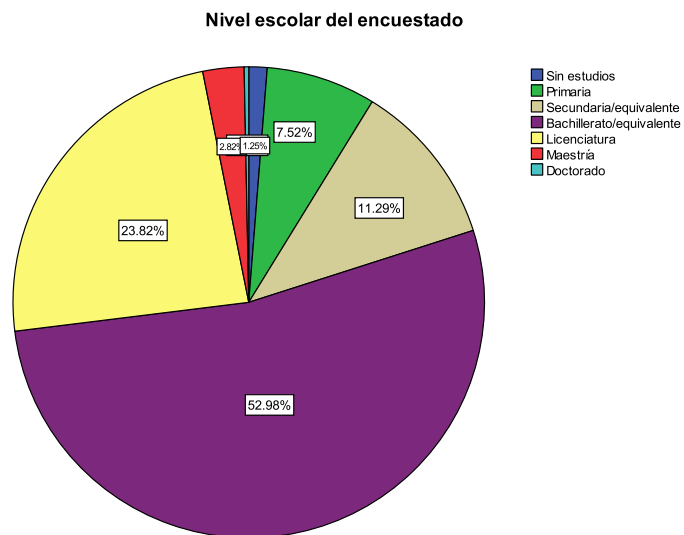


Gráfico 4.3. Edad del encuestado.

Fuente: Propia, con apoyo del SPSS.

En cuanto a la consideración de la confianza que tiene la sociedad en general, en el entorno, se muestran los Gráficos del 4.4 al 4.6. Los cuales nos describen el nivel de confianza en los Cuerpos de Seguridad (ver Gráfico 4.4). Aquí se tiene un promedio del 68.33%. Esto es el reflejo de las diferentes acciones negativas que han empañado el entorno estatal. Como son los asesinatos a políticos de primer nivel y un exgobernador. Se incluye también la pelea de “La plaza”, por parte de grupos ligados al crimen organizado, donde no han salido airosos los cuerpos policiacos.

¿Confía en los cuerpos policiacos del Estado de Colima?

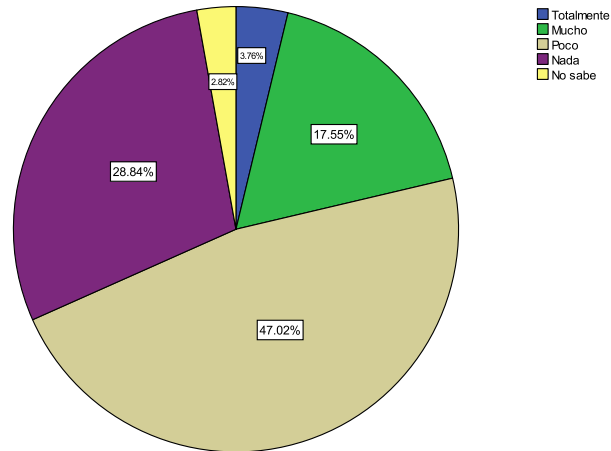


Gráfico 4.4. Confianza en los cuerpos de seguridad.

Fuente: Propia, con apoyo del SPSS.

En referencia a la confianza que el elector muestra con las personas que acuden a rendir culto, en los templos de su misma creencia religiosa (Ver Gráfico 4.5), la confianza se incrementa. Ya que muestra un promedio del 84.33%. Lo anterior, quizá motivado por la misma creencia que profesan.

¿Confía en la gente que acude a rendir culto en la iglesia de su preferencia?

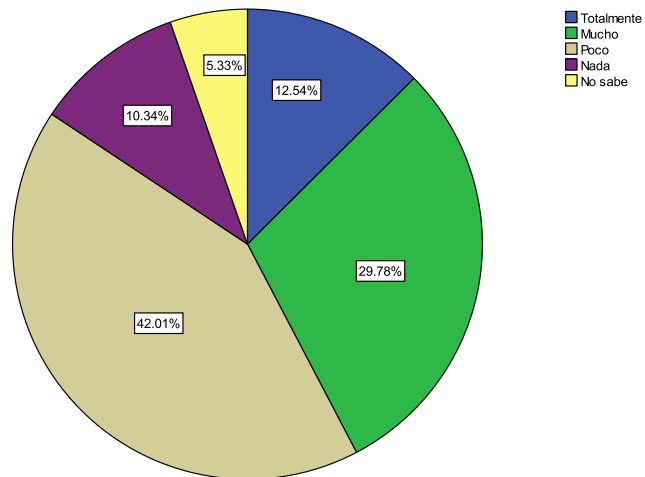


Gráfico 4.5. Confianza en los miembros de su culto.

Fuente: Propia, con apoyo del SPSS.

En cuanto a los medios de comunicación, existe una situación similar a la anterior. Ya que las personas encuestadas nos muestran un promedio acumulado del 88.71%. Esto, porque es un Estado pequeño, donde los medios tienen un alto impacto, por los diferentes escenarios que están involucrados. Principalmente en cuestiones de; protección civil, enlace con poblaciones alejadas y con limitantes de vías de comunicación. Por lo que en general son bien vistas y esto se aprecia en el Gráfico 4.6.:

¿Confía en los medios de información local (radio, televisión, prensa)?

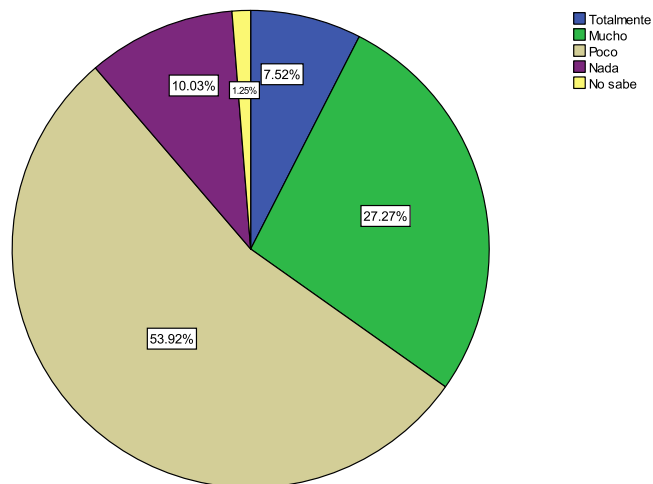


Gráfico 4.6. Confianza en los medios de información.

Fuente: Propia, con apoyo del SPSS.

En el Gráfico 4.7 y 4.8 se muestra que existe una inclinación, en el acumulado de confianza, hacia los proveedores de Internet y Telefonía, con un porcentaje del 63.01% y 78.06%, respectivamente, por parte de la muestra. Este dato se relaciona de manera fiel con el estudio realizado por Aguirre Paz y Ortega Castañeda (2005), en su análisis de servicio por parte de los proveedores de telefonía e internet, siendo en el Estado de Colima, el proveedor dominante, la compañía Teléfonos de México (TELMEX).

¿Confía en su proveedor de Internet?

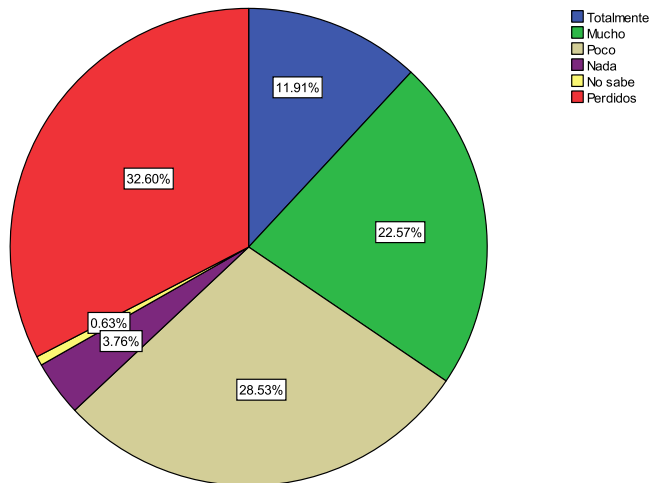


Gráfico 4.7. Confianza en el proveedor de Internet.

Fuente: Propia, con apoyo del SPSS.

¿Confía en su proveedor de telefonía?

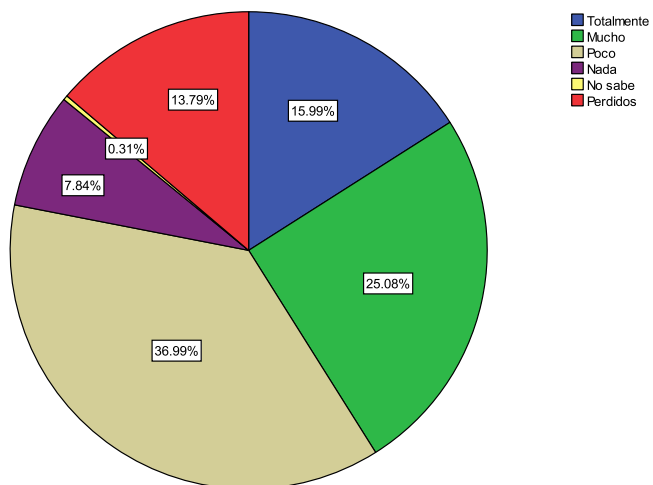


Gráfico 4.8. Confianza en el proveedor de Telefonía.

Fuente: Propia, con apoyo del SPSS.

En cuanto al manejo electrónico de los datos, por parte de nuestras autoridades, la percepción es un tanto equilibrada. Sin dejar de ser un dato algo alentador, ya que el acumulado es poco a totalmente del 59.88% (ver Gráfico 4.9). Este dato se ve reflejado de ese modo, pues la percepción de la población es que no hubo impacto real con este programa, por parte de la Secretaría de Gobernación (SEGOB).

¿Confía en que la Secretaría de Gobernación hará un manejo responsable de los datos almacenados en el RENAUT?

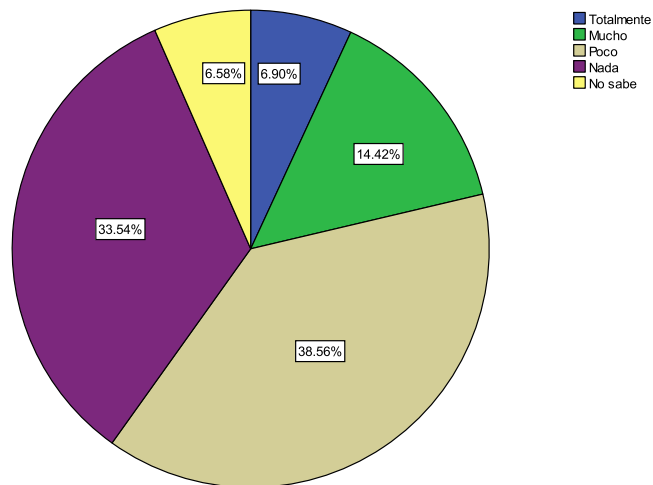


Gráfico 4.9. Confianza en los datos almacenados en el RENAUT.

Fuente: Propia, con apoyo del SPSS.

Del mismo modo, se cuestionó qué grado de confianza se tiene en las operaciones bancarias, usando cajeros automáticos. El Gráfico 4.10 marca un acumulado, de poco a totalmente, con un promedio del 83.38%. Porcentaje que es un tanto alentador, por lo que implica el manejo de cajeros, el uso de la tecnología y sus interfaces.

Indique el grado de confiabilidad que tiene usted en las operaciones bancarias que se realizan a través de los cajeros automáticos

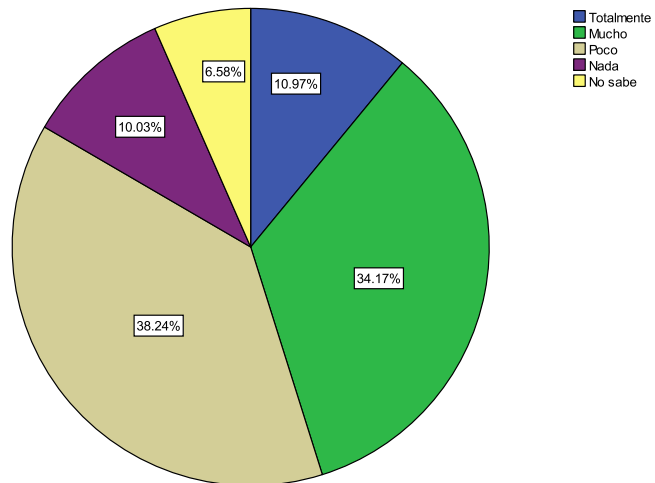


Gráfico 4.10. Grado de confianza en las operaciones bancarias, usando cajeros automáticos.

Fuente: Propia, con apoyo del SPSS.

Así mismo, los encuestados manifestaron tener acceso a una computadora, en un 87.46% (ver Gráfico 4.11). Porcentaje por demás halagador, para el propósito de la construcción y uso de la urna electrónica.

¿Tiene acceso a una computadora? (Si la respuesta es NO, especifique la razón y pase a la pregunta 37)

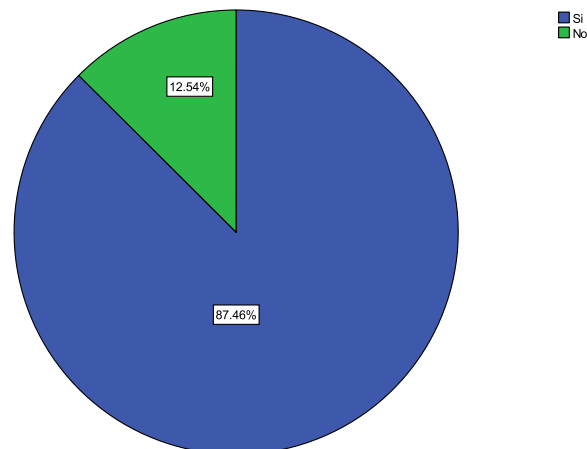


Gráfico 4.11. ¿Tiene acceso a una computadora?.

Fuente: Propia, con apoyo del SPSS.

Continuando con el acceso a las computadoras personales (PC), los interrogados manifestaron que, en mayor parte, el acceso a esta tecnología es en el hogar, con un promedio del 54.55% y en el trabajo con un 15.99%. Lo que hace el uso y penetración de las PC, la piedra angular de este trabajo.

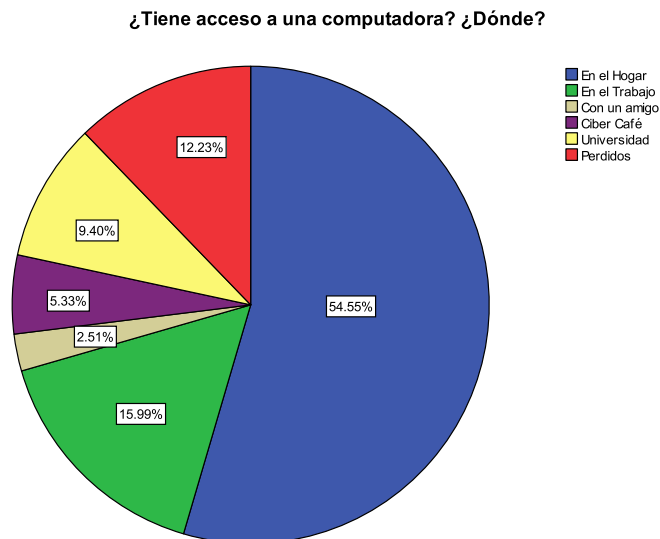


Gráfico 4.11. ¿Tiene acceso a una computadora?.

Fuente: Propia, con apoyo del SPSS.

Siendo el manejo de la tecnología, importante para este proyecto, se les cuestionó acerca de poseer cuenta de correo electrónico. A lo cual, el Gráfico 4.12 manifiesta un porcentaje del 80.88%. Lo que permite señalar la alta penetración que tiene en la población, este tipo de comunicación y su relación estrecha con la población.

¿Utiliza alguna cuenta de correo electrónico?

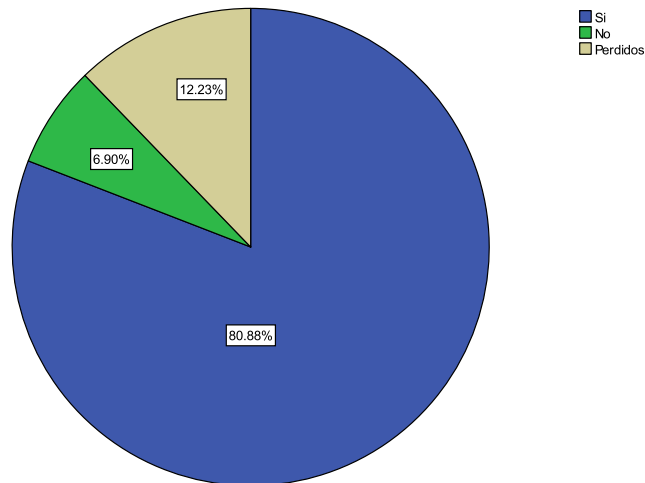


Gráfico 4.12. ¿Utiliza alguna cuenta de correo electrónico?.

Fuente: Propia, con apoyo del SPSS.

En los Gráficos 4.13 y 4.14 se pueden observar cómo la gente está muy familiarizada con el uso de los Kioskos de servicio del Gobierno del Estado, ya que el 73.35% manifestó que sí ha hecho uso de los beneficios que se ofrecen.

¿Ha usado los kioscos del Gobierno del Estado de Colima para realizar algún trámite?

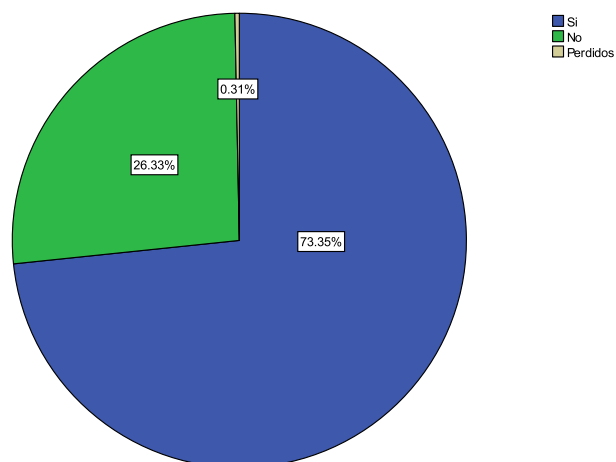


Gráfico 4.13. ¿Ha usado los Kioskos del Gobierno del Estado de Colima para realizar algún trámite?.

Fuente: Propia, con apoyo del SPSS.

En el Gráfico 4.14 se hace notar la frecuencia con que las personas asisten a realizar algún trámite.

¿Con qué frecuencia utiliza los kioscos del Gobierno del Estado de Colima para realizar algún trámite?

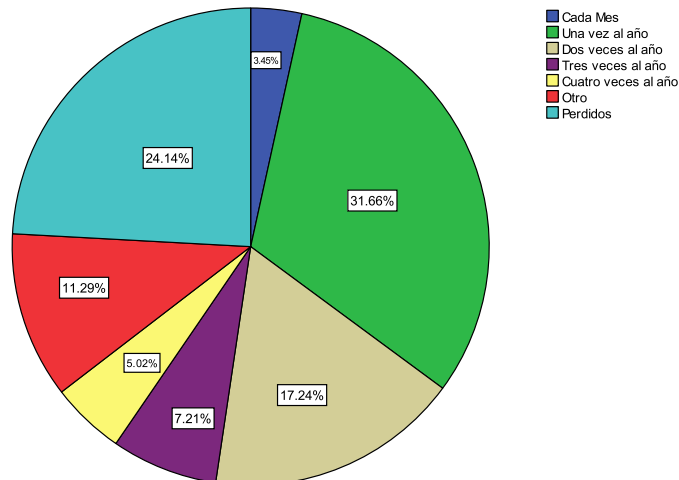


Gráfico 4.14. Frecuencia de uso de los Kioscos del Gobierno del Estado de Colima.

Fuente: Propia, con apoyo del SPSS.

En el Gráfico 4.15 se le cuestionó a las personas si les gustaría que las elecciones, en el Estado de Colima, fueran usando tecnología similar a la de un cajero automático. A lo cual respondieron de manera afirmativa con un 36.68%, y 55.49% de forma negativa. Este dato será determinante para fincar la estrategia de penetración.

