



Universidad Popular Autónoma del Estado de Puebla

Centro Interdisciplinario de Posgrados

**Una estrategia basada en patrones de interacción para mejorar la  
experiencia de usuario con factores críticos de seguridad  
informática**

Tesis profesional presentada por:

M.C. Sandra Rocío Murillo Cano

Para obtener el título en:

Doctorado en Tecnologías de Información y Análisis de Decisiones

Asesor: Dr. Alfredo Sánchez Huitrón

Puebla, Pue. México

Mayo 2015



**UPAEP – Secretaría General**

Dirección General de Apoyos Académicos

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

Biblioteca Central - **Karol Wojtyla**

**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.

## Índice General

|                                                                                        |    |
|----------------------------------------------------------------------------------------|----|
| Resumen .....                                                                          | 6  |
| 1. Introducción .....                                                                  | 8  |
| 1.1 Contexto .....                                                                     | 8  |
| 1.2 Motivación .....                                                                   | 10 |
| 1.3 Contribuciones.....                                                                | 11 |
| 1.4 Delimitación y recursos .....                                                      | 12 |
| 1.5 Metodología de la investigación .....                                              | 13 |
| 1.6 Estructura del documento .....                                                     | 14 |
| 2. Trabajo relacionado.....                                                            | 16 |
| 2.1 Experiencia de usuario.....                                                        | 16 |
| 2.1.1 Objetivos de la experiencia de usuario .....                                     | 17 |
| 2.1.2 Métodos de evaluación de la experiencia de usuario .....                         | 17 |
| 2.2 Usabilidad.....                                                                    | 18 |
| 2.2.1 Estándares relativos a la usabilidad.....                                        | 18 |
| 2.2.2 Métodos de evaluación de usabilidad .....                                        | 19 |
| 2.3 Patrones de interacción.....                                                       | 20 |
| 2.3.1 Lenguaje de patrones de interacción .....                                        | 21 |
| 2.3.2 Colecciones significativas de patrones de interacción.....                       | 22 |
| 2.3.3 Impacto en el desarrollo de software .....                                       | 24 |
| 2.4 Seguridad y cultura informática.....                                               | 25 |
| 2.4.1 Cultura de seguridad informática en usuarios finales .....                       | 25 |
| 2.4.2 Privacidad de datos.....                                                         | 25 |
| 2.4.3 Visualización estandarizada de información personal .....                        | 28 |
| 2.4.4 Administración de redes y seguridad .....                                        | 31 |
| 2.5 Factores humanos.....                                                              | 33 |
| 2.6 Áreas de oportunidad .....                                                         | 35 |
| 3. Administración de datos personales e Interfaz de usuario .....                      | 40 |
| 3.1 Elementos de un aviso de privacidad y su relación con el usuario de Internet ..... | 40 |
| 3.1.1 Metodología.....                                                                 | 40 |
| 3.1.2 Resultados acerca de la percepción de interacción.....                           | 41 |
| 3.1.3 Resultados acerca de la estructura de un aviso de privacidad.....                | 42 |
| 3.1.4 Discusión sobre la interacción con un aviso de privacidad.....                   | 42 |
| 3.1.5 Conclusión.....                                                                  | 43 |
| 3.2 Privacidad en Internet: factores técnicos y humanos.....                           | 43 |
| 3.2.1 Estilos de aprendizaje e Interfaz de usuario .....                               | 44 |
| 3.2.2 Metodología.....                                                                 | 44 |
| 3.2.4 Factores críticos de privacidad e interfaz.....                                  | 46 |

|       |                                                                                                                                   |     |
|-------|-----------------------------------------------------------------------------------------------------------------------------------|-----|
| 3.2.4 | Correlación entre los factores de estudio.....                                                                                    | 47  |
| 3.2.5 | Resultados acerca de los factores críticos de privacidad .....                                                                    | 48  |
| 3.2.6 | Resultados acerca de factores humanos y de interfaz .....                                                                         | 49  |
| 3.2.7 | Método sugerido para construir interfaces basado en correlaciones .....                                                           | 50  |
| 3.2.8 | Conclusión.....                                                                                                                   | 52  |
| 4.    | Administración de seguridad de red e interfaz de usuario .....                                                                    | 54  |
| 4.1   | Metodología.....                                                                                                                  | 54  |
| 4.2   | Elementos técnicos y elementos de interfaz.....                                                                                   | 55  |
| 4.3   | Importancia de factores críticos en herramientas de estudio .....                                                                 | 57  |
| 4.4   | Correlación de factores críticos de administración de seguridad en una red y elementos de Interfaz.....                           | 58  |
| 4.5   | Discusión sobre la percepción de la línea de comandos .....                                                                       | 60  |
| 4.6   | Implementación .....                                                                                                              | 61  |
| 4.7   | Conclusión.....                                                                                                                   | 61  |
| 5.    | Patrones de interacción y diseño de interfaces .....                                                                              | 63  |
| 5.1   | Metodología.....                                                                                                                  | 63  |
| 5.2   | Herramientas tradicionales de desarrollo para aplicaciones de seguridad .....                                                     | 65  |
| 5.3   | Patrones de interacción: una propuesta para un aviso de privacidad .....                                                          | 66  |
| 5.4   | Utilidad de las herramientas tradicionales de desarrollo en aplicaciones de seguridad .....                                       | 67  |
| 5.5   | Impacto del uso de patrones de interacción en aplicaciones de seguridad .....                                                     | 68  |
| 5.6   | Discusión sobre la necesidad de patrones de interacción .....                                                                     | 69  |
| 5.7   | Resumen de patrones de interacción generados .....                                                                                | 71  |
| 6.    | Conclusiones.....                                                                                                                 | 73  |
| 6.1   | Síntesis del trabajo desarrollado .....                                                                                           | 73  |
| 6.2   | Cumplimiento de objetivos .....                                                                                                   | 74  |
| 7.    | Trabajo y líneas de investigación futuras .....                                                                                   | 77  |
| 8.    | Referencias .....                                                                                                                 | 80  |
|       | Appendix A. Doctoral Consortium .....                                                                                             | 91  |
|       | Appendix B. Patrones de interacción y su aplicación a la privacidad en Internet.....                                              | 95  |
|       | Appendix C. Studying the relationships between the management of personal data privacy and user interface.....                    | 104 |
|       | Appendix D. Enhancing privacy awareness through interaction design. ....                                                          | 115 |
|       | Appendix E. Empowering Interfaces for Network Security Administrators. Keeping the Command Line in Mind when Designing GUIs. .... | 120 |
|       | Appendix F. Cuestionario sobre Factores críticos de privacidad.....                                                               | 125 |