¿Le gustaría que los procesos electorales en el Estado de Colima se realizaran a través de medios electrónicos similares a un cajero automático?

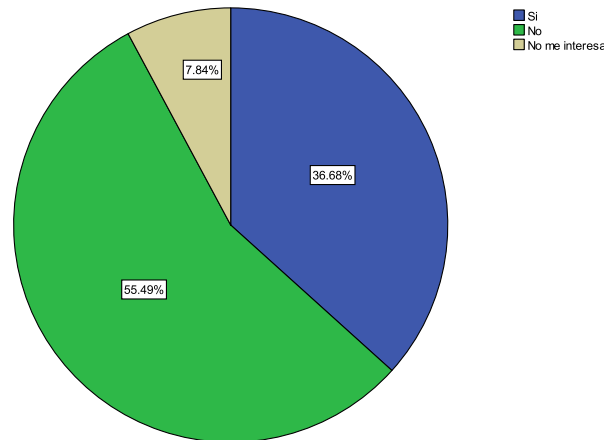


Gráfico 4.15. ¿Le gustaría que los procesos electorales, en el Estado de Colima, se realizaran a través de medios electrónicos, similares a un cajero automático?.

Fuente: Propia, con apoyo del SPSS.

El Gráfico 4.16 va muy de la mano con el sentir general de la población. Ya que la confianza del entorno, por si misma, está muy mermada. Se le añade el uso de una tecnología que movería la dinámica social y democrática, además que la incrementaría. Igualmente, este es un factor a considerar en su implementación.

¿Confiaría usted en los resultados electorales finales si la gente votara a través de medios electrónicos similares a los de un cajero automático?

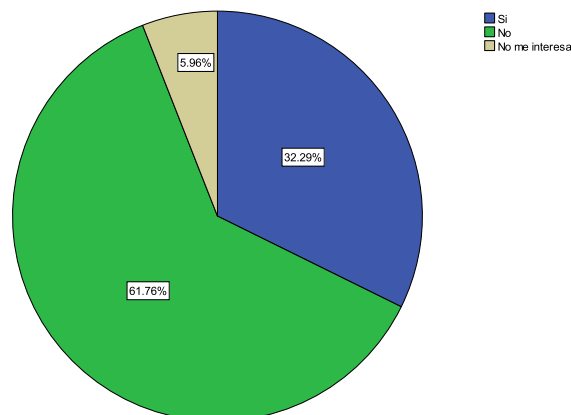


Gráfico 4.16. ¿Confiaría usted en los resultados electorales finales, si la gente votara a través de medios electrónicos, similares a un cajero automático?.

Fuente: Propia, con apoyo del SPSS.

Igualmente, se les cuestionó en qué tipo de proceso les gustaría emplear este tipo de tecnología. El porcentaje muestra una mayoría, con el 39.50% que desea se use en una consulta ciudadana. Seguido de un 31.35% en ambos tipos de elecciones (vinculante y consulta). Por otro lado, un 17.24% manifestó que no le gustaría en ningún proceso. Por último, un 11.91% indica que le agradaría fuera en elecciones vinculantes. En particular, este dato nos indica cómo hemos de iniciar el proceso de implementación, ver Gráfico 4.17.

En caso de que el voto electrónico sea permitido en el Estado de Colima, ¿en qué tipo de proceso le gustaría que se utilizara?

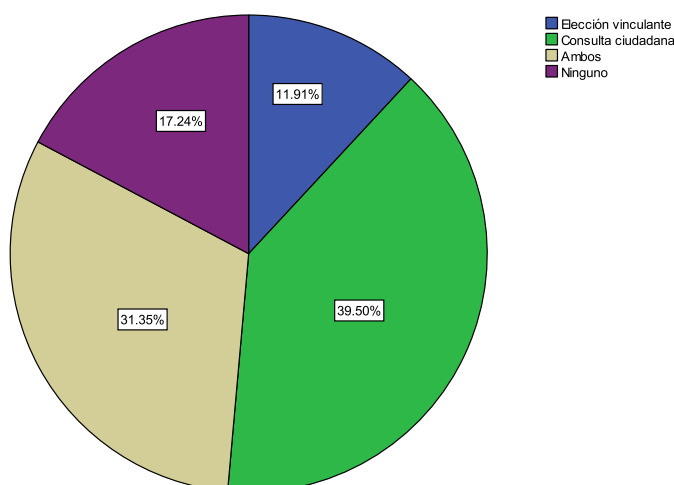


Gráfico 4.17. En caso de que el voto electrónico sea permitido en el Estado de Colima ...¿En qué tipo de proceso le gustaría que se utilizara?

Fuente: Propia, con apoyo del SPSS.

4.8 Video entrevista.

La video entrevista se llevó a cabo con el Ing, Carlos Alberto Arredondo Sibaja, Consejero Electoral del Instituto Electoral y de Participación Ciudadana del Estado de Coahuila (IEPC), quien explicó el desarrollo que han tenido las urnas electrónicas en dicha entidad. La importancia que han ganado de entonces a la fecha, la inversión que se realizó con los ciudadanos, la relevancia que le dieron los órganos de gobierno, legisladores y los propios partidos políticos.

Por otro lado, se observaron las diferentes versiones (IEPC, 2010). Desde el primer prototipo liberado en el año 2002, que tiene las siguientes características:

- Tarjeta madre; video, audio y tarjeta de red, integrados.
- Procesador Pentium.
- Memoria RAM
- Disco duro.
- Unidad de discos floppy.
- Monitor CRT 14”.
- Pantalla touchscreen.
- Lector de código de barras.
- Impresora de inyección de tinta.
- Fuente ininterrumpida de poder.
- Contenedor de madera.
- Sistema operativo XP.

Hasta la quinta versión, liberada en 2008, que tienen en uso y posee las siguientes características:

- Tablet PC
- Monitor LCD 12” (800x1280)
- Pantalla sensible al tacto
- Handy drive (memoria USB)
- Bocinas Integradas
- Lector de códigos de barra, tipo slot
- Impresora térmica, tipo punto de venta
- Fuente ininterrumpible de poder exterior
- Contenedor en plástico y aluminio
- Sistema operativo: Windows Vista – Windows 7.

Cabe señalar que en el Estado de Coahuila, desde el inicio del proyecto, se legisló al respecto. Además de que el proyecto, en su estructura básica, no fue para un sexenio o un periodo de gobierno en especial. Sino que se estructuró para que fuese parte fundamental de la democracia en aquel Estado.

La importancia en la logística, que han desarrollado en el IEPC, es un punto a resaltar, ya que iniciaron con un estudio de cómo llevar a cabo estos procesos. Lo han venido depurando en cada elección, dependiendo del tipo de sufragio y su proceso. Lo que lo convierte en un esquema innovador.

Se mencionó, por parte de los funcionarios, que la urna ha sido usada desde comunidades indígenas, en la Sierra Tarahumara, hasta universidades de primer mundo. Incluyendo otras asociaciones, instituciones y partidos políticos. Dentro y fuera del Estado han solicitado apoyo para llevar a cabo sus elecciones, por la gran transparencia que ofrece el sistema. Al mismo tiempo, la capacitación del personal con que cuenta y los altos valores éticos que poseen, convierten este proceso en un importante método democrático para sufragar.

Como parte relevante, se mencionó que la certeza depositada en cualquier método de sufragio, electrónico o tradicional, parte de que el ciudadano tenga confianza en las formas, métodos y sus instituciones. Además de la generación de certeza por parte, principalmente, de los actores, pues en ese momento son los líderes de opinión y quienes movilizan a las personas que simpatizan con ellos.

Como se menciona en la entrevista, es importante que todas las aristas de una elección sean cuidadas, de manera celosa y profesional. Además de seguir innovando en las formas como se lleva a cabo. Ya que la intención es que el proceso sea más universal, incluyente para personas con capacidades diferentes. También, que de manera paulatina, más personas, independientemente de la zona donde vivan, tengan acceso a estos esquemas electrónicos.

4.9. Conclusiones.

En el Estado de Colima se cuenta con la infraestructura adecuada, ya que para el arranque del proyecto, se posee una infraestructura de red adecuada, para permitir un flujo de datos seguros, como el que se busca. Ver Figura 4.2:



RED UNIVERSITARIA

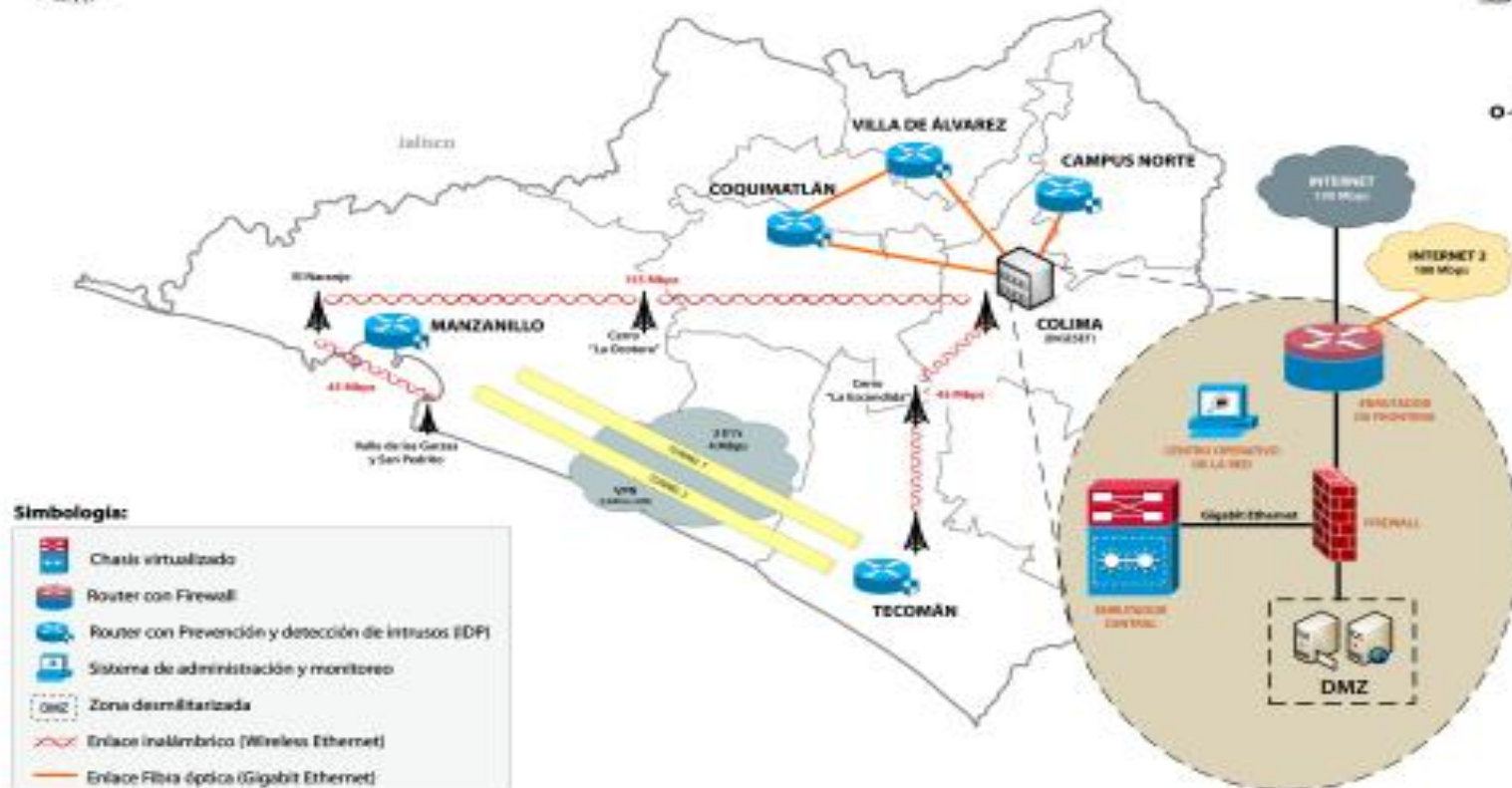


Figura 4.2. Infraestructura de red de la Universidad de Colima.

Fuente: Dirección General de Servicios Telemáticos. Universidad de Colima.

De manera detallada se tiene la siguiente infraestructura, como se detalla en la Tabla 4.4.

Tabla 4.4. Relación de los enlaces en la Universidad de Colima.

| <i>Lugar</i> | <i>Tipo de enlace</i> |
|-------------------------------|---|
| Campus central | Fibra óptica |
| Campus Villa de Álvarez | Fibra óptica |
| Campus Tecomán (“El Crucero”) | Enlace inalámbrico (Microonda) al Campus central. |
| Armería | Enlace inalámbrico al Campus “El Crucero” |
| Campus San Pedrito | Enlace inalámbrico a Comercio Exterior (Valle de las Garzas). |
| Minatitlán | Infinitum |
| Cuauhtémoc | Infinitum |
| El Colomo | Infinitum |
| Albarrada | Enlace inalámbrico al Campus Villa de Álvarez |
| Comala | Infinitum |
| Campus Coquimatlán | Fibra óptica |
| Cerro de Ortega | Enlace inalámbrico al Campus “El Crucero” |
| Quesería | Infinitum |
| Santiago | Infinitum |
| Camotlán de Miraflores | Infinitum |
| Tepames | Infinitum |
| Cofradía de Juárez | Enlace inalámbrico al Campus “El Crucero” |
| Suchitlán | Banda ancha móvil |

Fuente: Propia, con base en la información de la Dirección General de Servicios Telemáticos.

Por otro lado, se tiene que en Colima, de manera general, la sociedad está familiarizada con la tecnología de los cajeros automáticos, el uso de kioscos de servicios, el manejo de la telefonía celular y residencial. Por lo que la penetración tecnológica es la adecuada, para iniciar el proceso de inducción al voto electrónico.

También la encuesta refleja que la sociedad, en general, tiene un ánimo de desconfianza de su entorno. Lo que nos indica que la inducción debe ser gradual y con elementos que sean familiares al elector.

Capítulo V.- Modelo de Seguridad para Elecciones Presenciales en el Estado de Colima.

5.1 Modelo general de seguridad.

Para la integración de la propuesta del *Modelo de Seguridad para Elecciones Presenciales en el Estado de Colima*, se ha pensado de manera integral la planeación estratégica para su diseño. De tal forma que sea incluyente, no sólo en los aspectos tecnológicos, sino que involucre desde las más altas esferas ejecutivas en el Gobierno Constitucional del Estado de Colima, Cámara de Diputados Local, pasando por los órganos electorales, hasta llegar a la sociedad y los electores. Éstos son, finalmente, a quienes deben llegar esas herramientas automatizadas, para la toma de decisiones. En particular, la democrata, para poner en puestos fundamentales y trascendentales, a las personas que han de dirigir los destinos de miles de ciudadanos.

En la Figura 5.1 se observa la descripción general que se consideró para el desarrollo del modelo. Debe ser integral en todas las aristas que se contemplen. Con la intención de minimizar los errores, tanto legal, de logística, como de desarrollo e implementación. Evaluando de manera constante su desempeño, para que sea transparente y tangible hacia todos los involucrados.

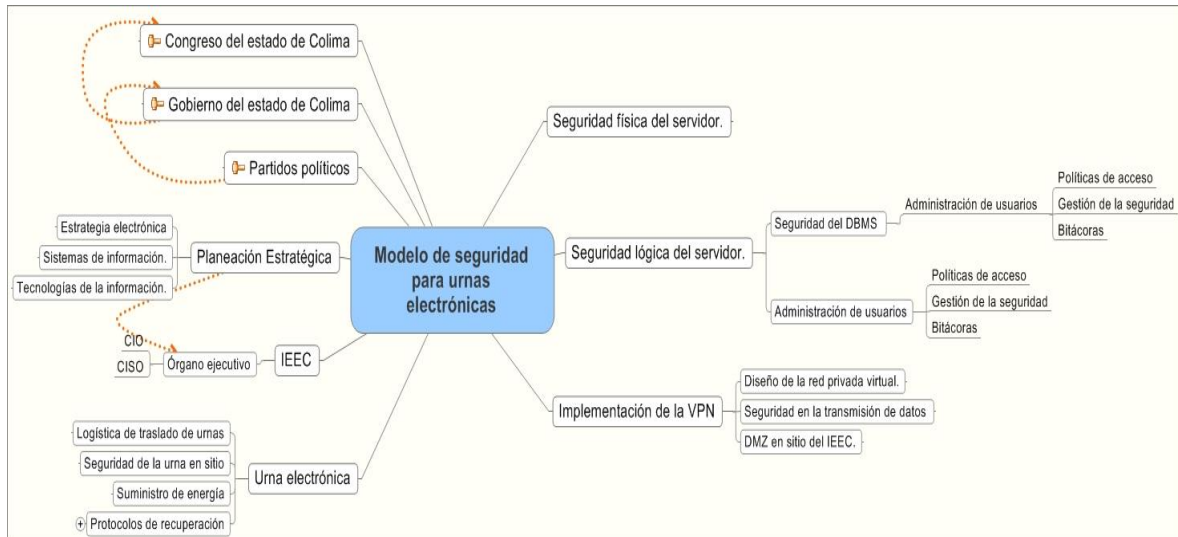


Figura 5.1. Modelo de Seguridad para Elecciones Presenciales en el Estado de Colima.

Fuente: Fuente propia, con ayuda del software Mindjet V7.

5.2 Planeación Estratégica de la Seguridad.

Toda planeación requiere de un liderazgo que conduzca a buen puerto cualquier proyecto, empresarial o gubernamental. De este liderazgo dependerá el éxito o fracaso, según se proyecte y administre. Para ello se requiere poner a las personas adecuadas, con las habilidades y características que se necesitan, para desempeñarse en el puesto o cargo.

Así pues, el hablar de liderazgo lleva implícito, no necesariamente, de un buen administrador o viceversa. Aunque en México, bajo la cultura gubernamental, como sucede por lo regular, el administrador debe ser el líder de una entidad y debe poseer las siguientes características:

- Rol informativo.
- Rol interpersonal.
- Rol decisional.

Al mencionar al líder, se deben tener en cuenta los diferentes tipos de liderazgo, que son:

- **El Liderazgo Autocrático.** Es el liderazgo que impone.

- **El Liderazgo Democrático.** Es el liderazgo que escucha. Sabe potenciar las habilidades y ventajas de cada uno de los integrantes del grupo, para tomar la mejor decisión.
- **El Liderazgo Liberal.** Aquí los integrantes del equipo disfrutan de total libertad, para la toma de decisiones. Si requieren el apoyo del líder, lo obtienen, pues se caracteriza por no hacerse presente en el grupo, tomando un rol pasivo.

Al integrar este proyecto se necesita un **Liderazgo Democrático**. Integrando las voces de todos los que participan en el proyecto. Siendo incluyente se garantiza el éxito de la implementación.

Dentro de la planeación estratégica se debe considerar que, desde las altas esferas ejecutivas, hasta los equipos operativos, deben tener claro; la misión, visión, objetivos y análisis. Todo lo anterior para que se logren las metas trazadas; a corto, mediano y largo plazo. No solamente sea, en el caso de la planeación de la burocracia en turno, o administración, por periodos de gobierno. Lo cual hace que todo el trabajo, desarrollado anteriormente, se pierda y se tenga que iniciar desde cero, por falta de planeación. O bien, por la egolatría de sus líderes, por erradicar el sello de la administración anterior e imponer el distintivo en turno, entre otros factores. A continuación se revisa, se compara y sugiere, en las diferentes esferas que competen al Instituto Electoral del Estado de Colima, para el Diseño y Planeación Estratégica de un Modelo de Seguridad Para Implementar Votaciones Electrónicas Presenciales en el Estado de Colima.

5.2.1. Gobierno del Estado de Colima y Congreso del Estado de Colima.

Para lograr el éxito en cualquiera de los proyectos de e-gobierno, se requiere que el Estado, en el Poder Ejecutivo y Legislativo, representado en el Gobierno y Congreso del Estado de Colima, respectivamente; propongan, apoyen e impulsen las leyes respectivas. Ya que se requiere una plataforma sólida de trabajo, como lo refieren las leyes que se enunciaron en el apartado 3.10.