## Índice de Figuras

|           |                                                                                            |    |
|-----------|--------------------------------------------------------------------------------------------|----|
| Fig. 1.1  | Esquema general de investigación.....                                                      | 12 |
| Fig. 1.2  | Áreas de investigación abarcadas por capítulo .....                                        | 14 |
| Fig. 1.3  | Enfoques de estudio.....                                                                   | 35 |
| Fig. 3.1  | Percepción de interacción con un aviso de privacidad.....                                  | 41 |
| Fig. 3.2  | Elementos presentes en los avisos de privacidad.....                                       | 42 |
| Fig. 3.3  | Relaciones significativas basadas en Coeficiente de Correlación de Pearson....             | 47 |
| Fig. 3.4  | Uso de datos personales y medidas de seguridad.....                                        | 48 |
| Fig. 3.5  | Estilo de aprendizaje y lectura de avisos de privacidad.....                               | 48 |
| Fig. 3.6  | Estilo de aprendizaje y personalización de navegador.....                                  | 49 |
| Fig. 3.7  | Personalización de navegador y medidas de seguridad.....                                   | 49 |
| Fig. 3.8  | Satisfacción general sobre el tema.....                                                    | 50 |
| Fig. 3.9  | Correlaciones de factores técnicos en un prototipo.....                                    | 51 |
| Fig. 3.10 | Correlaciones de elementos de interfaz en un prototipo.....                                | 51 |
| Fig. 3.11 | Presentación de patrones de interacción.....                                               | 52 |
| Fig. 4.1  | Evaluando herramientas con SUS.....                                                        | 55 |
| Fig. 4.2  | Correlaciones Snort.....                                                                   | 59 |
| Fig. 4.3  | Correlaciones Crack.....                                                                   | 59 |
| Fig. 4.4  | Correlaciones SNMP.....                                                                    | 59 |
| Fig. 4.5  | Correlaciones SNMP.....                                                                    | 59 |
| Fig. 5.1  | Prototipo de Navegación.....                                                               | 64 |
| Fig. 5.2  | Elementos gráficos de visualización.....                                                   | 64 |
| Fig. 5.3  | Visualización de un Aviso de Privacidad simplificado basada en estilos de Aprendizaje..... | 64 |
| Fig. 5.4  | Realidad aumentada.....                                                                    | 65 |
| Fig. 5.5  | Visualización basada en P3P.....                                                           | 65 |

## Índice de Tablas

|            |                                                                     |    |
|------------|---------------------------------------------------------------------|----|
| Tabla 2.1  | Resumen de trabajos relacionados sobre experiencia de usuario.....  | 36 |
| Tabla 2.2  | Resumen de trabajos relacionados sobre usabilidad.....              | 36 |
| Tabla 2.3  | Resumen de trabajos relacionados sobre patrones de interacción..... | 37 |
| Tabla 2.4  | Resumen de trabajos relacionados sobre seguridad informática.....   | 37 |
| Tabla 2.5  | Resumen de trabajos relacionados sobre factores humanos.....        | 38 |
| Tabla 3.1  | Carrera.....                                                        | 45 |
| Tabla 3.2  | Semestre.....                                                       | 45 |
| Tabla 3.3  | Sexo.....                                                           | 45 |
| Tabla 3.4  | Edad.....                                                           | 45 |
| Tabla 3.5  | Estilos de aprendizaje en la muestra.....                           | 46 |
| Tabla 3.6  | Resumen del procesamiento de los casos.....                         | 46 |
| Tabla 3.7  | Estadísticos de fiabilidad.....                                     | 46 |
| Tabla 4.1  | Demográficos.....                                                   | 54 |
| Tabla 4.2  | Resultados evaluación SUS.....                                      | 55 |
| Tabla 4.3  | Validez de instrumento.....                                         | 57 |
| Tabla 4.4  | Colores, tipografía e íconos.....                                   | 57 |
| Tabla 4.5  | Elegir posición y versión gráfica.....                              | 57 |
| Tabla 4.6  | Básicos, avanzados, esperados.....                                  | 58 |
| Tabla 4.7  | CLI y menú de administración.....                                   | 58 |
| Tabla 4.8  | Satisfacción General.....                                           | 59 |
| Tabla 4.9  | Comparación de resultados IDS.....                                  | 61 |
| Tabla 4.10 | Comparación de resultados Craker.....                               | 61 |
| Tabla 5.1  | Herramientas de programación, guías y estándares.....               | 65 |
| Tabla 5.2  | Utilidad de herramientas.....                                       | 67 |
| Tabla 5.3  | Elementos adicionales.....                                          | 68 |
| Tabla 5.4  | Tareas asociadas y calificación.....                                | 68 |
| Tabla 5.5  | Estimación de impacto de patrones de interacción.....               | 69 |
| Tabla 5.6  | Herramientas generales versus Patrones de Interacción.....          | 69 |

## Resumen

El incremento constante de usuarios en Internet exige mejores prácticas que faciliten la construcción de interfaces usables relativas a temas de seguridad para cumplir con su objetivo técnico y también lograr un impacto positivo en la experiencia de usuario, utilizando la tecnología como herramienta y no como obstáculo.

Es deseable que los desarrolladores de software conozcan no sólo los requerimientos de seguridad del sistema sino también al usuario final, sus necesidades, su entorno y variables culturales al momento de construir, modificar o dar mantenimiento a una solución de este tipo para así aplicar de forma eficiente el lenguaje (escrito, gráfico y sonoro) técnico y coloquial asociado a este rubro. En su mayoría estas aplicaciones son desarrolladas por expertos en seguridad, quienes no lo son necesariamente en temas de usabilidad, diseño gráfico o experiencia de usuario.

En el ámbito de la seguridad informática se han propuesto soluciones técnicas para gestionar algunas tareas asociadas a esta área del conocimiento. Sin embargo, se delega a las personas la responsabilidad de adaptarse a ellas y no viceversa. Hasta el momento, la experiencia de usuario no ha sido considerada un factor crítico en el diseño de las mismas.

Desde la perspectiva de la interacción humano-computadora, un patrón de interacción describe una solución exitosa a un problema recurrente relativo a la interfaz de usuario en un contexto dado. Sirve para describir relaciones visuales, estéticas y de satisfacción al mismo tiempo que define un problema, su contexto y solución. Esto facilita la comunicación entre miembros de distintas disciplinas, permitiendo registrar el conocimiento y la experiencia para construir prototipos de interfaz que sean usables.

Esta circunstancia ha motivado el desarrollo de esta tesis. Este trabajo presenta una estrategia basada en patrones de interacción para mejorar la experiencia de usuario con factores críticos de seguridad informática limitado a la administración de privacidad y administración de una red de cómputo y comunicaciones en un entorno universitario.

Como primera fase se identifican tres conjuntos de factores críticos de interacción para grupos específicos de usuarios: de seguridad, de interfaz y humanos. Posteriormente se determinan las correlaciones de los elementos de los tres conjuntos mediante métodos estadísticos para proponer un procedimiento de construcción de interfaces basado en dichos valores. En la siguiente etapa se documentan factores de la experiencia de usuario en torno a la interacción con tópicos emergentes de seguridad. Finalmente se construye y evalúa un conjunto de patrones de interacción para observar si la propuesta de integración de las áreas estudiadas aportan mejoras en la percepción y manipulación de interfaces relativas a un conjunto específico de tareas.

## Capítulo 1. Introducción

---

*“Lo último que uno sabe es por dónde empezar”*

*Blaise Pascal*

En este capítulo se presenta el contexto y la motivación que originaron este trabajo, sus contribuciones, la delimitación y recursos para el desarrollo del mismo así como la metodología de la investigación, el impacto esperado y la estructura del documento.

# 1. Introducción

La experiencia de usuario en torno a la seguridad informática se presenta como una disciplina emergente en un mundo donde se observan distintos fenómenos: el número de personas que usan Internet crece día con día, diversos perfiles de usuario tienen acceso desde distintos tipos de dispositivo, cada vez más se compromete información sensible desconociendo las consecuencias y las aplicaciones en su mayoría son desarrolladas por personas expertas en el tema. Las aplicaciones desarrolladas deben cumplir su función como herramienta de apoyo para facilitar las tareas para las que fueron diseñadas y no para ser un obstáculo o la causa de resultados no deseados para las personas.

## 1.1 Contexto

Existen una gran cantidad de guías, estándares y reglas ergonómicas para diseñar interfaces de aplicaciones informáticas usables (Hernández-Hernández, Alvarez-Carrión, & Muñoz-Arteaga, 2012). Sin embargo, aplicarlas no es sencillo debido a que el contexto en que se diseñaron no es precisamente el mismo que se requiere en la vida real, no se proveen ejemplos que aclaren cómo usarlos ni se cuenta con una descripción de las posibles consecuencias de su empleo.