Por lo tanto, y soportado sobre el código referido, tanto el Gobierno como el Congreso del Estado de Colima, están facultados para promover los ordenamientos legales correspondientes. En el marco de fortalecer la participación democrática, de todos los que integramos esta sociedad. Además, para implementar el voto electrónico en Colima, se requiere crear e impulsar leyes. Que incluyan conceptos, de acuerdo a la dinámica de la vida social que se tiene actualmente. Porque a pesar de que se incluyen apartados específicos, para disminuir la brecha digital, no se terminan por aterrizar correctamente los conceptos. Solamente queda como un apartado de gobierno y buenas intenciones.

Igualmente, después de la formulación de los códigos legales respectivos, se debe incluir el voto electrónico en el Plan Estatal de Desarrollo. Situación que no ha ocurrido. Si bien, se tiene un apartado de agenda digital (Numeral 154)² y se han modernizado algunas partes de la tramitología, eliminando el intermediarismo burócrata que aqueja a la sociedad, los avances no se ven reflejados en los esquemas democráticos que en la actualidad se tienen, que se demandan, por parte de la sociedad, ya que se requieren mecanismos que den certeza y claridad a los procesos democráticos.

Dicha planeación ha de requerir la ayuda de los órganos encargados de la democracia en el Estado de Colima. Por supuesto, la consulta a expertos en el área, como son; Ingenieros en Sistemas, Expertos en Planeación Estratégica, Politólogos, Expertos en Seguridad Informática, Abogados, para que se haga una correcta planeación y ejercer por este medio la democracia en la entidad.

Como se indicó en la Figura 2.2, las acciones realizadas en Japón, para desarrollar su estrategia de TI, requirió de un plan a mediano y largo plazo, para poder evolucionar y ser sustentables, con el fin de llegar a la ubicuidad electrónica, que sería el estado ideal.

² "154. Crear un Sistema digital que facilite la participación ciudadana, en los aspectos de gestión de Gobierno, tanto en propuestas como en resultados. Crear un modelo comunitario y digital que permitan la intercomunicación entre los habitantes de las comunidades del Estado, con sus familiares inmigrantes en los Estados Unidos. Diseñar y probar un modelo digital de emisión de sufragio electrónico."

Si se pensara en un punto intermedio, se tendría que recapacitar en el camino que recorrió el Estado de Coahuila, pues en esa entidad se impulsaron las acciones pertinentes. Se generó la planeación adecuada para llegar a usar la democracia electrónica, con las leyes promulgadas por el Congreso de Estado de Coahuila de Zaragoza, para tenerlo actualizado, a los tiempos que se viven en dicho lugar.

Así, con la correcta incursión de los esquemas en el Plan Estatal de Desarrollo, elaborado por el Gobierno del Estado de Colima, sustentado en las leyes respectivas que han de elaborar en el H. Congreso del Estado, se han de delegar las actividades de planeación al órgano encargado de organizar y validar las elecciones.

Para la elaboración de una correcta planificación gubernamental, a todos los niveles, se pueden tomar en cuenta las siguientes metodologías:

- Dirección de negocio.
- Análisis de las cinco fuerzas de M. Porter.
- Estrategias de mercado.
- Análisis FODA.
- E-strategy

Aunque se ha de considerar fuertemente la metodología de e-strategy, pues en todas las dependencias gubernamentales se tiene necesidad de planear, con el uso de tecnología, al estar inmersos los trámites con la firma digital. Lo anterior demuestra que sí se pueden trabajar proyectos tecnológicos, siempre y cuando existan los detonadores adecuados.

5.2.3 Órgano ejecutivo.

Queda clara la manera de cómo se elige al Consejo del Instituto, según el apartado 3.10. Lo que no queda establecido correctamente, en ningún ordenamiento, es la realización de la

Planeación Estratégica, su misión, visión y objetivos. Además, cómo los han de alcanzar y medir, teniendo como sustento determinados indicadores o estudios previamente realizados.

Asimismo, aunque el Consejo en lo general tiene experiencia en el área político-electoral, carece de algún adiestramiento o experiencia en el área de planeación. Por lo tanto, el organigrama del Instituto carece de un área especializada, a pesar de que existe una dirección de administración, según consta en el organigrama (Figura 3.11. Órganos Ejecutivos del IEEC).

Por lo que se requiere una planeación que dé certeza, de acuerdo al estandar ISO 17799-2005, para que el Instituto evolucione y no se quede en el oscurantismo, como muchas dependencias gubernamentales autónomas, o no. Lo anterior, independientemente del Consejo en turno, que debe evolucionar con directrices que hayan sido estudiadas, fundamentadas, soportadas en reglamentos y leyes. Pues con esto se dará mayor credibilidad al Instituto.

5.2.4 Director de Tecnologías de Información (*IT Director o CIO*).

En la actualidad, para el ingreso a la Sociedad de la Información, con el fin de disminuir la brecha digital, no solamente se requiere hacer decretos y leyes gubernamentales que lo establezcan. Se requiere que las dependencias se fortalezcan, con personal altamente capacitado. Que contemplen planes de capacitación para su personal ya contratado, y este es el caso, muy particular, del Director de Tecnologías de Información.

En el Instituto Electoral del Estado de Colima, como se aprecia en la Figura 3.11, existe la Dirección de Sistemas. Como tal, sólo existe una persona que funge como especialista en el área. Tiene una formación como Ingeniero en Sistemas. Es quien respalda al Instituto en todas las actividades referentes al manejo y administración de tecnología.

Al integrar la Planeación Estratégica, es deseable incorporar al organigrama, como tal, una Dirección Ejecutiva que se encargue de; planear, operar y administrar todo lo referente a la Planeación Tecnológica, como se muestra en la Figura 3.15. Esta parte del organigrama es crucial para la buena implementación, desempeño y evaluación del voto electrónico

5.3 Seguridad física de los servidores.

Para integrar la información correspondiente a la seguridad física de la urna, en un contexto amplio, se deben contemplar desde los servidores, sistemas de comunicación, algoritmos para encriptar y asegurar el voto. Seguir hasta llegar a la urna donde se va a emitir el sufragio. Se han de considerar los estándares internacionales que para el caso se aplican.

Por lo que, apoyados en el estándar del Instituto Nacional de Normas y Tecnología (*NIST*), así como de la Biblioteca de Infraestructura de Tecnologías de Información (*ITIL*), se desarrolló esta propuesta que a continuación se explica, por apartados, de acuerdo a las necesidades de Planeación, adaptándolas al entorno del Estado, procurando respetar las normas establecidas.

5.3.1 Instalaciones del Instituto Electoral del Estado de Colima (IEE).

a) Edificios.

El primer factor que se identifica es que el IEE no posee edificios con infraestructura propia. A diferencia de las otras instituciones que ya cuentan con la implementación de voto electrónico. Esto es primordial para poder instalar la infraestructura de red, aseguramiento de datos e instalaciones adecuadas para el resguardo de la información. Así como las correspondientes a las instalaciones eléctricas, para asegurar la operación de todo el equipo, tanto humano (operacional) como de infraestructura tecnológica.

El IEE ha sufrido varios cambios de domicilio. Lo que hace poco confiable que la infraestructura funcione de manera adecuada, al no tener estabilidad en su domicilio y sus instalaciones, ya que durante la gestión anterior sesionaron en el domicilio de Calzada Pedro

A. Galván 66, C.P. 28000 Col. Centro en Colima, Capital. En la transición sesionaron, con fecha al cierre al mes de octubre, en Calle Jorge Luis Borges # 1800 C.P. 28017 Col. Residencial Vista Hermosa, en Colima, Capital. Su nuevo domicilio será, a partir del 31 de octubre, en Rey Colimán 380, C.P. 28000 Colima, Centro, en Colima, Capital. Con lo anterior no es posible hacer una correcta planeación en la parte tecnológica, pues en cada cambio de domicilio se presume invertir en las adecuaciones a los edificios, para el correcto funcionamiento de la misma.

b) Suministro de energía.

El suministro de energía es uno de los riesgos críticos que se tienen, al tiempo de implementar un Plan de Tecnología, en el entorno; empresarial, gubernamental y de servicios, en general. Para cubrir este requerimiento se tienen presentes diferentes alternativas, como pueden ser:

- Plantas de Suministro de Energía.
- Unidades de Suministro Ininterrumpido de Energía (*Uninterruptible Power Supply o Uninterruptible Power Source, UPS*).
- Baterías de alto desempeño.

En el caso de las Plantas de Suministro de Energía, se tiene el inconveniente de que cuando se termina el combustible, deja de funcionar. Por lo que solamente usar las Plantas de Suministro de Energía, no garantiza el funcionamiento adecuado de los equipos de cómputo. Así como para suministrar energía a todo el complejo del IEE. Una mejor alternativa es usar unidades UPS's de una determinada cantidad de carga, que permitan desarrollar la actividad sin contratiempos. En caso de que la exigencia de energía sea prolongada, se puede contemplar el uso de Plantas de Suministro de Energía, para asegurar la integridad, en combinación con las UPS's para el desarrollo de la jornada electoral.

Otro problema que se prevé es cuando se deba suministrar energía en sitio, a las urnas, o cuando se esté desarrollando la elección. Para este caso se puede usar UPS's, además, baterías

de larga duración que permitan el desarrollo de todo el evento electoral, sin contratiempos, para así garantizar el evento democrático en turno.

c) Protocolos de recuperación.

Las Plantas de Suministro de Energía deben estar diseñadas para soportar cualquier eventualidad que ocurra durante el evento. Hay que verificar su constante monitoreo, aunque esto se puede realizar a distancia, sin la necesidad de estar en el espacio físico donde se encuentre la planta. Y para ello se deben considerar las siguientes características:

- Contenedor con caja acústica.
- Facilidad de manejo.
- Automática.
- Administración remota.
- Equipo de transferencia.
- Tableros de transferencia.
- Control y monitoreo, tanto remoto como en sitio.

El protocolo de autorecuperación de energía, preferentemente ha de ser autoadministrado por los mismos equipos, de manera autónoma. Las unidades UPS's, así como las plantas de energía, poseen puertos de administración. Por lo regular puertos DB9 que se conectan a los equipos de cómputo (servidores, pc's, etc.) que permiten autonomía en el manejo y recuperación de la energía eléctrica.

En el caso particular de los Servidores y PC's en sitio, del IEE, la combinación de las Plantas de Suministro de Energía y los UPS's hacen una mancuerna perfecta. Ya que prácticamente se

tendría controlado el suministro. El impacto de riesgo, por falta de energía, se reduciría al mínimo.

Igualmente, se deben considerar inspecciones rutinarias por los técnicos y especialistas del área, así como su mantenimiento y simulacros regulares, cuando no sea jornada electoral. Ya en el día que se lleven a cabo los comicios, previo al evento, se tendrán que efectuar las siguientes acciones:

- Simulacro de siniestro previo a la jornada.
- Dar mantenimiento mayor:
- Tener a los equipos de especialistas en alerta, para cubrir eventualidades.
- Tener a la mano; documentos, manuales operativos a la vista, así como alternativas de solución de problemas.

En cuestión de las urnas electrónicas, ubicadas en sitio donde se lleva a cabo la jornada electoral, se deben considerar:

- Empleo de UPS´s estándar de 3 horas de uso.
- Empleo de baterías de larga duración para las urnas (12 hrs).

Con lo anterior se ha de garantizar la disponibilidad de la urna durante la jornada electoral.

c) Personal adscrito.

El personal adscrito al IEE debe estar plenamente identificado, para evitar posibles infiltraciones y delitos electorales que puedan poner en riesgo la seguridad de los aspectos siguientes:

- De los sistemas.
- Del evento electoral en turno
- Robo de documentos o papelería.
- Vandalismo.

Para esto se han de usar controles biométricos, ya que estos ofrecen una alta seguridad y control, para el acceso a las diferentes áreas o departamentos del IEE. Con esto se ofrece que la garantía de acceso se pueda controlar a través de; lectura de retina, de huellas digitales o del rostro, dependiendo del nivel de acceso y seguridad que se desee para el caso.

Para una alta seguridad del control de acceso, se recomienda el escaner de iris, ya que difícilmente cambia con el tiempo, a diferencia de la huella dactilar o la geometría de la mano. Porque a ciertas personas, con el paso del tiempo, se les puede borrar la huella, en un porcentaje mínimo. Situación que también puede ocurrir en la geometría de la mano, que podría cambiar por malformaciones o enfermedades.

Por otro lado, debe considerarse el uso de controles de confianza, así como el de exámenes psicométricos, para que el personal con acceso a las instalaciones, sea el adecuado.

5.4 Seguridad lógica.

La seguridad lógica del servidor es por demás importante. Ya que si se siguen al pie de la letra las recomendaciones del Sistema de Defensa de Castillo, como se ilustra en la Figura 3.27, los efectos de un ataque pueden ser controlados y sus daños se minimizan en todo caso.

Asimismo, existen estándares que se deben implementar, como lo recomienda el NIST, ya que sin un protocolo a seguir, no se puede garantizar el buen funcionamiento de la infraestructura tecnológica. Por lo cual se deben implementar cualquiera de los siguientes estándares:

- Seguridad de la información del gobierno.
- El ISO 17799-2005.

También debe tenerse suma atención en la certificación de las diferentes áreas que lo conforman, como son; la certificación de las plataformas, operadores, sistemas de cableados y todos los componentes de la infraestructura tecnológica.

5.4.1 Seguridad del servidor.

La seguridad del servidor es una de las partes medulares de los sistemas de información, por lo que es apremiante que el protocolo de seguridad del servidor se lleve con estricto seguimiento.

Para lograrlo se deben implementar las siguientes acciones:

Para el acceso en sitio del servidor, se debe acceder por medios biométricos, preferentemente estables, ya que esto garantiza el ingreso del operador a las instalaciones. Igualmente, la autenticación al sistema se debe apegar al estándar del NIST 800-12, ya que establece claramente la asignación de; responsabilidades, roles, actividades y manejo de riesgo. Los cuales deben tomarse en cuenta, para que la seguridad de los diferentes tipos de servidores sea afectiva y se minimice el impacto en caso de alguna eventualidad.

Cabe señalar que el NIST tiene sus propios estándares, para los diferentes sistemas, como son; Unix, Microsoft Windows Server, Apple y Novell. Por lo que se deberá, para esta implementación en particular, señalar el estándar de Unix y en su defecto, para las cuestiones periféricas, si se requieren remitirse al estándar adecuado.

a) Administración de usuarios.

La administración de usuarios, por lo regular, es uno de los puntos más importantes para todo sistema informático. Se debe poner especial atención en la forma y manera que los usuarios (personal adscrito al IEE) acceden al sistema. En caso de operadores, se deben ajustar a los estándares que sus roles demandan, pero en el caso particular de los electores, que son catalogados como usuarios ocasionales, ellos no acceden de manera consuetudinaria al sistema. Por lo cual se deben asignar permisos temporales, por jornada electoral, además de aplicar ciertas reglas especiales de operación, que se ajusten a los estándares del sistema en uso.

Tanto en los servidores de Microsoft, como en los de Unix, existen plantillas para administrar correctamente a los usuarios, de manera remota y local. Lo anterior, aplicando las políticas y modos de acceso a los clientes disponibles, como se describió en el apartado 3.11.7

b) Políticas de acceso.

El control de acceso va estrechamente ligado a la administración de usuarios, para proteger la información, ya que de ello dependen los permisos que se otorguen a los usuarios, al momento de operar los equipos de; cómputo, terminales y servidores.

Existen dos maneras de acceder a los equipos de cómputo. La primera que ha tenido un alto impacto en la actualidad, son los controles biométricos, que pueden ser incluidos como parte del hardware que integra la computadora, o añadiéndolo como periférico. Teniendo como fundamento que sólo la persona habilitada puede acceder.

La otra alternativa que se considera, para este proyecto, es generando una clave de usuario que, por lo regular, son las que a corto y mediano plazo desaparecerán. Por lo que, para esta implementación, se ha de considerar el control biométrico de las huellas dactilares, como se enunció en el apartado 3.11.7.

Las siguientes son políticas obligatorias que han de establecerse para controlar a los usuarios:

- i. Restringir el acceso vía remota.
- ii. Aplicar las correspondientes listas de acceso, sólo al área de sistema que ha de modificar. En este caso, su acceso al voto y en su caso, verificación del sufragio.
- iii. Temporalizar el ámbito del acceso de los usuarios por:
 - a. Día.
 - b. Horas.
 - c. Cantidad de accesos.
 - d. Terminales desde las cuales han de acceder.
 - e. Direcciones IP (Direcciones lógicas de internet) administradas vía dirección MAC (Direcciones físicas de las tarjetas de red) desde las cuales acceden.
- iv. En caso de funcionarios que accedan desde varias terminales, indicar bajo qué condiciones acceden.
- v. Si se accede a zonas de alto riesgo, se debe acceder con los protocolos adecuados o software, que permita establecer conexiones seguras como son las VPN's.

c) Gestión de la seguridad.

La gestión de la seguridad queda enmarcada en los roles que asignan; el estándar del NIST, el ISO 17799-2005, así como el ISG. En particular, para el voto electrónico, se ha de contemplar la seguridad biométrica que ya se ha señalado en el apartado 3.11.7, considerando que muchas personas tienen capacidades diferentes. Por eso se han de especificar ambos esquemas, tanto el de huellas dactilares como lectura del iris, a juzgar por lo siguiente:

Muchas personas en el Estado de Colima carecen de algún miembro (ojos, manos, piernas) por lo que es indispensable contar con ambos esquemas para ser incluyente y así todos puedan participar. En el caso particular del voto, se insiste en el uso de controles biométricos, pues se distingue por estar basado en teorías del caos y prácticamente es imposible que con este tipo

de seguridad sea afectado el voto de las personas, a favor de alguien por quien no fue considerado por el elector.

5.4.2 Servicios de red.

La infraestructura de los servicios de red forman parte importante para la emisión del voto electrónico, pues se considera que ha de montarse sobre la infraestructura de la Universidad de Colima. Lo anterior por su impacto y alcance en la región, como se señaló en la Figura 4.1

1. Zona Desmilitarizada (DMZ) de la red.

La Zona Desmilitarizada de la red debe ser cuidada al extremo, pues es la parte de la red que está en comunicación con los diferentes entes que quieran acceder a los resultados, como son:

- Partidos políticos.
- Medios de comunicación.
- Organizaciones no gubernamentales.
- Tribunal electoral
- Otras entidades que previamente sean autorizadas para tal efecto.

Los puntos de acceso se han de tener en puertos muy específicos, similares a los puertos públicos. Además de tener definidas las listas de acceso por dirección IP, para un mejor control de los clientes que acceden a la información establecida en el servidor. Toda la gestión de tráfico se ha de realizar a través de un firewall, de alto rendimiento, con sus propias políticas de acceso; entrada, salida, redireccionamiento y bloqueo. Así como un control de acceso por usuario.

El único personal que puede ingresar al segmento de esta área, son quienes fungen con rol de administrador.

Otra alternativa a la distribución de datos es por medio de uso de una VPN, para protección de los datos, sin exponerlos, o bien, por una DMZ, para garantizar el control de acceso, usando las mismas políticas de control de acceso y usuarios, mencionadas antes, en el apartado 5.4.1.

2. Diseño de la Red Privada Virtual.

La Red Privada Virtual es la mejor manera de esconder los datos en una red pública, como lo es la red de la Universidad de Colima. El uso del protocolo SSL soporta el encapsulamiento adecuado, para poder transmitir la información de la urna electrónica, sin contratiempos. El único usuario habilitado para iniciar la conexión, es el presidente de casilla, a través de una tarjeta o control biométrico, con códigos que habilite el cliente de la VPN.

El diseño de la VPN ha quedar conformado de la siguiente manera como se ilustra en la Figura 5.2:

- Uso de un servidor de VPN.
- Cliente de OVPN por software.
- Uso de tarjeta inteligente o control biométrico, para habilitar el inicio/cierre de transacciones entre clientes y servidor.

Con lo anterior se protegen los túneles de transmisión, quedando identificado el proceso y usuario que lo disparó.



Figura 5.2. Red de comunicación para la urna electrónica.

Fuente: Propia, diseñada con SmartDraw.