Un patrón es un medio de comunicación que expresa una solución de interfaz en una forma textual y gráfica a un problema recurrente dentro de un contexto determinado. Su especificación permite comunicar la experiencia y el conocimiento en un área específica (Gamma, Helm, Ralph, & Vlissides, 1995) (Borchers, 2001). Un patrón de interacción describe una solución exitosa a un problema recurrente relativo a la interfaz de usuario en un contexto dado (Hernández-Hernández, Alvarez-Carrión, & Muñoz-Arteaga, 2012). Sirve para describir relaciones visuales, estéticas y de satisfacción al mismo tiempo que define un problema, su contexto y solución. Esto facilita la comunicación entre miembros de distintas disciplinas permitiendo registrar el conocimiento y la experiencia para construir prototipos de interfaz de usuario (Bayle E. , 1998) (Van-Welie, 2001) (Acosta & Zambrano, 2011).

(Joseph & Baraclow, 1997) introdujeron el concepto de patrones a la comunidad de seguridad informática . Desde entonces, diversos trabajos han propuesto soluciones en el área de patrones de seguridad. (Cranor, Romanowsky, Hong, Acquisti, & Friedman, 2006) (Yoshioka, Washizaki, & Maruyama, 2008) . De acuerdo al trabajo de (Muñoz Arteaga, Medina Medina, Guerrero, & Muñoz Lopez, 2009), disponer de una colección de patrones de interacción para el diseño de la retroalimentación visual puede contribuir a que el usuario tenga un mayor control sobre su seguridad. Sin embargo, día con día las necesidades son diversas y se requieren de nuevas propuestas.

Ante los problemas que han surgido como el robo de identidad, fraudes y extorsiones, entre otros, organismos de prestigio internacional han propuesto mecanismos para que los desarrolladores de software incluyan opciones que fortalezcan la seguridad del usuario. En la parte técnica ha sido posible detectar áreas de oportunidad y proponer soluciones. Sin embargo, el usuario promedio no las aprovecha como se espera. (Cranor & Garfinkel, 2005) (Garfinkel & Faith, 2005).

Hoy, la posibilidad de tener un punto de acceso a la red es muy alta y los perfiles de los usuarios son muy vastos, incrementándose con esto el uso cotidiano de software (AMIPCI, 2012). Algunas aplicaciones no incluyen medidas de seguridad informática para advertir al usuario acerca de los riesgos asociados a su uso (Lindskog H. , 2003). Además, cada software maneja términos (técnicos y legales) y simbología de forma distinta, lo que causa frustración y rechazo en los usuarios finales ante temas de seguridad.

Sobre la administración de la privacidad por parte de los usuarios a nivel mundial (Gage-Kelley, Brewer, Mayer, Cranor, & Sadeh, 2011) se reconoce lo siguiente:

- Las herramientas que se ofrecen dentro de las aplicaciones no son usadas de manera apropiada para cumplir con el objetivo de proteger la información y son percibidas por los usuarios como "una maraña desconcertante de opciones" que estorban, confunden y no aportan beneficios.
- Se desconocen los riesgos y consecuencias de no proteger los datos personales.
- Se percibe mayor comodidad al tener completa libertad para agrupar los elementos de acuerdo a sus preferencias y no siempre aceptan las opciones predeterminadas o sugeridas en la interfaz.

Los expertos en administración de prevención y solución de problemas informáticos también desean interfaces amigables. Algunos estudios (Winkler, 2012) (Chiasson, Biddle, & Somayaji, 2007) revelan que la usabilidad es un factor determinante para el software de administración de seguridad en una red. La libertad de personalizar la visualización de grandes volúmenes de información relativas al monitoreo mejoran la experiencia de usuario e incrementan la productividad (Luse, 2009) (Conti, Ahamad, & Staskp, 2005)

Desde el 2008, el proyecto de investigación PrimeLife (Life, 2008) ha sido desarrollado para crear una colección de patrones de Interacción con el objetivo de definir directrices sobre cómo diseñar interfaces usables para mejorar la seguridad en los sistemas interactivos. Sin embargo, estos son propuestos bajo un contexto de términos legales europeos. En general, los desarrolladores de sistemas que involucran seguridad enfrentan la misma situación: marcos legislativos de acuerdo a cada región o país y se carece de colecciones que propongan soluciones de diseño, desarrollo, evaluación o uso exitoso a situaciones recurrentes que incluyan factores humanos. (Murillo & Sánchez, 2014)

Existen diversas categorías en las se agrupan a los usuarios de tecnologías de información: edad, nivel de estudios, lugar geográfico de acceso, sexo, ocupación, tipo de sitios de Internet que frecuenta, entre otros. Considerar factores humanos podría sugerir principios para personalizar interfaces humano-computadora que contribuyan a mejorar la experiencia de usuario con factores críticos de seguridad en Internet. Diversos proyectos de investigación han comprobado que considerar estilos de aprendizaje en la creación de interfaces mejora la experiencia y ergonomía cognitiva del usuario. (Velasco-Santos, Laureano-Cruces, Mora-Torres, & Herrera-Bautista, 2011) (Velasco-Santos, Sánchez-Guerrero, & Laureano-Cruces, 2009). Sin embargo, poco se ha explorado sobre su aplicación para construir interfaces que faciliten el uso y la administración de factores críticos de seguridad informática.

Usuarios casuales y expertos, sin distinción, viven una situación común: utilizar las opciones para administrar los elementos de seguridad, si es que éstas existen en las

aplicaciones, requiere una alta curva de aprendizaje que no siempre se está dispuesto a afrontar. Los contrastes ocurren al comparar lo que debiera ocurrir con lo que ocurre en la realidad, de esta forma, se identifican las siguientes contradicciones:

- De manera ideal se esperaría que los desarrolladores de software dispusieran de herramientas para la implementación de interfaces efectivas y universales relativas a seguridad informática. En la realidad, cada equipo de trabajo implementa sistemas con base a su propia experiencia y requerimientos solicitados por el cliente, sin contar en ocasiones, con personas expertas en términos legales, usabilidad o diseño gráfico.
- De manera ideal se esperaría que los usuarios utilizaran las aplicaciones como herramientas de apoyo para interactuar con los factores críticos de seguridad, sin embargo, cada aplicación, aunque técnicamente sea buena y ofrezca opciones integrales, es diferente y el usuario debe adaptarse a la interfaz, sin poder trasladar su experiencia previa de uso a otras aplicaciones similares, causando frustración y pérdida de tiempo.

Con lo mencionado hasta el momento, se plantea la siguiente pregunta:

¿Cómo mejorar la experiencia de usuario para interactuar de manera efectiva con factores críticos de seguridad informática?

## **1.2 Motivación**

Hoy en día, la relación entre la seguridad informática y los temas de usabilidad ofrece un área de investigación activa en distintas universidades debido a su impacto social. Como el número de usuarios de Internet va en aumento y se espera que esta tendencia continúe (AMIPCI, 2012), se han desarrollado trabajos de investigación que proponen relaciones entre factores humanos y la interacción con una computadora, principalmente para obtener ventajas pedagógicas (Velasco-Santos, Laureano-Cruces, Mora-Torres, & Herrera-Bautista, 2011) (Velasco-Santos, Sánchez-Guerrero, & Laureano-Cruces, 2009) (Cela, Fuentes, Alonso, & Sánchez, 2010). Por otro lado, el área de seguridad ha sido estudiada principalmente desde la perspectiva técnica y teórica, dando muy poca relevancia al factor humano. Las presentaciones que se han hecho de los avances de este trabajo en foros internacionales relativos a interacción humano-computadora refuerzan la idea de integrar estas áreas de conocimiento para proponer mejoras en el uso cotidiano de aplicaciones bajo un contexto seguro para las personas. Estas aportaciones pueden contribuir para hacer un análisis sobre el uso de software y la administración de factores críticos de seguridad informática.

La investigación es pertinente, en lo particular para la Universidad Popular Autónoma del Estado de Puebla (UPAEP) debido al fortalecimiento que se desea dar desde la parte académica a la línea de Seguridad Informática, por el auge e importancia actual necesaria en los egresados de las carreras relacionadas con Tecnologías de Información. Este trabajo de investigación puede ser considerado por otras instituciones educativas, de desarrollo de software o de implementación de soluciones basadas en Tecnologías de Información que estén abordando estos temas.

El planteamiento de esta investigación surge, de manera personal, con base a los diferentes roles desempeñados como parte de mi vida profesional. Como administradora de servidores centrales en la (Universidad de las Américas - Puebla) UDLAP, administré servicios de web, correo electrónico, espacio de almacenamiento, clientes delgados y desarrollé herramientas para monitoreo, detección y corrección de actividad sospechosa en dicha red y sus elementos informáticos. Mi tesis de Maestría consistió en el Diseño y Aplicación de un Sistema Integral de Seguridad Informática para la UDLAP. Los últimos diez años he sido catedrático de tiempo completo en UPAEP y soy responsable de la línea curricular de Redes, Comunicaciones y Seguridad en la Facultad de Tecnologías de información del Departamento de Ingenierías. El interés de abordar este trabajo pretende fortalecer esta línea académica y generar una propuesta de valor para el entorno universitario.