3. Seguridad en la transmisión de los datos.

La seguridad en la transmisión de los datos queda conformada de la siguiente manera:

- i. Control de acceso a la red por medios biométricos, o en su defecto, una tarjeta inteligente que habilite la casilla, para registrar al usuario que ha de efectuar los siguientes movimientos:
 - ✓ Arrancar.
 - ✓ Iniciar el software de la casilla.
 - ✓ Iniciar los contadores de voto local.
 - ✓ Cerrar los contadores de voto local.
 - ✓ Cerrar el software de casilla.

- ✓ Cerrar la casilla electrónica.

- ii. Control del elector por medios biométricos. El control biométrico, por usar teoría de caos, genera una llave única por usuario, permitiendo que solo un usuario emita su voto. Por lo cual se toma esta llave para encriptar/desenscriptar la información, de punto a punto y contabilizar de manera efectiva el voto.

- iii. Control de acceso al medio, implementado sobre la red de la Universidad de Colima, donde se establece la administración de conexiones, por medio del control de direcciones físicas de red (MAC). Asimismo, sobre la red de la Universidad se implementa la VPN, que usa SSL para asegurar la conexión entre el cliente y el servidor.

Con lo anterior, se tiene pleno control de la transmisión, emisión y control de cifrado de los datos.

5.5 Urna electrónica.

La urna electrónica será la interfaz con la que el elector ha de interactuar. Por lo que es importante, en este punto, más que la seguridad, los diferentes elementos que la integran de manera visual, como son:

- Interfaz intuitiva.
- Agradable a la vista.
- Que sean fácil de localizar los elementos.
- Hacer uso de la ley Fitt.
- Minimizar los distractores que pudiera haber en la aplicación.

Igualmente, es importante destacar la logística de traslado, el suministro de energía y los protocolos de autorecuperación. Ya que de manera particular, en estos elementos ha de soportarse la integridad de la seguridad física y su buen funcionamiento.

5.5.1 Logística de traslado de la urna.

La logística de traslado de la urna ha de ser un factor importante, para que se logre la transparencia que se requiere. Por lo que al trasladarla a sitio, se ha de seguir el siguiente procedimiento:

- Selección aleatoria de las urnas. Con esto se asegura que ninguna urna estará truqueada o previamente preparada.
- Al equipo de logística, hasta media hora antes, se le otorgará la lista de las urnas, el distrito, sección y domicilio exacto al que corresponde.
- En su instalación se ha de realizar una inspección visual, de que no contenga periféricos no autorizados, memorias que no correspondan al equipo y en general, solamente sea instalado el equipo que corresponda con la lista de hardware emitida por el IEE.
- Al reconfigurar la Dirección de Tecnologías de la Información, se conforma un equipo especial para la jornada electoral, que ha de estar capacitado para la instalación y recolección de las urnas electrónicas.
- Se ha tener especial atención de que todas las urnas electrónicas estén:
 - Limpias de marcas o leyendas, que puedan causar sospechas de algún manejo por parte del equipo de logística.
 - En todo caso sólo las marcas que autorice el IEE.
- Cuando se termine la jornada electoral, las urnas serán resguardadas por la seguridad que en su momento designe el IEE, listando las siguientes actividades:

- Urnas limpias de marcas o leyendas, que puedan causar sospechas de algún manejo por parte del equipo de logística.
- Nadie está autorizado a mover, modificar o alterar las urnas, sin consentimiento expreso de la autoridad competente.

Lo anterior ha de garantizar su buen manejo y traslado.

5.5.2 Seguridad de la urna en sitio.

Para la seguridad de la urna en sitio, se consideran las siguientes recomendaciones:

- A partir de que la urna sea entregada, a la mesa correspondiente, la seguridad de la urna recae en los titulares de la mesa señalada. Así como en los representantes de partidos políticos y observadores electorales.
- La seguridad es corresponsable de todas las autoridades de la mesa electoral en turno. Así como de los observadores y representantes de los partidos políticos.
- Se considera el uso de sujetadores especiales para las urnas y dispositivos, los cuales sólo podrán ser manipulados por el equipo de logística del IEE.
- Cualquier anomalía se ha de reportar a la autoridad correspondiente, para evitar especulaciones y disturbios.

Es importante remarcar que a los responsables de las mesas se le debe ofrecer una especial capacitación, para el manejo de conflictos con las urnas. En todo momento el IEE ha de colaborar de manera estrecha con ellos.

5.5.3 Suministro de energía.

El suministro local de energía, para las urnas en sitio, es el proporcionado por la Comisión Federal de Electricidad, que es de 110 V. Igualmente, se ha de procurar que las instalaciones se encuentren en perfectas condiciones, evitando los aspectos siguientes:

- Cables mal presentados.
- Cables expuestos.
- Clavijas o enchufes en mal estado.
- Extensiones oxidadas.
- Sobrecarga de las instalaciones.
- Suministro correcto de la intensidad de la energía (Ampere).

El suministro ha de estar supervisado con antelación y debe cumplir con los requerimientos señalados, para evitar daños a la urna electrónica.

5.5.4 Protocolos de autorecuperación.

Durante el arranque de la urna electrónica, se requiere tener la disponibilidad de lector biométrico de retina. Pues este lector ha de permitir validar al presidente de casilla, quien es el único autorizado para iniciar los trabajos en la urna, sobre todo al empezar la operación del sistema operativo que esté instalado. De allí que su arranque debe ser autónomo, por medio del siguiente proceso:

- Para iniciar el arranque del programa, se activa con la huella dactilar de dos personas de la mesa electoral. Aunque todas las personas deben haber dado de alta sus huellas dactilares, para en caso de una sustitución, quede habilitada como alternativa otra persona. Como lo indica uno de los reglamentos operativos de las mesas de trabajo electorales (sustitución de funcionario).

- Con el uso de tarjetas previamente preparadas, con códigos de barras o el uso de lectoras de huellas dactilares, se prepara previamente para la operación de la urna y así evitar la interacción directa, en lo posible, con la urna. Dichas operaciones son:
 - Inicio del programa para captura de voto (casilla electrónica).
 - Inicio del protocolo o de contabilización de votos. Debe arrancar en cero e imprimir este saldo.
 - Cierre de casilla. Debe totalizar la urna los votos, por casilla en turno.
 - En caso de cierre inesperado de casilla, se debe habilitar, por medio de este procedimiento, el protocolo de dos fases de administración de bitácoras de procesos, para saber que los votos previos fueron correctamente contabilizados
- Los protocolos de autorecuperación deben generar una bitácora de todas las operaciones realizadas, para su posterior revisión.
- En caso de fallo definitivo, se debe dictaminar por parte del Colegio Electoral un protocolo alternativo, con uso de papel para mitigar la jornada pendiente.

Así pues, se debe destacar que no existe dispositivo que sea etiquetado con cero errores, o con una tasa cero de fallas. Por lo que todo protocolo y dispositivo es perfectible. Pero con el uso de la experiencia, como lo han hecho en otras democracias, se ha ido mejorando todo el aspecto de la participación electrónica.

5.6 Bitácoras de servicio.

Las bitácoras de servicio se deben contemplar en cada uno de los equipos de servicios, que se proveen para la seguridad y como se indican a continuación:

- Equipo que provee el servicio de la VPN.
- Equipo que sirve para autenticación de usuarios.
- Equipos que contiene la base de datos de los electores.

- Equipo que contiene la base de datos biométricos.

Las bitácoras de servicio tienen la peculiaridad que señalan, en tiempo real, el comportamiento de los sistemas. Cada acción que se dispara, lleva detrás otras más, por lo que es detectar el, o los posibles errores, o intentos de secuestro del sistema.

Asimismo, las bitácoras de servicio han de contemplar ciertos procesos, como se mencionó en el estándar NIST e ITIL, para mantenimiento y aseguramiento del desempeño:

- Mantenimiento preventivo y correctivo de los equipos. Cuando no sean tiempos electorales, cada mantenimiento debe ser programado con seguimiento en las bitácoras.
- Test de rendimiento de los equipos y en su caso, sustitución de equipo, presumiblemente bajo de performance.
- En el caso del mantenimiento de los servicios de red se contempla:
 - Manejo de las simulaciones de ataques al vuelo de los servicios.
 - Manejo de las simulaciones en el manejo de riesgos.
 - Manteamiento general a los usuarios integrados y temporales.

Todas las acciones antes señaladas se tienen contempladas para que, independientemente de quién realice la actividad, quede por escrito y tenga el mapa completo de las intervenciones que se tienen en todas las operaciones.

5.7 Auditorías.

Las auditorías tienen como objetivo hacer un trazado de los eventos que han ocurrido, en caso de pretender detectar alguna anomalía o revisión de algún proceso determinado.

Para realizar la auditoría se requiere:

- a. Autorización ejecutiva del Consejo del IEE.
- b. Presencia de los representantes de partidos políticos involucrados.
- c. La ejecución por parte de un auditor certificado para los efectos.
- d. Presencia controlada de las ONG's. Para tal caso se deben emitir los reglamentos respectivos, por parte del IEE, para su presencia y forma de actuar.
- e. La designación de expertos informáticos, por parte de los partidos políticos, sin que ellos puedan manipular el equipo. En todo caso, cuestionar las formas y métodos, procesos y actividades del sistema, a cargo de técnicos especializados por parte del IEE.

5.7.1 Auditorías de software.

El software lo componen tres partes que deben ser reguladas:

1. Programación y diseño de la interfaz.
2. Programación de los procesos internos.
3. Programación del entorno y políticas de conexión.

La acreditación respectiva se puede obtener de los laboratorios de acreditación, a través de su Programa Nacional Voluntario de Acreditación de Laboratorios (National Voluntary Laboratory Program, NVLAP). En este caso es la norma norteamericana, o se puede hacer uso también de la norma europea, de acuerdo a la recomendación Rec (2004) 11.

En lo que se refiere a la auditoría por parte de los partidos políticos y ONG's, una vez obtenida la acreditación por parte de los organismos acreditadores, aquellos sólo podrán auditar su operación. Sin que puedan revisar códigos o diseños. Igualmente, podrán sugerir ajustes menores, sujetos a aceptarse, o no, por parte del Consejo del IEE. Previa consulta de expertos del área o comisión respectiva, emitiendo la justificación y soporte indicado.

5.7.2 Auditorías de seguridad.

Las auditorías de seguridad han de referirse a la revisión de las diferentes formas de ataque, que pueden darse en un entorno agresivo, como lo es la red internet, para lo cual se harán pruebas previas al pilotaje.

Ya establecidos los previos de la seguridad de procesos menores (no vinculantes), a mayores (vinculantes), se han de ir adecuando los entornos y condiciones. Los cuales pueden ir siendo revisados en los siguientes procesos, sin que ello involucre saber el sufragio de los electores.

- a) Progreso de las elecciones.
- b) Apertura de conexión cliente-servidor
- c) Cierre de conexión cliente-servidor.
- d) Tipos de conexiones.
- e) Tiempo de las conexiones.
- f) Auditar procesos de mesa de casilla.
- g) Auditar procesos del IEE; tiempo, bitácora de usuario.
- h) Bitácoras de las bases de datos
- i) Bitácoras del firewall
- j) Bitácora de la VPN.

Las condiciones de la auditoría son similares a las mencionadas en el punto anterior. Esto, para seguridad y garantía de todos los participantes.

5.7.3 Auditorías generales.

Las auditorías generales del proceso se deben contemplar como una manera de integrar las que se enumeran en el proceso informático, como lo son:

- Selección de urnas de forma aleatoria para el proceso en cuestión.

- Entrega-recepción de urnas en sitio.
- Selección del porcentaje de urnas para su auditoría interna, pre y post proceso electoral.
- Auditoría del proceso de selección del personal.
- Auditoría de certificación de habilidades informáticas del personal contratado.

Todo lo anterior debe certificar el proceso electoral y su nivel de automatización.

5.8 Evaluación y desempeño del modelo, usando Cuadro de Mando Integral (*Balanced Score Card*).

El Cuadro de Mando Integral, como se refirió en el punto 3.13 del Cuadro de Mando Integral, conocido como *Balanced Score Card (BSC)*, es la herramienta que evaluará el desempeño de la seguridad de las urnas electrónicas. Ya que existen estándares establecidos para evaluar la seguridad de todos los elementos de seguridad informática. A continuación se muestran las figuras con los indicadores respectivos.

La Figura 5.3 muestra los indicadores para la Seguridad de las TI, la cual señala los siguientes:

- 1) Gestión de riesgos.
 - a) Plan de seguridad.
 - b) Controles de seguridad.
- 2) Planes de contingencia.
 - a) Frecuencia de respaldo.
 - b) Capacidad de respuesta.
- 3) Ciclo de vida del sistema.
 - a) Requerimiento OBM.
 - b) Seguimiento de auditorías.
- 4) Personal de seguridad.

- a) Concientización de la seguridad.
 - b) Control de accesos lógicos.
- 5) Integridad de los datos.
- a) Control de acceso lógico.
 - b) Protección de antivirus y anti espía.

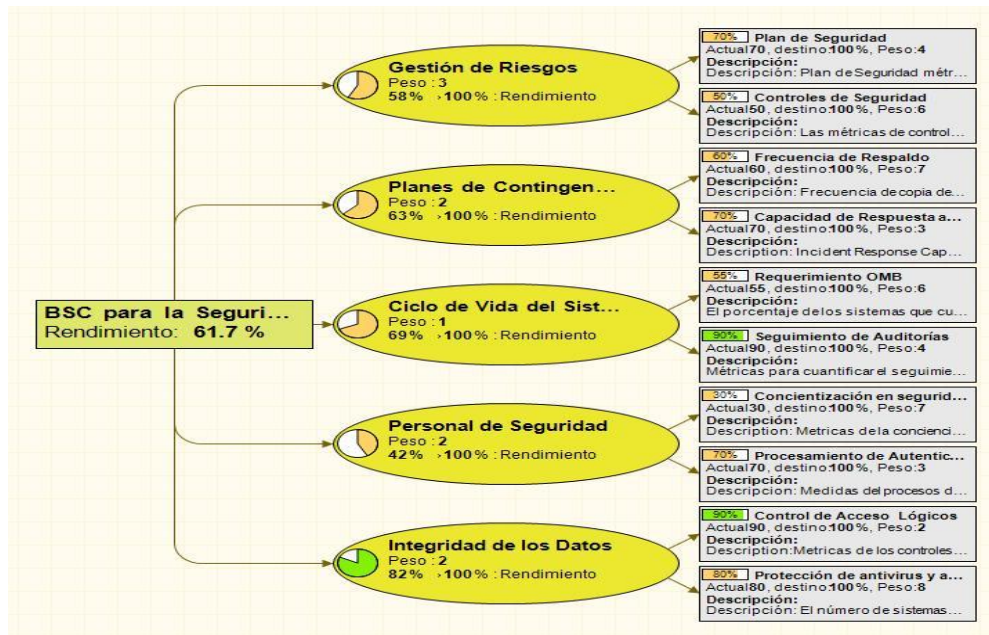


Figura 5.3. BSC para la Seguridad de las TI.

Fuente: Elaboración propia, con ayuda del software BSC Designer.

La Figura 5.4 muestra los indicadores para la Prevención y Detección de Intrusos, la cual señala los siguientes:

Seguridad de las TI, la cual señala los siguientes indicadores:

- 1) Perspectiva de los criterios de selección.
 - a) Relación de Confianza.
 - b) Índice de Escalabilidad.
 - c) Cociente de Interoperabilidad.
 - d) Índice de Compatibilidad.

- 2) Perspectiva Funcional
 - a) Tiempo de respuesta.
 - b) Fracción de los acontecimientos, en los cuales fueron tomadas medidas dentro del calendario demandado.
 - c) Disminución de la "La frecuencia de los ataques".
 - d) Proporción 'Frecuencia de Alertas'.
 - e) Relación de cumplimiento de las funciones.
- 3) Perspectiva Operacional y de Resultados.
 - a) Número de Tecnologías Implementadas.
 - b) Grado de Integración.
 - c) Preestablecer los objetivos de la reunión.
 - d) Costo: Razón del Beneficio.
- 4) Perspectiva de Evaluación del Sistema.
 - a) Proporción de Éxito.
 - b) Frecuencia de actualización.
 - c) Grado del Servicio.
 - d) Índice de Familiaridad de la Interface.

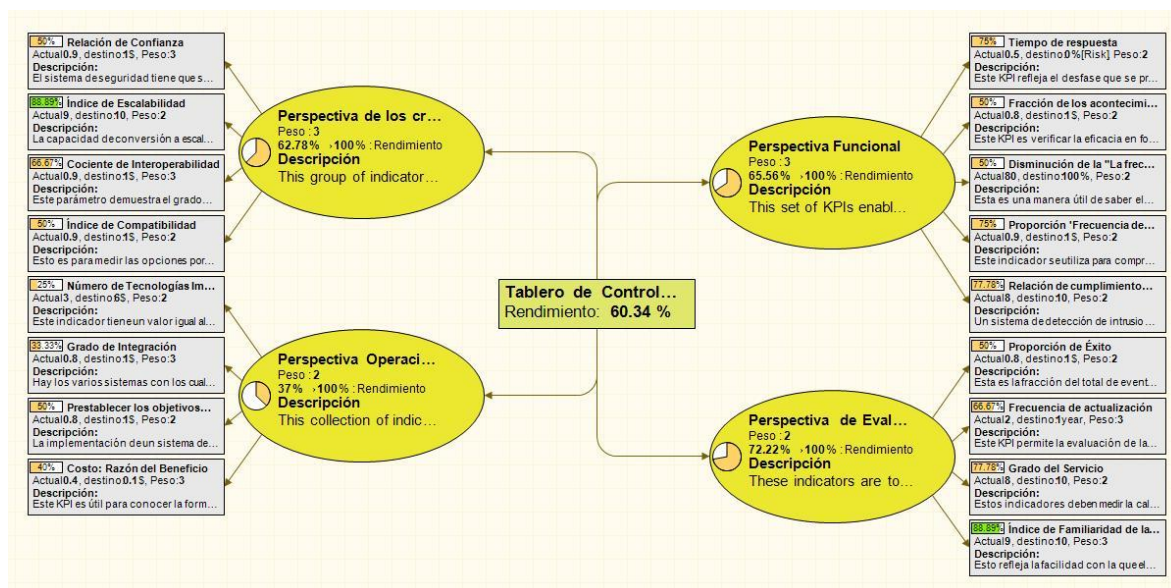


Figura 5.4. BSC para prevención y detección de intrusos.

Fuente: Elaboración propia, con ayuda del software BSC Designer.

La Figura 5.5 muestra los indicadores de BSC, para la Privacidad y la Identidad, la cual señala los siguientes:

- 1) Protección de la Computadora.
 - a) Cumplimiento del Sistema.
 - b) Incidente Forense.
- 2) Estructura de la Identidad de Información.
 - a) Tamaño del Repositorio de Identidad.
 - b) Objetos Asegurados.
 - c) Cobertura de proceso del aprovisionamiento.
 - d) Seguridad de la Identidad.
- 3) Proceso de Eficiencia.
 - a) Eficiencia de los procesos de aprovisionamiento.
 - b) Autorización de las reclamaciones.
 - c) Reclamaciones Sensibles.
 - d) Aprovisionamiento.
- 4) Efectividad del Personal.
 - a) Estadísticas de Cuentas de Usuario.
 - b) Fortalezas de las Pruebas de Identidad.
 - c) Auditoría de uso del sistema.
 - d) Cumplimiento de las políticas.
- 5) Perspectivas Financieras.
 - a) Retorno de la Inversión de Seguridad.
 - b) Daño Colateral Potencial (CDP).