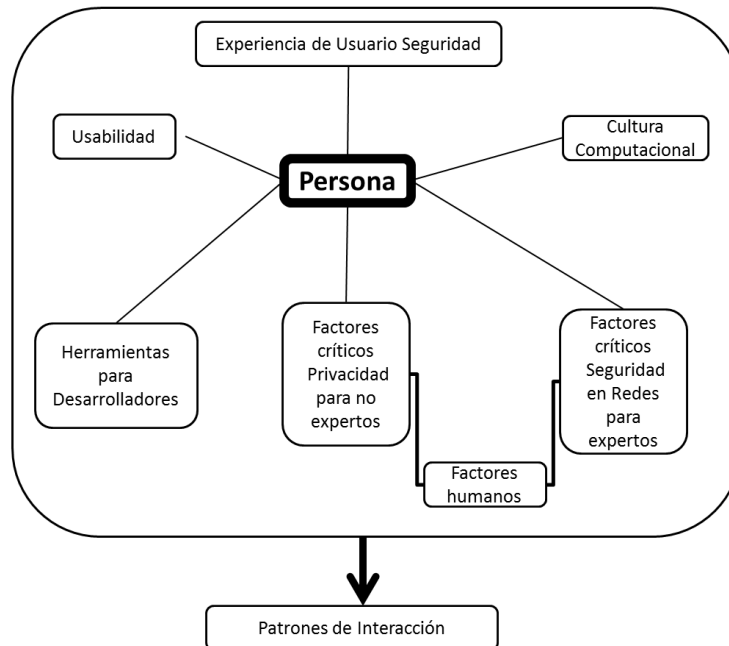
### 1.3 Contribuciones

Siendo congruente con la visión humanista de UPAEP, es lógico que la **persona** sea el centro y razón de ser de las actividades y proyectos institucionales. Por lo tanto, también debe de serlo desde el punto de vista de la ciencia y la tecnología. Es bien aceptado que en las Tecnologías de Información que el software y hardware no son el fin u objetivo sino un medio para mejorar la calidad de vida de las personas. Actualmente, existen ciencia y tecnología de áreas que no han colaborado entre sí para cumplir esta misión: el área de **Experiencia de Usuario** (denominada en la cultura informática como UX, User eXperience), **Seguridad Informática**, **Usabilidad** y el área emergente de **Patrones de Interacción**. Por lo tanto, en este trabajo se investigará a la persona respecto a algunos de sus factores (se les denominará **Factores Humanos**, entre ellos su Estilo de Aprendizaje) y su rol ante el Internet y las aplicaciones (si la persona es un **Desarrollador**, si la persona es **experta** en seguridad, cómo su cultura computacional le permite aprovecharlos o no, o si la persona **no es experta**) para hacer una propuesta aprovechando dicha investigación que permita el diseño y aplicación de Patrones de Interacción que mejoren la Experiencia de Usuario, haciendo énfasis en factores críticos de manejo de Privacidad y Seguridad en Redes. Lo anterior se resume en el esquema de la Figura 1.1.

La principal contribución de este trabajo al área de Interacción humano-computadora consiste en modelar un conjunto de patrones de interacción para mejorar la experiencia de usuario con factores críticos de seguridad informática en un entorno universitario.

Otras contribuciones incluyen lo siguiente:

- Se han Identificado correlaciones significativas entre factores críticos de seguridad, elementos de interfaz y factores humanos
- Se ha propuesto un método de construcción de interfaces determinado por correlaciones de sus componentes
- Se han documentado factores de la experiencia de usuario en torno a la interacción con tópicos emergentes de seguridad



**Fig. 1.1** Esquema general de investigación

- Se ha valorado el uso de patrones de interacción en la construcción de interfaces efectivas de seguridad
- Se ha producido un conjunto de patrones de interacción basado en factores humanos que facilite la percepción y manipulación de interfaces relativas a seguridad informática en un entorno universitario.

La hipótesis general de este trabajo de investigación se planteó de la siguiente manera:

Si existiera un conjunto de patrones de interacción que considere factores humanos se podría mejorar la experiencia de usuario con factores críticos de seguridad informática en un entorno universitario.

## 1.4 Delimitación y recursos

Las delimitaciones del presente trabajo se dieron en tres aspectos:

1. La espacial, teniendo como lugar geográfico la ciudad de Puebla en el estado de Puebla, México y en específico la participación de una institución de educación superior, la Universidad Popular Autónoma del Estado de Puebla.
2. La temporal, de agosto 2012 a diciembre 2014 en el cual se llevará a cabo el estudio de investigación.
3. Teórica, debido a que la investigación abarca distintas disciplinas. Es importante destacar que la interacción humano-computadora será la principal disciplina donde

se hará el estudio. Otras disciplinas que aportarán a la investigación son: patrones de interacción, usabilidad, seguridad informática y experiencia de usuario.

Es importante delimitar la población donde se llevó a cabo el estudio para comprobar la hipótesis de investigación. Fueron alumnos de licenciatura escolarizada de UPAEP y profesores de nivel licenciatura de las Facultades de Tecnologías de Información y Electrónica de la misma Universidad.

Los recursos necesarios para llevar a cabo la investigación serán el acceso a equipo de cómputo y bibliotecas digitales, así como el apoyo de estudiantes, becarios y tesis para realizar las encuestas, los prototipos y procesar la información.

## **1.5 Metodología de la investigación**

La metodología de investigación para este proyecto se planteó de orden cualitativo con las siguientes etapas:

- a) Diagnóstico de la situación actual.
- b) Identificación de las variables involucradas en la investigación.
- c) Identificación de objetivos, alcances y limitaciones.
- d) Este proyecto se construyó con base en una investigación experimental basada en un análisis descriptivo y paramétrico (coeficientes de correlación) de datos cuantitativos relativos a factores críticos de seguridad. (Hernández Sampieri, 2010)
- e) Selección y formación del grupo experimental.
- f) Construcción de una colección de patrones de interacción.
- g) Aplicación de los instrumentos de evaluación en las distintas etapas.
- h) Diseño de los parámetros e indicadores clave para evaluar y medir el cumplimiento de objetivos.
- i) Evaluación de resultados.
- j) Documentación de las aportaciones.
- k) Desarrollo de conclusiones.
- l) Elaboración de reporte de investigación.

## 1.6 Estructura del documento

En el capítulo 2 se presenta el trabajo relacionado que da sustento teórico a esta investigación en las áreas de Experiencia de usuario, Usabilidad, Patrones de Interacción y Seguridad informática.

En el capítulo 3 se identifican las correlaciones significativas entre factores críticos de administración de datos personales, factores humanos e interfaz de usuario mediante un análisis de la estructura actual de dichos avisos conforme los parámetros que exige la ley, la percepción que se tiene de la información dentro del mismo y un estudio etnográfico. Con base en estos resultados, se sugiere un método preliminar de construcción de interfaces.

En el capítulo 4 se presentan las correlaciones significativas entre factores críticos de administración de seguridad en una red e interfaz de usuario tomando como base un estudio de usabilidad de herramientas básicas y al identificar los elementos técnicos y humanos comunes a dichas aplicaciones.