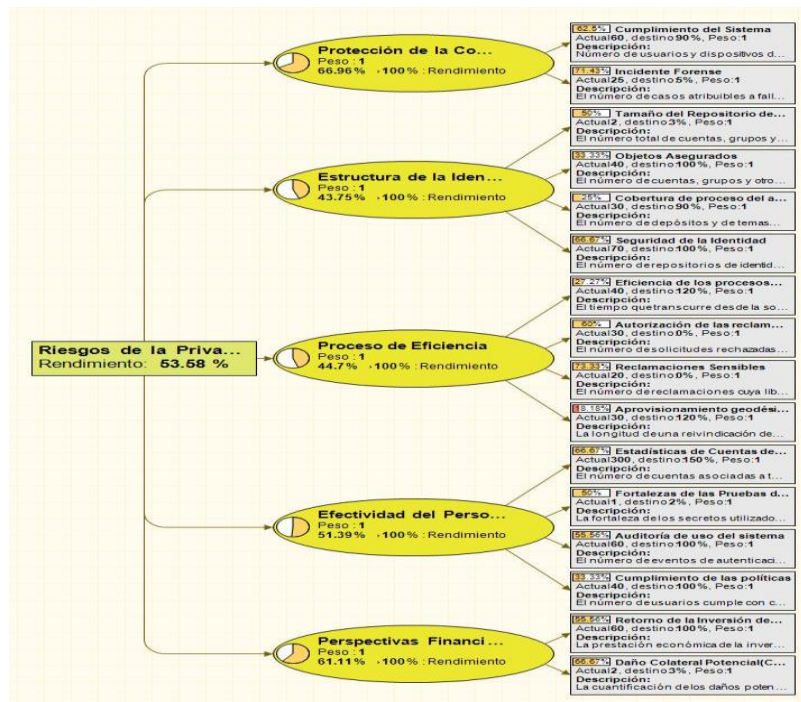


Figura 5.5. BSC para la Privacidad de la Identidad.

Fuente: Elaboración propia, con ayuda del software BSC Designer.

La Figura 5.6 muestra los indicadores de BSC, para la Seguridad y la Privacidad, la cual señala los siguientes:

- 1) Perspectiva Financiera.
 - a) Valor en Riesgo.
 - b) Retorno de Inversión.
 - c) Daño Colateral Potencial (CDP).
- 2) Perspectiva del Empleado.
 - a) Cumplimiento de Usuario.
 - b) Actitud de los Empleados.
 - c) Sensibilización de los empleados.
 - d) Eficacia de las Claves.
- 3) Cumplimiento de la seguridad.

- a) Nivel del Servicio del Sistema.
- b) Nivel de Servicio de la Red.
- c) Dispositivos Compatibles.
- 4) Historia de Incidentes.
 - a) Número de Compromisos.
 - b) Impacto en la Organización de los Compromisos (Incidentes).
 - c) Accesos no Autorizados.
 - d) Virus Detectados.
- 5) Eficacia de las políticas de seguridad.
 - a) Conteo de Vulnerabilidad.
 - b) Incidente Forense.
 - c) Tiempo de Reparación.

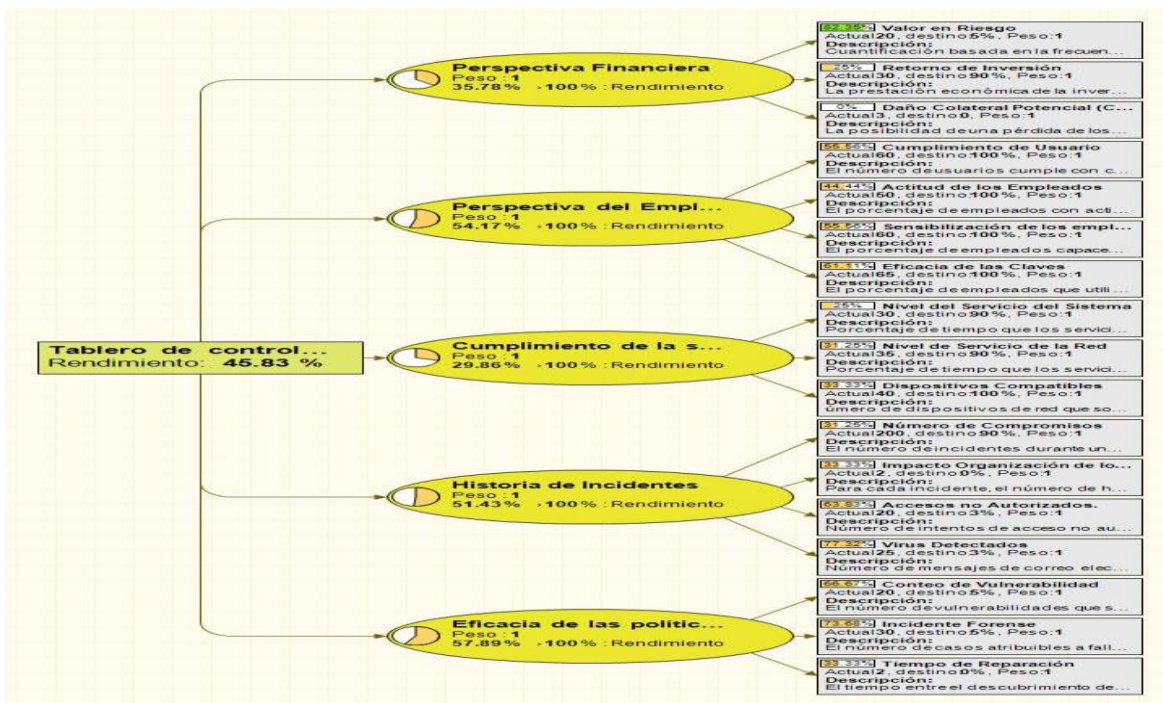


Figura 5.6. BSC para la Seguridad y Privacidad.

Fuente: Elaboración propia, con ayuda del software BSC Designer.

5.9 Conclusiones.

En la actualidad, los sistemas electorales deben estar a la altura de lo que requiere la ciudadanía, sus modos y estilo de vida. Porque la emisión de un sufragio, en un mundo tan globalizado y dinámico, no debe estar limitado o sujeto a la movilidad del ciudadano; si vive, trabaja, se traslada, o no, a un determinado lugar.

Por otro lado, se debe considerar una correcta planeación estratégica de los medios tecnológicos. Que se han de usar para que esto se lleve a cabo de manera precisa y sin errores. Pero sobre todo segura. Así, los sistemas de urnas electrónicas deben ser flexibles. De acuerdo a su entorno, modificables, para que al mismo tiempo que se reconocen en su comunidad, considerando las necesidades del momento, se vuelvan autónomos en su operación. Lo anterior, para minimizar las sospechas y suspicacias de posibles eventos fraudulentos.

Con lo anterior, estos sistemas electorales deben ser auditables en cada aspecto de su operación. También deben tener esquemas que evalúen el desarrollo y desempeño de un proceso electoral, considerando los siguientes componentes:

- Su logística.
- Desempeño del sistema.
- Usabilidad.
- Facilidad de uso.
- Seguridad.
- Personal adscrito.
- Autonomía.
- Manejo y solución de conflictos.

Con estos puntos se puede obtener un sistema seguro, bien planeado y sustentado. Para que al final de cualquier jornada electoral, queden los interesados, sin duda, de que el proceso fue honesto y transparente.

Análisis de Resultados.

En el Estado de Colima, de acuerdo a su geografía, es posible implementar un sistema de voto electrónico. Aunque esto debe llevarse en una correcta planeación estratégica, para que el proceso de inducción sea de modo paulatino, sin exabruptos y lo acepten los electores, a partir del sustento legal que se le dé en las altas magistraturas estatales.

Lo anterior es sustentado por el nivel escolar que presentó la población, como se indicó en la Gráfica 4.3, que arrojó un promedio del 52.98% con Bachillerato y un 23.82% con estudios de Licenciatura. Lo que permite tener una población preparada e informada.

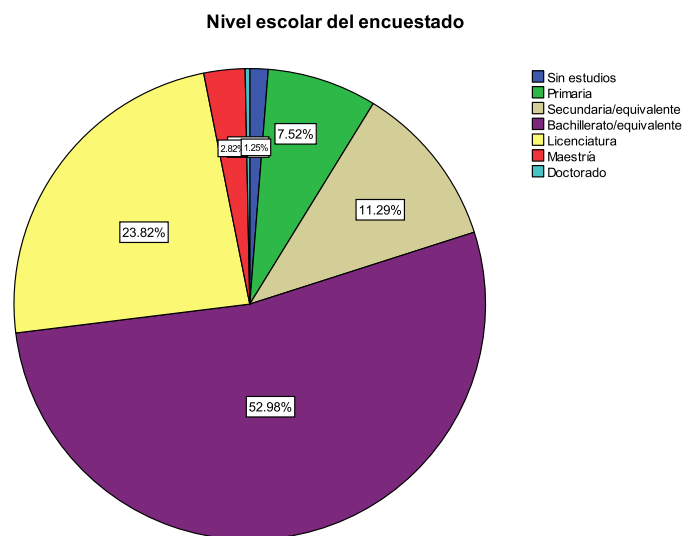


Gráfico 4.3. Edad del encuestado.

Fuente: Propia, con apoyo del SPSS.

Por otro lado, se tiene que en general la población cuenta con una confianza relativa en los cuerpos de seguridad. Como lo ilustra la Gráfica 4.4 con un porcentaje del 68.33%. Lo anterior debido al aire de inseguridad que se respira en los medios y la vida nacional.

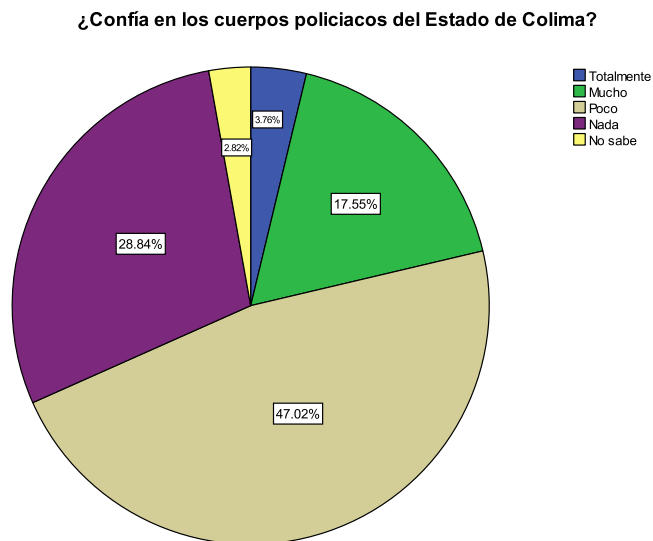


Gráfico 4.4. Confianza en los cuerpos de seguridad.

Fuente: Propia, con apoyo del SPSS.

En cuanto a la confianza que se tiene en su entorno comunitario y medios de comunicación, se manifestaron en un 84.33% y 88.71% en las Gráficas 4.5 y 4.6, respectivamente. Lo anterior es alentador, pues en Colima la sociedad se conoce y ubica a los miembros que lo integran. Lo cual arroja que en las anteriores votaciones fueron pocos los problemas que se suscitaron en las mesas electorales.

¿Confía en la gente que acude a rendir culto en la iglesia de su preferencia?

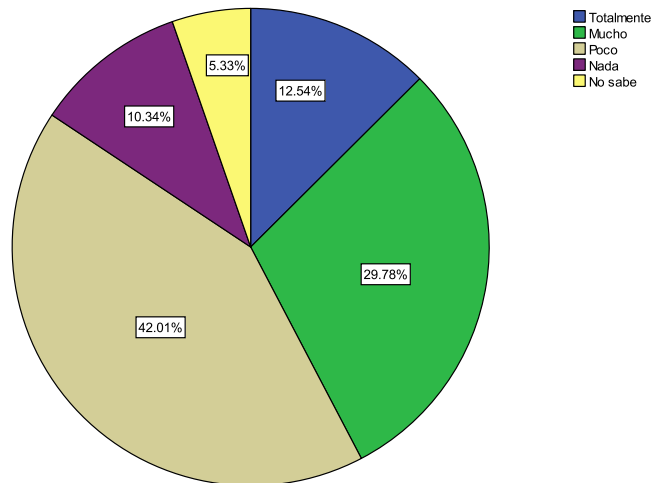


Gráfico 4.5. Confianza en los miembros de su culto.

Fuente: Propia, con apoyo del SPSS.

¿Confía en los medios de información local (radio, televisión, prensa)?

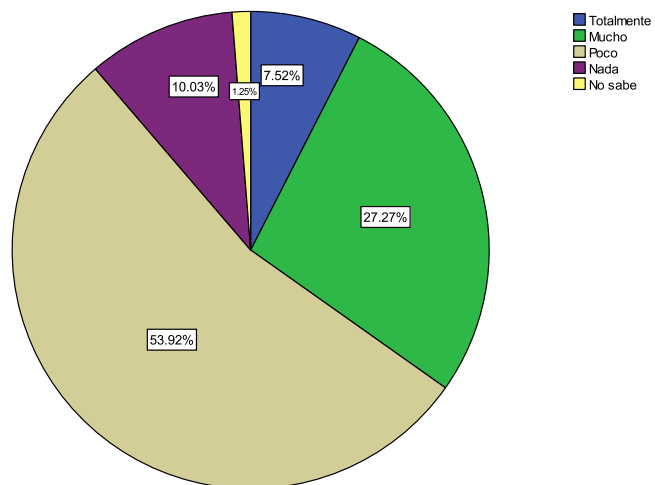


Gráfico 4.6. Confianza en los medios de información.

Fuente: Propia, con apoyo del SPSS.

Si se observa las Gráficas 4.7 y 4.8, el acumulado de confianza hacia los proveedores de Internet y Telefonía, de poco a totalmente, es del 63.01% y 78.06%. Lo anterior es el reflejo de la compañía dominante en el entorno, que es TELMEX. Aunque ha mejorado su calidad en el servicio, aún existen áreas de oportunidad para la empresa.

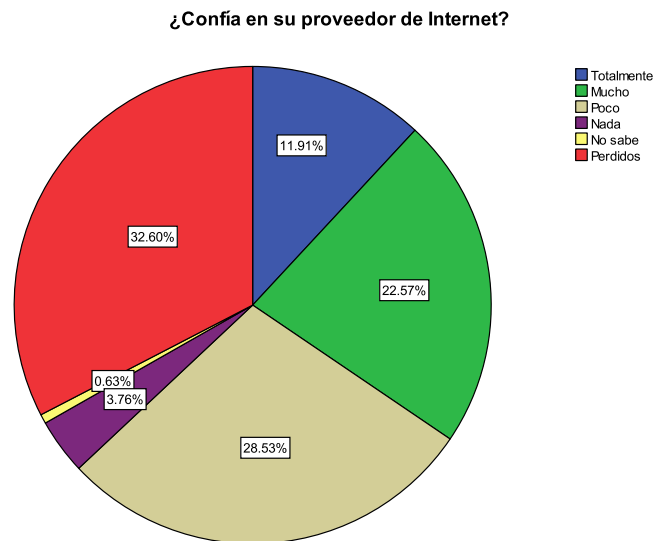


Gráfico 4.7. Confianza en el proveedor de Internet.

Fuente: Propia, con apoyo del SPSS.

¿Confía en su proveedor de telefonía?

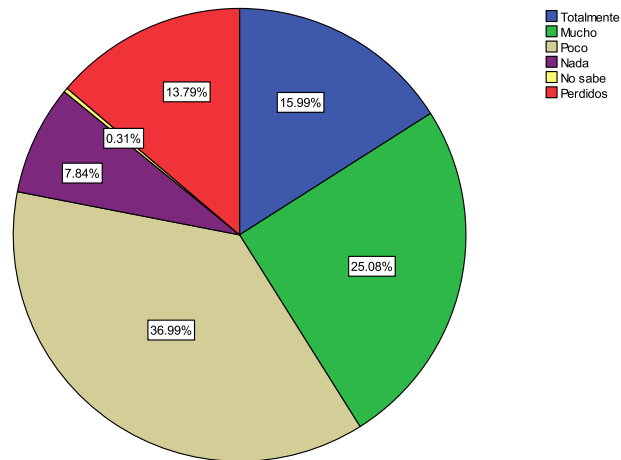


Gráfico 4.8. Confianza en el proveedor de Telefonía.

Fuente: Propia, con apoyo del SPSS.

En cuanto a la manera en que las personas se familiarizan con la tecnología, las personas mostraron mucha afinidad y confianza en el uso de cajeros automáticos, como lo refleja el resultado de la Gráfica 4.10, con un porcentaje del 83.38% en la confianza acumulada.

Indique el grado de confiabilidad que tiene usted en las operaciones bancarias que se realizan a través de los cajeros automáticos

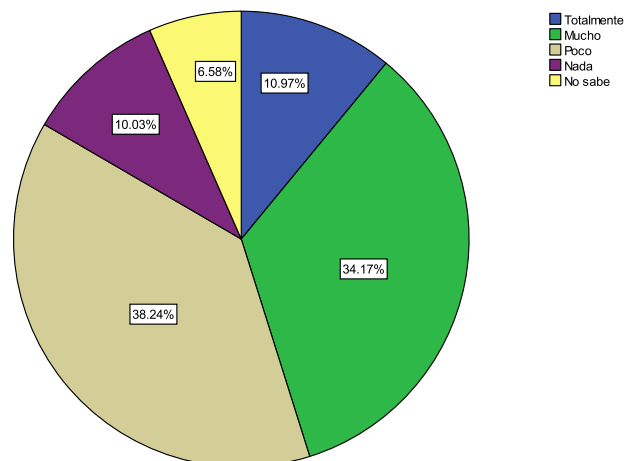


Gráfico 4.10. Grado de confianza en las operaciones bancarias, usando cajeros automáticos.

Fuente: Propia, con apoyo del SPSS.

Asimismo, la sociedad en Colima tiene, en general, aprecio por el uso de la tecnología y las comunicaciones, como lo arrojó el dato de las Gráficas 4.11 y 4.12, con un 87.46% y 80.88%, respectivamente. Este porcentaje permite tener una visión alentadora de la introducción de las urnas electrónicas, pues entre más familiarizadas estén las personas, con el uso y manejo de las TIC's, menos será el tiempo de adopción de las urnas electrónicas, su manejo y operación.

¿Tiene acceso a una computadora? (Si la respuesta es NO, especifique la razón y pase a la pregunta 37)

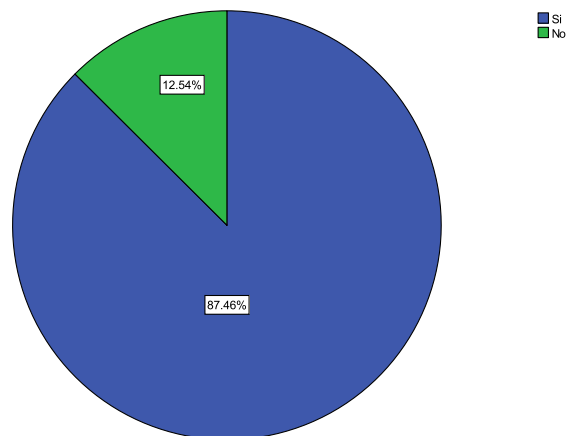


Gráfico 4.11. ¿Tiene acceso a una computadora?

Fuente: Propia, con apoyo del SPSS.

¿Utiliza alguna cuenta de correo electrónico?

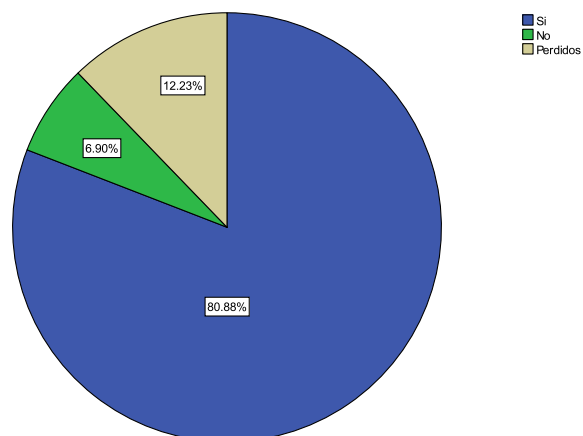


Gráfico 4.12. ¿Utiliza alguna cuenta de correo electrónico?

Fuente: Propia, con apoyo del SPSS.

Otro dato interesante es el uso de los Kioscos del Gobierno del Estado de Colima, pues le ha dado una imagen más eficiente al régimen político. Esto, al automatizar muchos de los procesos burocráticos, pues como lo señala el Gráfico 4.14, se hace uso frecuente de los mismos.

¿Con qué frecuencia utiliza los kioscos del Gobierno del Estado de Colima para realizar algún trámite?

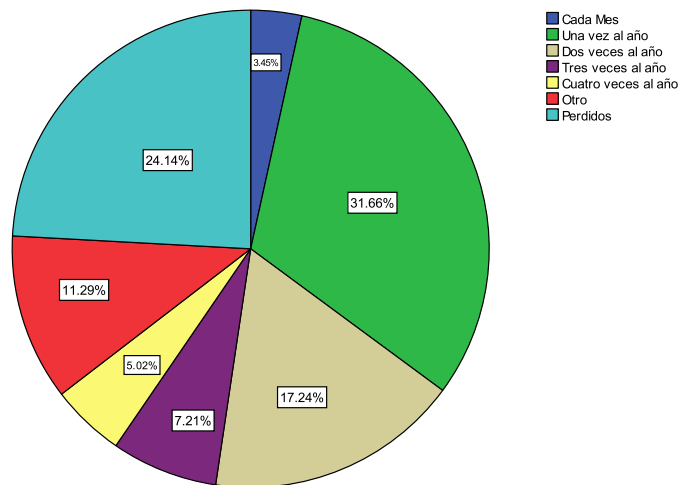


Gráfico 4.14. Frecuencia de uso de los Kioscos del Gobierno del Estado de Colima.

Fuente: Propia, con apoyo del SPSS.

Lo que de manera relevante señala la encuesta, es que la introducción de las urnas electrónicas debe hacerse, primero, en elecciones no vinculantes, como se observa en la Gráfica 4.18, con un porcentaje del 39.5% y en seguida, en una vinculante, con un promedio de aceptación ubicado en el 31.35%.

Con la acción anterior, se pretende mejorar el índice de confianza que se tiene, en el uso o no, de esta tecnología (Confianza). Su evaluación, en la Gráfica 4.17, obtuvo un promedio del 61.76% en respuestas negativas.

¿Confiaría usted en los resultados electorales finales si la gente votara a través de medios electrónicos similares a los de un cajero automático?

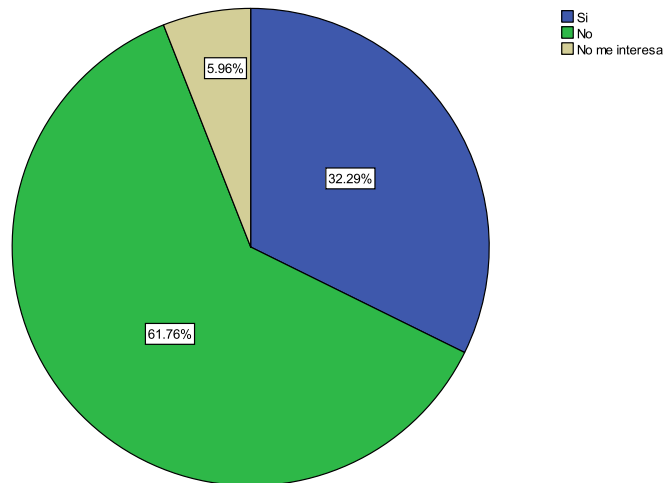


Gráfico 4.17. ¿Confiaría usted en los resultados electorales finales, si la gente votara a través de medios electrónicos, similares a un cajero automático?

Fuente: Propia, con apoyo del SPSS.

Considerando otros rubros, hay que poner atención en la falta de legislación al respecto, en la planeación gubernamental y la certeza política por parte de los partidos. Esto no agrega, en nada positivo, a la introducción de las TIC's en los procesos electorales. Por lo que se debe poner énfasis en que la clase política gobernante, se actualice y legisle al respecto.

El uso de estándares internacionales como son el ITIL y el NIST permite la incorporación de patrones que son funcionales, incorporando el uso de e-strategy. Por otro lado la medición de todos los procesos del órgano electoral usando Balaced Score Card permite controlar cada uno de los aspectos críticos de la jornada electoral, así como su evolución en tiempo real, ya que es posible monitorear, las diferentes pruebas antes del proceso, así como su evolución de manera automatizada

Con los datos anteriores, tenemos que todos los sistemas electorales, en el mundo, deben ser customizados de acuerdo a la democracia en turno y no al revés. Igualmente, se debe tener un

cuidado extremo en su planeación, implementación, divulgación y sustento legal, para que logre validez y la democracia siguiente tenga oportunidad de evolucionar.



Conclusiones.

Para dar el salto que se pretende hacia un país democrata, libre, autónomo y transparente, se debe, como Estado, establecer una Planeación Estratégica con rumbo. Primero, observando el camino que transitaron los países que cuentan con este tipo de tecnologías, para elegir a sus gobernantes. Con todos los indicadores posibles y las condiciones socio-político generales bien detectadas. Para poder establecer las condiciones ideales e iniciar esta nueva forma de hacer democracia.

La Planeación Estratégica debe darse desde las altas esferas ejecutivas del gobierno. De ahí, seguir hasta llegar a los poblados más humildes, pero alineados en un solo objetivo, con bases sólidas que permitan este crecimiento y maduración como país.

Hoy en día, un país que no esté inmerso en las TIC's es un país analfabeta. Con grietas por donde quiera, pues hoy los medios tecnológicos prácticamente están en todas las actividades del ser humano. Más profundos serán estos abismos, cuando vemos cómo los medios para hacer la democracia, se están dirigiendo hacia la tecnificación. Sin embargo, los electores desconocen las formas en que operan estas nuevas formas de elegir gobernantes. No saben claramente de su normativa legal, por lo que urge, al igual como se hizo con otros sistemas (bancarios, crediticios y departamentales), propagar el uso de la tecnología para hacer democracia.

Así, con una correcta Planeación alineada con las TIC's, harán que se lleve a buen puerto cualquier proyecto tecnológico. Lograrán que se impulse y apoye de manera correcta. En el caso del voto electrónico, seguro debe seguir las premisas que lo han enmarcado, tal y como se enunciaron en la Tabla 3.7.

Tabla 3.7. Propiedades del voto electrónico.

| Propiedad | Definición |
|------------------|---|
| Democracia | Sólo los electores elegibles pueden participar en la elección. |
| Conveniencia | Los electores pueden emitir su voto fácil y rápidamente. |
| Movilidad | No hay restricciones impuestas a la ubicación donde los votantes pueden emitir su voto. |
| Eficiencia | Los electores deben emitir su voto en una cantidad razonable de tiempo y no es necesario esperar a otros para completar el proceso. |
| Robustez | Nadie puede alterar o perturbar las elecciones a causa de la independencia de los procesos de votación. |
| Anonimato | Nadie puede rastrear la identidad de los votantes de las urnas. |
| Autenticación | Las autoridades y los electores deben verificar, uno al otro, durante el proceso de votación. |
| Validación | Las autoridades son capaces de comprobar si los votos son válidos o no. |
| Unicidad | Los electores no pueden votar más de una vez. |
| Completo | Un elector elegible siempre es aceptado por las autoridades. |
| Justicia | Las autoridades tienen prohibido engañar, incluso si intentan colusión. |

Fuente: Chou-Chen, Ching-Ying, y Hung-Wen (2004).

En el Estado de Colima se cuenta con la correcta infraestructura, para llevar a efecto comicios electorales, de forma electrónica adecuada. Lo anterior, porque su territorio es pequeño y es fácil adaptar las condiciones de la tecnología habilitada para tal efecto. Además, la presencia de la Universidad de Colima en todo el territorio colimense, da fe de lo que se enuncia. Así como la familiaridad con la que los ciudadanos acuden a los diferentes Kioscos de servicio, a realizar trámites. Igualmente, se presenta un fenómeno interesante, ya que la mayoría de los empleados usan banca electrónica, para disposición de su nómina. Razón por lo cual las personas están habituadas al uso de medios electrónicos en su entorno diario.

Por otro lado, el promedio de escolaridad de la ciudadanía permite que durante su estadía en la misma, se le capacite en el uso de herramientas orientadas al Internet, permitiendo que el usuario fácilmente se adapte al empleo de nuevas herramientas.

Por estas razones, es susceptible que en el Estado de Colima se haga uso y desarrollo del voto electrónico presencial seguro.

Como cierre final de este trabajo, se considera responder las preguntas de investigación antes enunciadas, en el apartado 1.4.

¿Cuál es el impacto estratégico de las acciones que realizan el IEEC, Gobierno del Estado de Colima, legisladores y partidos políticos, para motivar el uso de las TIC's en los diferentes escenarios, a través de los cuales se vinculan con la sociedad colimense?

Las tecnologías de la información y la comunicación han venido a cambiar la dinámica social, gubernamental, de negocios, y en general, todo aquel campo de acción donde el ser humano tiene injerencia.

La sociedad en su conjunto está preparada para recibir este tipo de cambios tecnológicos. Ya que muchos trámites los realizan por medios electrónicos, en forma presencial o a distancia. Lo único que pide, a cambio, es certidumbre, transparencia en las instituciones y órganos públicos.

Otra prueba fehaciente son los premios que ha ganado el Gobierno Estatal, como ejemplo; el premio I + T Gob., por parte del Comité de Informática de la Administración Pública Estatal y Municipal A.C. (CIAPEM). Lo anterior, por la expedición de documentos con firma electrónica.

Otra experiencia exitosa en la implementación de los Kioscos de Servicios Electrónicos, en donde la sociedad puede solicitar las atenciones siguientes; copias certificadas de nacimiento, defunción, matrimonio y divorcio. O bien; renovación de licencias de conducir de automovilista, chofer y motociclista, trámite de la clave CURP, pago de contribuciones vehiculares (tenencia y holograma) y canje de placas vehiculares.

Con las acciones anteriores, se ha mostrado interés y voluntad de los partidos políticos al impulsar, validar y dar certeza a esta tecnología. Amplia visión del gobierno al buscar los expertos, planear y diseñar el modelo adecuado, para ser referente nacional. Favorable prospectiva de la Cámara de Diputados por emitir las leyes correspondientes. Sobre todo la sociedad, que ya goza de los servicios ofrecidos por medios electrónicos, sin que se sufra por; errores, intermediarismo o burocracia absurda.

Aunque falta mucho trabajo por hacer en las diferentes dependencias, procesos y procedimientos, para que el Estado de Colima se posicione en lugares de vanguardia, como son:

- Democracia Electrónica.
- E-Gobierno.
- Ubicuidad Electrónica.

¿El Estado de Colima cuenta con la infraestructura tecnológica, logística, legal y política necesaria, para desarrollar un modelo estratégico de votaciones electrónicas presenciales seguras, e implantarlo a mediano plazo?

Al hablar de donde se ha tenido éxito, implica volver la vista hacia los procesos que nos falta mejorar. En el entorno democrático no es la excepción, e independientemente de los esquemas que se usen, cualquier sistema que intente implementarse debe venir acompañado de la confianza que generen los actores políticos en turno y la certidumbre hacia las instituciones.

La base legal con la cual deberán sustentarse los esquemas democráticos, es por demás importante. Constituye el marco normativo para que las instituciones; planeen, den camino y soporte, a las diferentes estrategias, para que las instituciones crezcan y no se estanquen.

En el Estado de Colima se necesita hacer el trabajo respectivo en:

- Legislación.
- Planeación Estratégica.
- Diseño, difusión y soporte de las TIC's.

Lo anterior es relevante, ya que no solamente implementar diseños será suficiente. Entendámoslo: para que los proyectos trasciendan, deben tener todo el soporte y trabajo antes mencionado.

Actualmente el Estado de Colima cuenta con la infraestructura adecuada para la implementación de las urnas electrónicas seguras. Esto, a través de la red de la Universidad de Colima, ya que cuenta con presencia en toda la entidad.

Cabe señalar que se ha realizado un intento previo para establecer la Democracia Electrónica, pero no hubo eco por parte de los actores. Ni un correcto impulso de parte de las autoridades y mucho menos difusión, por carecer de una adecuada planeación estratégica y el uso de estándares para tal efecto.

¿Qué tan informada está la sociedad colimense con respecto a las votaciones electrónicas seguras?

Como se mostró en la encuesta, la sociedad no ha tenido mayor información referente de las votaciones electrónicas seguras. Porque se requiere mayor difusión y propaganda por parte de nuestras autoridades. Por otro lado, no se tiene información del nivel de madurez de la tecnología que existe en los países del bloque europeo o asiático.

¿Qué tecnologías de hardware y software se requieren para desarrollar un modelo estratégico de seguridad, para votaciones electrónicas presenciales, que apoyen al proceso democrático en el que participa la sociedad?

Actualmente se tienen en el mercado, el hardware y software adecuado, para desarrollar un modelo estratégico que permita realizar votaciones electrónicas presenciales seguras. Y es que, en el caso de software, independientemente del que se elija, las plataformas de desarrollo están orientadas a red, como ejemplo:

- Microsoft framework™, en cualquiera de las versiones de desarrollo; Visual Basic, C++, C##, etcétera.
- Java™.
- Las plataformas de desarrollo de Borland™: JBuilder y BuilderC++.
- Rational Rose™.

En lo que se refiere a las bases de datos, las plataformas que se pueden usar son:

- SQL Server™.
- Oracle™.
- MySql.
- Postgresql.

Cabe destacar que las plataformas de uso libre, en su mayoría, sólo aceptan un subconjunto de las funcionalidades de las casas comerciales. Aunque soportan la seguridad adecuada para el proyecto, con total compatibilidad de los lenguajes base.

En lo referente a hardware, las arquitecturas de cómputo son muy nobles, pues se puede desarrollar en 32 y 64 bits. De acuerdo a las necesidades de procesamiento. De igual manera, se pueden usar indistintamente ambas, aunque para la seguridad y base de datos se ha requerir de plataformas de 64 bits.

Para el caso del firewall y la detección de intrusos, existen múltiples soluciones, como se enuncian a continuación, tanto en software como en hardware:

- SunScreen™.
- Enterasys™.
- Mcafee™.
- Ipchains.
- Iptable.

En el caso particular, las versiones comerciales tienen la ventaja de que la investigación y desarrollo, actualización y soporte, recae en quien es propietario de la marca o sus subsidiarias, quedando la administración en manos de personal de la institución. En cuanto a las versiones libres, absolutamente todo recae en el administrador de la seguridad.

¿Cuáles son los algoritmos de seguridad más confiables, para soportar transmisión y encriptación de los datos en una red de computadoras?

Los algoritmos de seguridad más confiables son en la actualidad SSL, para conexiones seguras entre varios sitios. Para el caso de la identificación y autenticación de personas, son aquellos soportados en teorías de Caos soportados en biometría. Asimismo, se puede echar mano de algoritmos similares al PGP, que usa llaves públicas y privadas.

En el caso de las VPN's para la comunicación de los equipos, se soporta sobre tuneleo (tunneling). Lo que garantiza un libre medio de comunicación, sin que los espías o hackers puedan interceptar la información.

Todas las tecnologías antes mencionadas son enumeradas y enmarcadas en los estándares NIST e ITIL, para minimizar los posibles ataques a los sistemas. Sin dejar de señalar que no existe sistema infalible y que las mayorías de los errores son causados por el ser humano.

¿Cuáles son las políticas de seguridad informática más adecuadas, para resguardar los sufragios de acuerdo al entorno actual, que cumplan con los estándares internacionales?

Los esquemas de seguridad que exigen estos medios, para hacer eficiente la democracia, ya existen, como se aprecia en los trabajos hechos en el NIST, ISO e ITIL. Además, se han implementado en otras latitudes, como son:

- a) Canadá.
- b) La mayoría de los países de Europa.
- c) Japón
- d) Venezuela.
- e) Brasil.

Algunos de estos países tienen un menor índice de desarrollo que nuestra nación. La única diferencia es la confianza que se la ha dado a sus instituciones, así como el sustento que se les otorgó por medio de la reglamentación y la legislación adecuada.

Es claro que la transición a medios electrónicos no es en automático. Requirió de una planeación estratégica y logística adecuada. Mucho de este trabajo fue sustentado con la complicidad de la academia y la industria, apoyado por los entornos políticos adecuados.

Por lo que se puede decir que, en Colima, se espera un arduo trabajo para; la planeación, implementación y legislación de este tipo de tecnologías. Con intención de que la sociedad, partidos políticos y gobierno, puedan disfrutar de los avances tecnológicos de hoy en día, disminuyendo la brecha digital en este rubro.

Trabajos Futuros.

Para dar continuidad a este trabajo de investigación, es necesario avanzar en las líneas de investigación con el amplio panorama de las disciplinas que se mencionaron y que por sí mismas cada una son susceptibles de profundizar, el trabajo futuro que se tiene se resume en:

- Gobierno Electrónico y su desempeño ya que en México la mayoría de los gobiernos ostentan esa bidireccionalidad con sus gobernados, pero en algunos casos lejos de optimizar el trabajo, parece que se hace más difícil el acceso a los servicios y comunicación con la burocracia gubernamental, es impórtate la evaluación y la implementación de estándares internacionales para que sea realmente efectivo.
 - Estandarización de los sistemas electorales a nivel nacional, esta parte de desarrollo es importante pues al parecer cada estado en lo particular está desarrollando tecnología sin considerar los esfuerzos que se hacen o se han hecho en otras latitudes, en la intensión de que se homologuen en un solo sistema o en su defecto se genere el estándar para que los sistemas a desarrollar cumplan y se apeguen a requerimientos mínimos.
 - Establecer una mejor estrategia para la penetración de las TIC's en los diferentes sistemas que usan para que la población agilice sus tramites y que estos no dependan de la burocracia en turno, ofreciendo sistemas pensados y diseñados a la altura de los usuarios y sus necesidades, siendo estos incluyentes a las personas con capacidades diferentes.
 - El desarrollo de sistemas de información usando software libre como alternativa para abatir los altos costos que involucra usar software comercial, siendo las universidades públicas de la entidad impulsor y baluarte para que exista una alta penetración del software libre y generar una nueva cultura de desarrollo en el Estado de Colima.
-

-
- En el ámbito legal se deben establecer nuevas premisas y leyes para el uso de las TIC's, ya que en la actualidad existe poco trabajo al respecto, en este punto en particular debe existir una colaboración multidisciplinar para que las leyes se desarrollen a la altura de la exigencia de la sociedad que cada día está más inmersa en una sociedad digitalizada.
 - La migración de todas las plataformas de los diferentes niveles de gobierno usando esquemas de estrategias electrónicas (e-strategy) pues a pesar de tener las plataformas adecuadas en algunos casos, no existe una alineación con ella al momento de plantear su planeación estratégica.
-

Contribuciones para futuras líneas de investigación.

Al finalizar este trabajo, se abre un abanico de opciones interesantes para el desarrollo de:

- Políticas públicas para el desarrollo de las TIC's.
- La evaluación y desarrollo de métricas del E-Gobierno.
- Planeación del establecimiento de la ubicuidad electrónica en la República Mexicana.
- Impacto de las políticas electrónicas en las TIC's.
- Normalización de procesos electrónicos (Planeación estratégica de los procesos).
- La aceptación de la e-strategy en nuestro país y sus estados, como una vía de éxito empresarial.
- La vinculación de las empresas con el gobierno, por medios electrónicos, en todos sus procesos (E-Government-E- Business).

En fin, el abanico es amplio y extenso. Solamente se enuncian aspectos que, en primer plano, urge que se den por la premura de que nuestro país y entidad evolucione hacia el futuro, con bases sólidas.

Aporte al conocimiento que se realiza con la presente tesis.

En las entidades de la República Mexicana se realizar esfuerzos aislados y poco planeados, en las diferentes áreas del conocimiento que conciernen a esta investigación, como son; administración pública, política, gestión y prácticamente se pueden enunciar todas las aristas de la planeación gubernamental.

En particular, para el desarrollo del voto electrónico seguro, se tiene de manera contundente que existen: la tecnología y los estándares tecnológicos. Aunque no integrados a una planeación estratégica adecuada, que utilice las clásicas teorías de la planeación, así como la integración de los nuevos esquemas como el e-strategy. Por otro lado, se tiene que el desarrollo que realizó la Dra. Rebecca Mercuri, en su mayoría, sólo contempla los aspectos tecnológicos y de logística, sin alinear una planeación estratégica, ni los procedimientos al interior de los sistemas de información y comunicación. Igualmente, diferentes autores solamente desarrollan una parte de la tecnología, de los procedimientos o la logística, sin llegar a ser por sí mismos un esquema integral.