En el capítulo 5 se investiga cuáles son las herramientas que usan los desarrolladores para construir software relativo a seguridad y se propone un conjunto de patrones de interacción basado en factores humanos para resolver un conjunto de tareas específicas relativas a seguridad evaluando su impacto.

En el capítulo 6 se presentan las conclusiones de la investigación y el trabajo a futuro.

En Fig. 1.2 se representa de forma gráfica los temas cubiertos en el presenta trabajo por capítulo.

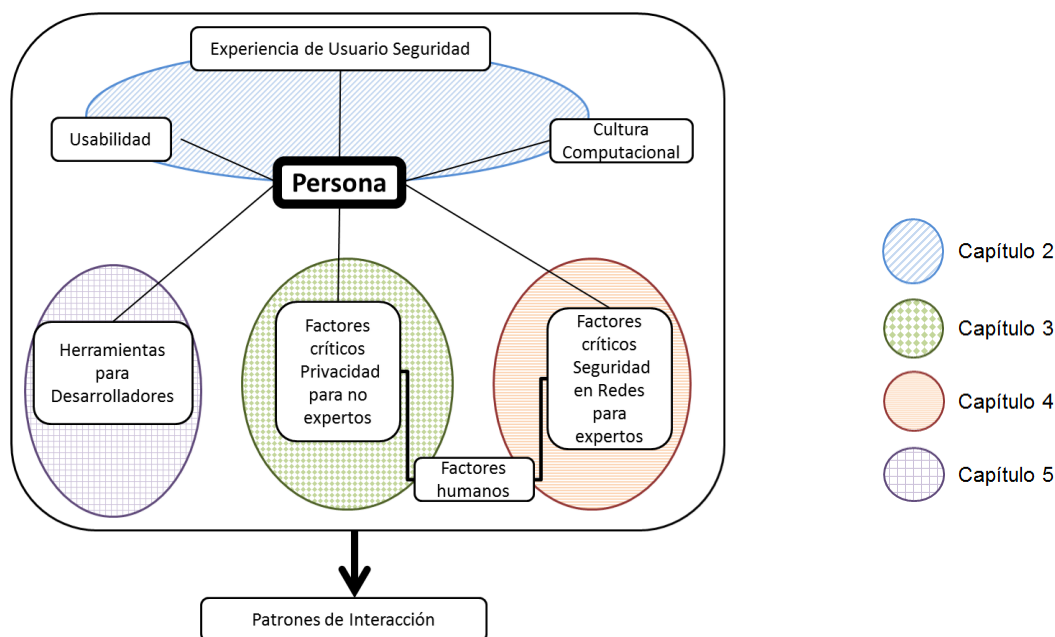


Fig. 1.2 Áreas de investigación abarcadas por capítulo

## Capítulo 2. Trabajo relacionado

---

*"La mayoría de las ideas fundamentales de la ciencia son esencialmente sencillas y, por regla general pueden ser expresadas en un lenguaje comprensible para todos"*

*Albert Einstein*

En este capítulo se presenta el trabajo relacionado que da sustento teórico a esta investigación en las áreas de Experiencia de usuario, Usabilidad, Patrones de Interacción y Seguridad Informática.

## 2. Trabajo relacionado

Desde diversas áreas del conocimiento se ha estudiado la interacción con factores críticos de seguridad. En este capítulo se presentan las contribuciones sobresalientes que resaltan la necesidad de un trabajo multidisciplinario para mejorar la relación de las personas con tópicos emergentes de seguridad.

### 2.1 Experiencia de usuario

Las limitaciones de los enfoques tradicionales para el diseño de productos interactivos olvidan incluir factores críticos como puede ser el comportamiento emocional del usuario (Ramírez-Barrera, 2012). Para crear experiencias exitosas no se debe enfocar todos los esfuerzos sólo en la usabilidad del producto sino también en crear sensaciones únicas, ayudar a conquistar aspiraciones, apelar a los cinco sentidos y al intelecto para comprometer a los usuarios creativamente. Es necesario a través de una personalidad tangible del producto crear recuerdos positivos y personales que alienten las relaciones con éste, haciéndolas duraderas y diferenciadas. La experiencia de usuario se involucra en la resolución del problema estratégico de la utilidad del producto y el problema psicológico del placer y la diversión de su uso.

La experiencia de usuario se define como el conjunto de percepciones, sensaciones y valoraciones del usuario resultado de la interacción con un producto, sistema o servicio en condiciones particulares considerando variables culturales. Se enfoca en tener un conocimiento profundo de las necesidades de los usuarios, de lo que valoran, de sus habilidades y sus limitaciones. Las mejores prácticas relativas promueven mejorar la calidad de la interacción de los usuarios (Rusu, 2014) ((HHS), 2004) (NNG., 2003). Los nuevos paradigmas de desarrollo de sistemas y la creciente cantidad y diversidad de los mismos exigen que la experiencia de usuario sea tan importante como los entregables mismos.