Lo anterior ha de traer como beneficio que cuando se realiza la planeación de las diferentes entidades, se alinean los factores administrativos, de TI y de SI, como un todo, para que las entidades se posicionen con un rumbo claro, dando continuidad a sus esquemas en; corto, mediano y largo plazo.

En la parte de gestión y planeación, en particular, se observó poca congruencia entre los Planes de Desarrollo Gubernamentales; nacional, estatales y municipales. En la mayoría de ellos encontramos indicadores que no debieron tomarse en cuenta para desarrollar los planes y los objetivos trazados Asimismo, la manera de evaluar es poca objetiva, por lo que deben tomarse en cuenta verdaderos indicadores que se puedan usar, soportados en herramientas como el BSC, que permite ver al instante si se está ejecutando el Plan de manera adecuada y con poco margen de error. También podrían emplearse herramientas automatizadas, como el

BSC Desginer™ o plantillas hechas en Excel™, soportadas en red en Ms Project™, e incluso, soporte de herramientas de distribución libre.

Así pues, y por separado en este trabajo, se da cuenta que la integración de las TIC's, los SI, la Planeación Estratégica y las Buenas Prácticas, al ser integradas de manera pertinente, con una evaluación adecuada, darán como resultado una empresa con rumbo.

Índice de Figuras.

| | |
|--|------------|
| Figura 1.1. Ejemplo de un modelo estratégico de negocios. ----- | 15 |
| Figura 1.2. Elementos de la estrategia de SI/TI y sus interdependencias. ----- | 27 |
| Figura 1.3. Elementos del diamante de Leavitt y sus interrelaciones.----- | 27 |
| Figura 1.4. Elementos de seguridad del entorno informático. ----- | 35 |
| Figura 1.5. Generación de llaves PGP.----- | 44 |
| Figura 1.6. Políticas de Windows.----- | 45 |
| Figura 1.7. Ejemplo de una red privada virtual.----- | 53 |
| Figura 1.8. Metodología inicial propuesta.----- | 55 |
| Figura 2.1 Soporte para la confianza electoral en Estonia.----- | 65 |
| Figura 2.2. Acciones realizadas en Japón para desarrollar su estrategia de TI.----- | 78 |
| Figura 2.3. Distribución de los encuestados por sexo (en %).----- | 92 |
| Figura 2.4. Distribución de los encuestados, según su nacionalidad. ----- | 93 |
| Figura 2.5. Canales de información sobre la Consulta Ciudadana “Madrid Participa” (en %). ----- | 96 |
| Figura 2.6. Evaluación de la información recibida (en %).----- | 96 |
| Figura 2.7. Sistema de votación preferido por los encuestados (en %).----- | 97 |
| Figura 2.8. Sistema de votación preferido por los encuestados, según grupos de edad.97 | |
| Figura 2.9. Valoración comparativa de tecnologías de voto electrónico. ----- | 98 |
| Figura 2.10. Sistema de votación preferido por los encuestados, según grupos de edad.98 | |
| Figura 2.11. Sistema de votación preferido por los encuestados, según nivel de renta.99 | |
| Figura 2.12. Predisposición al uso de las NTIC y nivel de ingresos, según grupos de edad. ----- | 99 |
| Figura 2.13. Predisposición al uso de las NTIC y nivel tecnológico, según grupos de edad. ----- | 100 |
| Figura 2.14. Predisposición a la utilización de un sistema electrónico de votación, según el tipo de proceso participativo (en %).----- | 101 |

| | |
|--|-----------------|
| Figura 2.15. Predisposición a la utilización de un sistema electrónico de votación en elecciones vinculantes, según grupos de edad. ----- | 101 |
| Figura 2.16. Predisposición a la utilización de un sistema electrónico de votación, en elecciones vinculantes, según nivel de ingresos. ----- | 102 |
| Figura 2.17. Porcentaje de participación en las Elecciones Federales de Canadá (1980-2000). ----- | 120 |
| Figura 2.18. Flujo de trabajo para automatizar el proceso electoral en Canadá. ---- | 122 |
| Figura 2.19. Definición de los archivos electorales. ----- | 123 |
| Figura 2.20. Modelo de datos para la elección de los servicios automatizados. ----- | 123 |
| Figura 2.21. Ejemplo de una boleta electrónica. ----- | 126 |
| Figura 2.22. Reporte y procesamiento de la elección. ----- | 126 |
| Figura 3.1. Apreciación de los escudos nacionales. ----- | 173 |
| Figura 3.2. Los cuatro números de la sección. ----- | 173 |
| Figura 3.3. Imagen de seguridad con el logotipo del IFE. ----- | 174 |
| Figura 3.4. Fotografía con las dos tramas de seguridad. ----- | 174 |
| Figura 3.5. Fotografía digital impresa. ----- | 175 |
| Figura 3.6. Micro línea que aparece en el contorno de la fotografía. ----- | 175 |
| Figura 3.7. Nombre del titular que aparece al exponer la credencial en una lámpara de luz negra. ----- | 176 |
| Figura 3.8. Números que sirven para verificar si la credencial es genuina. ----- | 176 |
| Figura 3.9. Impresión micro línea, con el nombre del titular de la credencial. ----- | 177 |
| Figura 3.10. Secciones para marcar la participación del votante, en elecciones federales y locales. ----- | 177 |
| Figura 3.11. Órganos Ejecutivos del IEEC. ----- | 182 |
| Figura 3.12. Planeación Top-Down para la Seguridad de la Información. ----- | 190 |
| Figura 3.13. Planeación de la Organización. ----- | 192, 256 |
| Figura 3.14. Niveles de Planeación. ----- | 193 |
| Figura 3.15. Enfoques para la Implementación de la Seguridad. ----- | 195 |
| Figura 3.16. Relación entre los sistemas de información y los niveles de una organización. ----- | 196 |

| | |
|--|------------|
| Figura 3.17. Actividades del Ciclo de Vida Clásico de Desarrollo de Sistemas. ----- | 197 |
| Figura 3.18. Ciclo de vida de Software. ----- | 200 |
| Figura 3.19. Ciclo de Vida del Desarrollo de los Sistemas de Seguridad. ----- | 202 |
| Figura 3.20. Fase de Iniciación del SecSDLC. ----- | 207 |
| Figura 3.21. Control de acceso por teclado. ----- | 221 |
| Figura 3.22. Lector de tarjeta ----- | 223 |
| Figura 3.23. Acceso con rehilete o torniquete. ----- | 224 |
| Figura 3.24. Escáner de huellas digitales. ----- | 224 |
| Figura 3.25. Escáner de retina. ----- | 225 |
| Figura 3.26. Escáner de rostro. ----- | 225 |
| Figura 3.27. Sistema de defensa del castillo. ----- | 228 |
| Figura 3.28. El ciclo de vida del servidor físico. ----- | 233 |
| Figura 3.29. Puntos de acción para el manejo de riesgos. ----- | 236 |
| Figura 3.30. Ciclo de control de riesgos. ----- | 237 |
| Figura 3.31. Análisis del factor de riesgo de la información. ----- | 238 |
| Figura 3.32. Microsoft Identity y Access. ----- | 240 |
| Figura 3.33. Estructura de LDAP. ----- | 248 |
| Figura 3.34. Cuadro perspectiva del BSC. ----- | 253 |
| Figura 3.35. Interfaz del BSC Designer. ----- | 255 |
| Figura 4.1. Diagrama de actividades. ----- | 260 |
| Figura 4.2. Infraestructura de red de la Universidad de Colima. ----- | 301 |
| Figura 5.1. Modelo de Seguridad para Elecciones Presenciales en el Estado de Colima. ----- | 304 |
| Figura 5.2. Red de comunicación para la urna electrónica. ----- | 319 |
| Figura 5.3. BSC para la Seguridad de las TI. ----- | 329 |
| Figura 5.4. BSC para prevención y detección de intrusos. ----- | 330 |
| Figura 5.5. BSC para la Privacidad de la Identidad. ----- | 332 |
| Figura 5.5. BSC para la Seguridad y Privacidad. ----- | 333 |

Índice de Gráficos.

| | |
|---|-----------------|
| Gráfico 2.1. Frecuencia de la participación en las elecciones locales de Estonia, con voto electrónico (2005). ----- | 69 |
| Gráfico 4.1. Género del encuestado. ----- | 285 |
| Gráfico 4.2. Edad del encuestado. ----- | 286 |
| Gráfico 4.3. Edad del encuestado. ----- | 287 |
| Gráfico 4.4. Confianza en los cuerpos de seguridad. ----- | 288 |
| Gráfico 4.5. Confianza en los miembros de su culto. ----- | 288 |
| Gráfico 4.6. Confianza en los medios de información. ----- | 289 |
| Gráfico 4.7. Confianza en el proveedor de Internet. ----- | 290 |
| Gráfico 4.9. Confianza en los datos almacenados en el RENAUT. ----- | 291 |
| Gráfico 4.10. Grado de confianza en las operaciones bancarias, usando cajeros automáticos. ----- | 292 |
| Gráfico 4.11. ¿Tiene acceso a una computadora?. ----- | 292, 293 |
| Gráfico 4.12. ¿Utiliza alguna cuenta de correo electrónico?. ----- | 294 |
| Gráfico 4.13. ¿Ha usado los Kioskos del Gobierno del Estado de Colima para realizar algún trámite?. ----- | 294 |
| Gráfico 4.14. Frecuencia de uso de los Kioskos del Gobierno del Estado de Colima. | 295 |
| Gráfico 4.15. ¿Le gustaría que los procesos electorales, en el Estado de Colima, se realizaran a través de medios electrónicos, similares a un cajero automático?. ----- | 296 |
| Gráfico 4.16. ¿Confiaría usted en los resultados electorales finales, si la gente votara a través de medios electrónicos, similares a un cajero automático?. ----- | 296 |
| Gráfico 4.17. En caso de que el voto electrónico sea permitido en el Estado de Colima ...¿En qué tipo de proceso le gustaría que se utilizara? ----- | 297 |

Índice de Tablas.

| | |
|--|----|
| Tabla 1.1. Indicadores de competitividad en estados que han implementado voto electrónico. ----- | 5 |
| Tabla 1.2. Clasificación de países y tecnología que usa para voto electrónico.----- | 34 |
| Tabla 2.1. Nivel competitivo de Estonia.----- | 61 |
| Tabla 2.2. Evolución en el uso de las TIC's: Estonia. ----- | 62 |
| Tabla 2.3. Índice de desarrollo de las TIC's (IDI*) en Estonia (2002 y 2007). ----- | 62 |
| Tabla 2.4. Proporción de hogares con computadora en Estonia.----- | 63 |
| Tabla 2.5. Principales partidos políticos en Estonia.----- | 64 |
| Tabla 2.6. Estadísticas del voto por Internet en Estonia. Elecciones 2005 y 2007. ---- | 67 |
| Tabla 2.7. Estadística general de las elecciones para gobierno local en Estonia (2005). | 68 |
| Tabla 2.8. Electores del sistema electrónico por edad y género (2005). ----- | 69 |
| Tabla 2.9. Participación en áreas rurales y urbanas (2005). ----- | 70 |
| Tabla 2.10. Nivel competitivo de Japón. ----- | 71 |
| Tabla 2.11. Evolución en el uso de las TIC's: Japón. ----- | 72 |
| Tabla 2.12. Índice de desarrollo de las TIC's (IDI*) en Japón (2002 y 2007).----- | 72 |
| Tabla 2.13. Proporción de hogares con computadora en Japón. ----- | 73 |
| Tabla 2.14. Principales partidos políticos en Japón. ----- | 74 |
| Tabla 2.15. Calendario para implementar e-Gobierno en Japón.----- | 75 |
| Tabla 2.16. Proceso para el desarrollo del primer dispositivo de votación electrónica, en Japón. ----- | 81 |
| Tabla 2.17. Nivel competitivo de España. ----- | 82 |
| Tabla 2.18. Evolución en el uso de las TIC's: España.----- | 83 |
| Tabla 2.19. Índice de desarrollo de las TIC's (IDI) en España (2002 y 2007).----- | 83 |
| Tabla 2.20. Proporción de hogares con computadora en España. ----- | 84 |
| Tabla 2.21. Resultados de las elecciones generales del 9 de marzo de 2008. ----- | 85 |
| Tabla 2.22. Principales partidos políticos en España. ----- | 85 |
| Tabla 2.23. Distribución de los encuestados por grupos de edad.----- | 93 |

| | |
|--|------------|
| Tabla 2.24. Nivel de ingresos mensuales y posesión de computadora en el domicilio (en %). | 94 |
| Tabla 2.25. Acceso a Internet según nivel de ingresos mensuales (en %). | 94 |
| Tabla 2.26. Perfil tecnológico de los encuestados (en %). | 95 |
| Tabla 2.27. Escenario futuro de utilización de un sistema electrónico de votación. -- | 100 |
| Tabla 2.28. Nivel competitivo de Dinamarca. | 103 |
| Tabla 2.29. Evolución en el uso de las TIC's: Dinamarca. | 104 |
| Tabla 2.30. Índice de desarrollo de las TIC's (IDI*) en Dinamarca (2002 y 2007). -- | 104 |
| Tabla 2.31. Proporción de hogares con computadora en Dinamarca. | 105 |
| Tabla 2.32. Principales partidos políticos en Dinamarca. | 105 |
| Tabla 2.33. Nivel competitivo de Polonia. | 106 |
| Tabla 2.34. Evolución en el uso de las TIC's: Polonia. | 107 |
| Tabla 2.35. Índice de desarrollo de las TIC's (IDI*) en Polonia (2002 y 2007). | 107 |
| Tabla 2.36. Proporción de hogares con computadora en Polonia. | 108 |
| Tabla 2.37. Principales partidos políticos en Polonia. | 109 |
| Tabla 2.38. Nivel competitivo de Estados Unidos. | 111 |
| Tabla 2.39. Evolución en el uso de las TIC's: Estados Unidos. | 112 |
| Tabla 2.40. Índice de desarrollo de las TIC's (IDI*) en Estados Unidos (2002 y 2007). | 112 |
| Tabla 2.41. Proporción de hogares con computadora en Estados Unidos. | 113 |
| Tabla 2.42. Principales partidos políticos en Estados Unidos. | 114 |
| Tabla 2.43. Nivel competitivo de Canadá. | 115 |
| Tabla 2.44. Evolución en el uso de las TIC's: Canadá. | 116 |
| Tabla 2.45. Índice de desarrollo de las TIC's (IDI*) en Canadá (2002 y 2007). | 116 |
| Tabla 2.46. Proporción de hogares con computadora en Canadá. | 117 |
| Tabla 2.47. Principales partidos políticos en Canadá. | 117 |
| Tabla 2.48. Nivel competitivo de Argentina. | 127 |
| Tabla 2.49. Evolución en el uso de las TIC's: Argentina. | 128 |
| Tabla 2.50. Índice de desarrollo de las TIC's (IDI*) en Argentina (2002 y 2007). | 128 |
| Tabla 2.51. Proporción de hogares con computadora en Argentina. | 129 |
| Tabla 2.52. Principales partidos políticos en Argentina. | 129 |

| | |
|---|------------|
| Tabla 2.53. Nivel competitivo de Brasil. ----- | 132 |
| Tabla 2.54. Evolución en el uso de las TIC's: Brasil. ----- | 133 |
| Tabla 2.55. Índice de desarrollo de las TIC's (IDI*) en Brasil (2002 y 2007). ----- | 133 |
| Tabla 2.56. Proporción de hogares con computadora en Brasil. ----- | 134 |
| Tabla 2.57. Principales partidos políticos en Brasil. ----- | 134 |
| Tabla 2.58. Nivel competitivo de Venezuela. ----- | 136 |
| Tabla 2.59. Evolución en el uso de las TIC's: Venezuela. ----- | 137 |
| Tabla 2.60. Índice de desarrollo de las TIC's (IDI*) en Venezuela (2002 y 2007). --- | 137 |
| Tabla 2.61. Proporción de hogares con computadora en Venezuela. ----- | 138 |
| Tabla 2.62. Principales partidos políticos en Venezuela. ----- | 138 |
| Tabla 2.63. Nivel competitivo de México. ----- | 140 |
| Tabla 2.64. Evolución en el uso de las TIC's: México. ----- | 141 |
| Tabla 2.65. Índice de desarrollo de las TIC's (IDI*) en México (2002 y 2007). ----- | 141 |
| Tabla 2.66. Proporción de hogares con computadora en México. ----- | 142 |
| Tabla 2.67. Principales partidos políticos en México. ----- | 142 |
| Tabla 2.68. Participación de los ciudadanos mexicanos residentes en el extranjero (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006). ---- | 146 |
| Tabla 2.69. Paquetes electorales postales enviados y recibidos por continente. Participación de los ciudadanos mexicanos residentes en el extranjero (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006). ----- | 148 |
| Tabla 2.70. Participación ciudadana a nivel nacional y por entidad federativa * (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006). ---- | 148 |
| Tabla 2.71. Porcentaje de participación ciudadana a nivel nacional y por entidad federativa* que representan los votos válidos y los votos nulos (Elecciones Federales para Presidente de los Estados Unidos Mexicanos, 2006). ----- | 155 |
| Tabla 2.72. Índice de competitividad global. ----- | 158 |
| Tabla 2.73. Usuarios de Internet 2005-2008. ----- | 159 |
| Tabla 2.74. Suscriptores de banda ancha 2005-2008. ----- | 159 |
| Tabla 2.75. Suscriptores de telefonía móvil 2005-2008. ----- | 160 |
| Tabla 2.76. Índice de desarrollo de las TIC's (IDI) (2002 y 2007). ----- | 162 |

| | |
|---|------------|
| Tabla 2.77. Proporción de hogares con computadora. ----- | 163 |
| Tabla 3.1 Consejos Municipales Electorales del Estado de Colima. ----- | 183 |
| Tabla 3.1. Amenazas a la seguridad de la información. ----- | 204 |
| Tabla 3.3. Resumen de los sistemas voto electrónico. ----- | 211 |
| Tabla 3.4. Manejadores de Base de Datos. ----- | 217 |
| Tabla 3.5. Lenguajes de Programación. ----- | 217 |
| Tabla 3.6. Tipos de SO y características. ----- | 218 |
| Tabla 3.7. Propiedades del voto electrónico. ----- | 258 |
| Tabla 4.1. Distribución de la población en los 10 municipios de Colima. ----- | 283 |
| Tabla 4.2. Distribución de la población, en edad de votar, en los 10 municipios de Colima. ----- | 284 |
| Tabla 4.3. Distribución final por estratos, de acuerdo a la proporción de las edades. ----- | 284 |
| Tabla 4.4. Relación de los enlaces en la Universidad de Colima. ----- | 302 |

Referencias.

- Aceproject. (2008). Countries with e-voting projects. Recuperado el 05 de Noviembre de Noviembre, de http://aceproject.org/ace-es/focus/fo_e-voting/countries
- Acharya, L. (2003). Internet Voting. Parliament of Canada.
- Afuah, A., Tucci, C., & Tucci, C. (2002). Internet Business Models and Strategies: Text and Cases.
- Aguirre Paz, J., & Ortega Castañeda, E. (2005). La calidad del servicio como uno de los elementos formadores de imagen. Estudio de caso: Telmex-Maxcom. Recuperado el 10 de 10 de 2011, de http://catarina.udlap.mx/u_dl_a/tales/documentos/lco/aguirre_p_j/
- AKS-Labs. (s.f.). BSC Designer Home Page. Recuperado el 11 de 03 de 2011, de <http://www.bscdesigner.com/>
- Andal, A., Cartwright, P., & Yip, G. S. (Review). The digital transformation of traditional businesses. MIT Sloan Management , 34-41.
- Anónimo. (2000). Linux Máxima Seguridad. Madrid, España: SAMS.
- Arévalo, M. E., Garzón, M., & Roa, H. Sistema de votación electrónica S-Vote. Revista Tecnológica , 17 (1).
- arsvi.com. (15 de 10 de 2009). Recuperado el 15 de 10 de 2009, de <http://www.arsvi.com/2000/0212mt.htm>
- Awio Web Services LLC. (02 de 2011). Global Stats. Recuperado el 10 de 03 de 2011, de <http://www.w3counter.com/globalstats.php>
-

- Barranco, M. (14 de 03 de 2007). Interface de usuario. Recuperado el 5 de 11 de 2008, de <http://wwwdi.ujaen.es/~barranco/publico/ofimatica/tema7.pdf>
- Barrat, J., & Reniu, J. M. (2004). Democracia y Participación Ciudadana. Observatorio de Voto Electrónico, Madrid.
- Barrati, E. J., & Reniu Vilamala, J. M. (2004). Legal and Social Issues in Electronic Voting. Report on The Catalan Essays during the Elections of November, 2003. (e.- G. a. e-Democracy, Ed.) Distrito Federal, México.
- Barrientos, F. (2007). El voto electrónico y el déficit democrático europeo. TEXTOS de la CiberSociedad (12).
- Brown, S. (2000). Implementación de Redes Privadas Virtuales. Distrito Federal, México: Mc Graw Hill.
- Brunazo Filho, A. (2005). Voto Electrónico - Las nuevas tecnologías en los procesos electorales. Buenos Aires, Argentina: Grupo Editorial Planeta S.A.I.C. .
- Business Software Alliance. (2008). Recuperado el 22 de 03 de 2011, de <http://portal.bsa.org/2008eiu/study/2008-eiu-study-spanish.pdf>
- Carr, N. G. (01 de 05 de 2003.). IT Doesn't Matter. Harvard Business Review .
- Carracedo Gallardo, J., & Pérez Belleboni, E. (s.f.). Voto telemático. Recuperado el 06 de 10 de 2011, de http://vototelematico.diatel.upm.es/articulos/Voto_electronico_Salamanca.pdf
- Casidy, A. (2006). Information systems strategic planning. Florida: Auerbach Publications.
- CBC News. (25 de 01 de 2003). Computer vandal delays leadership vote. Recuperado el 10 de 11 de 2009, de http://www.cbc.ca/stories/2003/01/25/ndp_delay030125
-

Chew, E., & Gottschalk, P. (2009). Information Technology Strategy and Management: Best Practices (Premier Reference Source). New York: Information Science Reference.

Chew, E., Swanson, M., & Stine, K. (s.f.). National Institute of Standards and Technology. Recuperado el 26 de Noviembre de 2010, de <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>

Chou-Chen, Y., Ching-Ying, L., & Hung-Wen, Y. (2004). Improved Anonymous Secure E-voting over network. Information & Security. An International Journal , 15 (2), 181-195.

Cisco Networks. (27 de 11 de 2008). Network Security Policy: Best Practice White Paper. Recuperado el 27 de 11 de 2008, de http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a08014f945.shtml

Dueñas, S. (s.f.). Elementos que componen una interfaz. Recuperado el 05 de 11 de 2008, de <http://www.creatifweb.com.ar/multimedia/pdf/Doc9Interfaz.pdf>

El Universal. (19 de 04 de 2010). Recuperado el 16 de 03 de 2011, de <http://www.eluniversal.com.mx/notas/673768.html>

elections.ca. (4 de 12 de 2007). elections.ca. Recuperado el 10 de 11 de 2009, de <http://www.elections.ca/content.asp?section=loi&document=p3&dir=vot&lang=e>

Embajada del Japón en México. (s.f.). Información general. Recuperado el 01 de 12 de 2009, de <http://www.mx.emb-japan.go.jp/sp/japon/info-general.htm>

Enciclopedia de las naciones. (2009). Recuperado el 01 de 12 de 2009, de Enciclopedia de las naciones. (2009). Estonia <http://www.country-data.com/frd/cs/eetoc.html#ee0013>

- Eonsoo , K., I Nam, D.-I., & Stimpert, J. (2004). The Applicability of Porter's Generic Strategies in the Digital Age: Assumptions, Conjectures, and Suggestions. *Journal of Management* , 569-589.
- Federal Election Comissions. (09 de 11 de 2009). Election Assistance Commision. Recuperado el 09 de 11 de 2009, de http://www.eac.gov/voting%20systems/voluntary-voting-guidelines/docs/voting-systems-standards-volume-i-performance.pdf/attachment_download/file
- Feld, C. S. (2004). Getting IT Right. *Harvard Business Review* .
- FEM. (2009). The Global Competitiveness Report 2009-2010. Recuperado el 31 de 08 de 2009, de <http://www.weforum.org/pdf/GCR09/GCR20092010fullreport.pdf>
- Fernández Rodríguez, J. J., Barrat, J., Fernández Riveira, R. M., & Reniu, J. M. (2007). Voto Electrónico. Queretaro: FUNDAP.
- González Yáñez, A. (27 de 06 de 2007). Camara de Senadores en México. Recuperado el 10 de 10 de 2009, de <http://www.senado.gob.mx/index.php?ver=sp&mn=5&sm=3&id=413>
- Gonzalo, M. (s.f.). El voto electrónico venezolano, primeras aproximaciones. Recuperado el 2009 de 10 de 05, de http://www.funredes.org/mistica/castellano/ciberoteca/participantes/docupartie_votovenezolano.pdf
- Grant, R. (2003). Strategic planning in a turbulent environment: evidence from the oil majors. *Strategie Management Journal* , 24 (6).
-

Grover, V., & Saeed, K. A. (2004). Strategic orientation and performance of internet-based businesses. *Information Systems Journal* , 23-42.

Hansen, M. T., Nohria, N., & Tierney, T. (23 de 11 de 1999). What's Your Strategy for Managing Knowledge? *Harvard Business Review* .

Harris, B. (24 de 08 de 2004). Sum of a Glitch. Recuperado el 16 de 03 de 2011, de http://www.inthesetimes.com/article/978/sum_of_a_glitch/

Harris, B., & Allen, D. (2003). *Black Box Voting*. (L. Alexander, Ed.) USA.

Help America Vote Act of 2002. (s.f.). Help America Vote Act of 2002. Recuperado el 09 de 11 de 2009, de <http://www.fec.gov/hava/hava.htm>

Hernández Sampieri, R., Fernández-Collado, C., & Baptista Lucio, P. (2008). *Metodología de la Investigación* (4 ed.). Distrito Federal: Mc. Graw Hill.

<http://www.soumu.go.jp>. (s.f.). Recuperado el 15 de 10 de 2009, de http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol12/Vol12_16.html

<http://www.votersunite.org>. (s.f.). Recuperado el 16 de 03 de 2011, de <http://www.votersunite.org/info/ES&Sinthenews.pdf>

IEPC. (04 de 11 de 2010). Recuperado el 28 de 06 de 2011, de <http://www.iepcc.org.mx/index/pdf/democracia%20digital/evolucion%20de%20la%20urna.pdf>

IFE. (25 de 09 de 2008). Recuperado el 25 de 09 de 2008, de <http://www.ife.org.mx>

- IFE. (s.f.). Escrutinio y cómputo de la casilla. Recuperado el 24 de 10 de 2008, de 2007:
http://www.ife.org.mx/docs/Internet/FAQ/Docs_ES_PDF/etapas-y-actividades.pdf
- IFE. (2008). Estructura del Instituto Federal Electoral. Recuperado el 24 de 10 de 2008, de
<http://www.ife.org.mx/portal/site/ifev2/Estructura/>.
- IFE. (2006). Etapas y actividades sustantivas del proceso electoral. Recuperado el 24 de 10 de
2008, de
http://www.ife.org.mx/documentos/Reforma_Electoral/jornada/casilla_cofipe.pdf.
- IFE. (2008). Historia del Insituto Federal Electoral. Recuperado el 24 de 10 de 2008, de
<http://www.ife.org.mx/portal/site/ifev2/menuitem.cdd858023b32d5b7787e6910d08600a0/>
- IFE. (2008). Integración del Consejo General del IFE. Recuperado el 24 de 10 de 2008, de
http://www.ife.org.mx/portal/site/ifev2/Consejo_General/
- IMCO A.C. (2008). Recuperado el 12 de 1 de 2010, de
<http://imco.org.mx/images/pdf/%C3%8Dndice%20de%20Competitividad%20Estatal%202008.%20%20Aspiraciones%20y%20realidad.%20Las%20agendas%20del%20ofuturo.pdf>
- INE. (2009). Estimaciones de la Población Actual de España. Recuperado el 08 de 11 de
2009, de <http://www.ine.es/jaxiBD/tabla.do>
- INEGI. (2009). Perspectiva estadística Colima. Recuperado el 21 de 10 de 2009, de
<http://www.inegi.gob.mx/est/contenidos/espanol/sistemas/perspectivas/perspectiva-col.pdf>
-

Informática hoy. (s.f.). Tipos de licencias. Recuperado el 17 de 05 de 2011, de <http://www.informatica-hoy.com.ar/software-libre-gnu/Tipos-de-licencia-de-Software.php>

Instituto de Investigaciones Jurídicas de la UNAM. (17 de 03 de 2010). Voto Electrónico, derecho y otras implicaciones. Recuperado el 10 de 04 de 2010, de <http://www.bibliojuridica.org/libros/6/2801/10.pdf>

Instituto Electoral del Distrito Federal. (08 de 04 de 2008). Estudio Comparativo. Recuperado el 17 de 05 de 2011, de <http://www.iedf.org.mx/de/deoyge/EstudioComparativo2008.pdf>

Instituto Electoral del Estado de Colima. (10 de 10 de 2008). Instituto Electoral del Estado de Colima. Recuperado el 10 de 10 de 2008, de <http://www.ieec.col.gob.mx>

Internet World Stats. (2008). Recuperado el 11 de 11 de 2009, de <http://www.internetworldstats.com/am/ca.htm>

ITESO. (23 de 10 de 2008). Instituto Tecnológico de Estudios Superiores de Occidente A.C. Recuperado el 23 de 10 de 2008, de <http://www.soj.iteso.mx/libros/cap-4.PDF>

Johnson, G., & Scholes, K. (2002). Exploring corporate strategy. Harlow, Essex, UK: Prentice Hall.

Julien, P.-A., & Ramangalahy, C. (2003). Competitive Strategy and Performance of Exporting SMEs: An Empirical Investigation of the Impact of Their Export Information Search and Competencies. 27 (3), 227-245.

Kassab, B. (07 de 10 de 2001). Recuperado el 16 de 03 de 2011, de http://articles.orlandosentinel.com/2001-10-07/news/0110050592_1_election-workers-poll-workers-elections-office

Krimmer, R. (2006). Electronic Voting 2006. En O. Goran, H. James, & I. Nick, Election Workflow Automation - Canadian Experiences (págs. 131-141). Bregenz, Austria.

LDAPman home page. (09 de 05 de 2000). LDAPman home page. Recuperado el 17 de 03 de 2011, de http://www.ldapman.org/articles/sp_arbol_diseno.html

Lind, D. A., & Mason, R. D. (2000). Estadística para Administración y Economía. Distrito Federal, México: Mc Graw Hill.

Maaten, E., & Hall, T. (08 de 2008). Improving the Transparency of Remote E-Voting: The Estonian Experience. GI Editions , 31-42.

Madis, Ü. (s.f.). E-vote in Estonia experience. Obtenido de val@riigikogu.ee

Madise, Ü., & Martens, T. (2006). E-voting in Estonia 2005. The first practice of country-wide. En R. Krimmer, Electronic Voting 2006 (pág. 253). Bregenz, Austria: GI-Editions.

Maiorano, A. (2009). Criptografía. Distrito Federal, México: Alfaomega.

Maps of the world. (2009). Political Parties of Estonia. Recuperado el 01 de 12 de 2009, de <http://www.mapsofworld.com/estonia/politics-and-government/political-parties.html>

Mathias Lock and Key. (2011). Security Systems | Mathias Lock and Key | Denver and Colorado Springs. Recuperado el 14 de Enero de 2011, de <http://www.mathiaslockandkey.com/>

McAfee, A. (11 de 2006). Dominar los tres mundos de. Harvard Business Review .

Mercuri, R. (1 de 9 de 2010). Electronic Voting. Recuperado el 6 de 10 de 2011, de <http://www.notablesoftware.com/evote.html>

Mercuri, R. (2005). Security Watch. Communications of the ACM , 48 (5), 15-19.

Microsoft Corp. (2011). Windows Server 2008: Identidad y Acceso. Recuperado el 26 de 02 de 2011, de <http://www.microsoft.com/latam/windowsserver2008/ida-mw.mspx>

Ministerio del Interior de España. (19 de 06 de 1998). Dirección General de Política Interior. Recuperado el 13 de 10 de 2009, de http://www.mir.es/DGPI/Normativa/Normativa_Autonomica/Pais_Vasco/aut_pv_05.htm

Ministry of Internal Affairs and Communications. (2005). Statistics Bureau, Director-General for Policy Planning (Statistical & Standards) & Statistical Research and Training Institute. Population of Japan. Recuperado el 01 de 12 de 2009, de <http://www.stat.go.jp/english/data/kokusei/2005/poj/pdf/2005ch02.pdf>

Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan. (08 de 2001). Recuperado el 11 de 01 de 2011, de http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol12/Vol12_16.html#2

Mintzberg, H. (1994). Rise and Fall of Strategic Planning . NY: The Free Press.

Montesinos López, O. A., Luna Espinoza, I., Hernández Suárez, C. M., & Tinoco Zermeño, M. Á. (2009). Muestreo Estadístico. Colima, Colima, México: Universidad de Colima.

Morelis, G. (s.f.). El voto electrónico venezolano, primeras aproximaciones. Recuperado el 05 de 10 de 2009, de http://www.funredes.org/mistica/castellano/ciberoteca/participantes/docupart/e_votovenezolano.pdf

Murata, T., & Sakajiri, M. (3 de 12 de 2002). Universal Design for E-Voting System in Japan. Recuperado el 15 de 10 de 2009, de <http://www.bfp.rcast.u-tokyo.ac.jp/murata/2002p05e.htm>

MVS. (21 de 03 de 2010). Recuperado el 16 de 03 de 2011, de <http://www.youtube.com/watch?v=IGrbltNxQ4g>

National Institute of Standards and Technology . (10 de 2008). Security and Consideration in the System Development Life Cycle. Recuperado el 17 de 05 de 2011, de <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

National Institute of Standards and Technology . (s.f.). CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS. Recuperado el 26 de Noviembre de 2010, de <http://www.itl.nist.gov/lab/bulletns/bltnjun02.htm>

National Institute of Standards and Technology. (s.f.). SECURITY CONSIDERATIONS IN THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE. Recuperado el 26 de Noviembre de 2010, de <http://www.itl.nist.gov/lab/bulletns/bltndec03.htm>

NIST. (25 de 09 de 2008). National Institute of Standar and Technology. Recuperado el 25 de 09 de 2008, de <http://csrc.nist.gov/groups/STM/index.html>

Porter, M. (1985). *Competitive Advantage*. NY: The Free Press.

Porter, M. (2001). *Competitive Strategy*. NY: The Free Press.

Porter, M. (2001). *Strategy and the Internet*. Harvard Business Review. Harvard Business Review , 17 (03).

Presno Linera, M. Á. (s.f.). *La globalización del voto electrónico*. Recuperado el 10 de 10 de 2009, de <http://www.unioviado.es/constitucional/miemb/presno/La%20globalizacion%20del%20voto%20electronico.pdf>

Pressman, R. S. (2002). *Ingenieria de Software un Enfoque Práctico (Quinta Edición ed.)*. Madrid, España: Mc Graw Hill.

Prosser, A., & Krimmer, R. (s.f.). *The Dimensions of Electronic Voting, Law, Politics and Society*. Institute for Information Processing, Information Business and Process Management , 21-27.

Qingkai, M. (2010). Recuperado el 01 de 03 de 2011, de http://www.utica.edu/faculty_staff/qma/riskmanagement.pdf

Raya, J. L., & Raya, E. (2001). *Windows 2000 Server*. Bogota, Colombia: Alfaomega- Rama. Rodriguez-Henríquez, F., Ortiz-Arroyo, D., & García-Zamora, C. (2007). *Yet another improvement over the Mu-Varadharajan e-voting protocol*. ScienceDirect , 471-480.

Ruest, D., & Ruest, N. (2008). Microsoft Windows Server 2008. Distrito Federal, México: Mc Graw Hill.

Sabherwal, R., & Chan, Y. (2001). Alignment Between Business and IS Strategies: A Study of Prospectors, Analyzers, and Defenders. *Information Systems Research* , 12 (1), 11-33.

Scarfone, K. S., Grance, T., & Masone, K. (s.f.). Recommendations of the National Institute of Standards and Technology. Recuperado el 26 de Noviembre de 2010, de <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>

Schiaffini , R. (2006). El sistema de planeación mexicano hacia el siglo XXI. Ciudad de México, México: Porrúa.

Schneier, B. (2004). Voting Security and Technology. Recuperado el 10 de 10 de 2009, de <http://www.schneier.com/essay-039.pdf>

Schneier, B. (2004). What's Wrong With Electronic Voting Machines? Recuperado el 31 de 10 de 2008, de <http://www.schneier.com/essay-068.html>

Senn, J. S. (2002). Análisis y Diseño de Sistemas de Información. Naucalpan , Edo. de México, México: Mc. Graw Hill.

Slyke, B. V. (2003). E-Business Technologies: Supporting the Net-Enhanced Organization. NY: Wiley.

Soucre O., C. E. (06 de 09 de 2004). Recuperado el 23 de 09 de 2011, de http://www.urru.org/papers/Fraude_y_sistemas.pdf

- Southwest Research Institute. (05 de Marzo de 2010). SwRI: Full Life Cycle Development: Information System Engineering, full life development. Recuperado el 18 de Noviembre de 2010, de <http://www.swri.org/4org/d10/ised/fulllife.htm>
- Tapscott, D. (2000). Rethinking Strategy in a Networked World (or Why Michael Porter is Wrong about the Internet). Business Magazine .
- Telléz Valdés, J. (s.f.). Asociación de Empresas del Sector TIC, las Comunicaciones y los Contenidos Digitales. Recuperado el 10 de 10 de 2009, de <http://www.asimelec.es/media/II%20Convenci%C3%B3n%20Derecho%20Inform%C3%A1tico/doc%20conferencias/TELLEZVOTO.pdf>
- Temple University. (2009). Information systems assurance: security and risk management. Recuperado el 02 de 12 de 2010, de <https://community.mis.temple.edu/mis3580sec001fall2010/2010/10/03/w6-discussion-questions/>
- Thompson, A. A., & Strickland, A. J. (2003). Strategic management: concepts & cases (13 ed.). McGraw-Hell.
- Trechsel, A. H., & Mendez, F. (2005). The European and E-voting. NY, United States of America: Routledge.
- UNAM-CERT. (26 de 11 de 2008). Departamento de Seguridad de la UNAM. Protegiendo la privacidad. Recuperado el 27 de 10 de 2009, de <http://www.seguridad.unam.mx/doc/?ap=articulo&id=118>
- Unión Europea. (2009). Estados miembros de la UE. Estonia. Recuperado el 01 de 12 de 2009, de http://europa.eu/about-eu/countries/member-countries/estonia/index_es.htm
-

Vega Lebrún, C., Arvizu Gutiérrez, D., & García Santillán, A. (2008). Algoritmos Para Encriptación de Datos. Boca del Río, Veracruz, México.

Watson, R. T., & Mundy, B. (2001). A Strategic Perspective of Electronic Democracy. Communications of the ACM , 44 (1), 27-30.

Watters, P. (2003). Solaris 9. Madrid, España: Mc. Grar Hill.

Wired.com. (10 de 11 de 2004). Recuperado el 16 de 03 de 2011, de <http://www.wired.com/politics/security/news/2004/11/65665>

Withman, M., & Mattord, H. (2010). Management of Information Security. Boston, Massachusetts, United States of America: Course Technology.

World Economic Forum. (2009). The Global Competitiveness Report. Genova, Ginebra, Suiza.

Zacker, C. (2004). Windows Server 2003 Network Infraestructure. (C. Sánchez González, Ed.) Madrid, España: Mc Graw Hill/Interamericana de España.