Nielsen & Norman Group (Nielsen & Normand, 1998), expertos en el área de usabilidad, proponen una definición que involucra una relación usuario-producto-empresa:

*"La experiencia del usuario abarca todos los aspectos de la interacción del usuario final con la empresa, sus servicios y sus productos. El primer requisito para una experiencia de usuario ejemplar es encontrar las necesidades exactas del cliente. Después viene la sencillez y la elegancia que producen los productos fáciles de usar. La verdadera experiencia del usuario va mucho más allá de dar a los clientes lo que ellos dicen que quieren, o proporcionar lista de verificación. A fin de alcanzar la experiencia de usuario de alta calidad en la oferta de una empresa debe haber una fusión sin fisuras de los servicios de múltiples disciplinas, incluyendo la ingeniería, el mercadeo, el diseño gráfico e industrial, y el diseño de interfaz"*

Para (Kankainen, 2002) la experiencia del usuario es resultado de una acción motivada en un contexto determinado, haciendo especial énfasis en la importancia condicionante de las expectativas del usuario y las experiencias previas, y por lo tanto en la capacidad de

influencia de la actual y futura experiencia. (Morville, 2004) recalca que para que exista una experiencia de usuario con valor y significado, la información debe de ser:

- Útil: Su contenido debe ser original y satisfacer una necesidad
- Usable: El sitio debe ser fácil de usar
- Deseable: imagen, identidad, marca, y otros elementos de diseño se utilizan para evocar emoción y apreciación
- Localizable: El contenido tiene que ser navegable y localizable en el sitio y fuera de este
- Accesible: El contenido tiene que ser accesible a personas con discapacidades
- Creíble: Los usuarios deben confiar y creer en lo que se les diga

### 2.1.1 Objetivos de la experiencia de usuario

De acuerdo a (Montero) la experiencia de usuario define tres objetivos:

- 1) **Expansión del concepto de interacción como unidad de análisis.** La experiencia de usuario representa un marco temporal más amplio que el concepto de interacción. Esta se inicia antes de que el usuario utilice el producto, en el momento en el que se crean expectativas acerca del mismo. Por otro lado, no finaliza cuando termina la interacción, ya que esta experiencia condiciona la valoración posterior del usuario acerca del producto, juicio que se modifica en el tiempo con el uso de otros productos.
- 2) **Expansión del concepto de usabilidad como atributo de calidad.** Desde esta perspectiva se entiende que la facilidad de uso no es el concepto central, ya que las emociones, la diversión, la utilidad o el placer de uso desempeñan un papel crucial.
- 3) **Expansión de los límites de la disciplina.** La experiencia de usuario y el diseño de las mismas son usados para incluir diferentes disciplinas de aportación significativa: ingeniería de usabilidad, diseño de interacción y arquitectura de la información.

### 2.1.2 Métodos de evaluación de la experiencia de usuario

A través de procesos objetivos en ambientes subjetivos se espera analizar, documentar y evaluar la experiencia de usuario. El trabajo de (Arhippainen, 2003) hace una breve revisión de metodologías adaptadas para evaluar cómo resulta la experiencia del usuario, y poder utilizar esa información para el diseño. La autora clasifica estos métodos en: Entrevistas y métodos de observación, guiones y relatos, prototipado de la experiencia, y diarios basados en papel y en voz. Por su parte, (Irons, 2003) defiende la importancia de los métodos etnográficos para suplir las carencias de los métodos de laboratorio propios de la ingeniería de la usabilidad.

El proyecto de (Hekkert, 2001) hace una revisión de diferentes técnicas para capturar la experiencia emocional, la experiencia estética y la relación de adhesión entre usuario y producto. Entre los métodos revisados se encuentra PrEmo (Desmet, Hekkert, & Hillen, 2003), una herramienta no-verbal basada en 18 animaciones de un personaje de cómic, donde cada animación representa una emoción. Cada participante escoge aquella animación que se corresponda con su propia reacción emocional ante el uso de un producto. Por su parte, (Rauschenberger & Medien-Systempartne, 2012) proponen una herramienta basada en User Experience Questionnaire (Laugwitz, 2008) para evaluar la interacción con un producto con poco esfuerzo y en distintos idiomas.

## **2.2 Usabilidad**

La usabilidad se refiere a la capacidad de un software o sistema interactivo de ser comprendido, aprehendido, usado fácilmente y atractivo para un usuario, en condiciones específicas de uso. Describe la efectividad con la que un producto fabricado por humanos permite alcanzar sus objetivos específicos (Nielsen J. , 1993) (Bevan, Kirakowsky, & Maissel, 1991) (Rosson & Carroll, 2002) . Desde la visión de Nielsen, pionero en la difusión de la usabilidad, ésta es un término multidimensional: indica que un sistema usable debe poseer los siguientes atributos: Capacidad de aprendizaje, eficiencia en el uso, facilidad de memorizar, tolerante a errores y subjetivamente satisfactorio.

Para Steve Krug, la usabilidad significa estar seguro de que algo funciona bien: que una persona con habilidades promedio, e incluso por debajo del promedio, pueda utilizar una cosa, ya sea un sitio web, un jet de combate, o una puerta rotatoria, para su fin sin terminar enormemente frustrado (Krug, 2006). Para Janice Redish (Redish, 1995) , el término usabilidad no se refiere solamente a hacer que los sistemas sean simples, sino que incluye la comprensión de los objetivos de los usuarios, el contexto de su trabajo y cuál es el conocimiento y la experiencia de que disponen. Consiste en proporcionar a los usuarios las herramientas para encontrar lo que necesitan, entender lo que encuentran, actuar apropiadamente sobre ese entendimiento y hacer todo esto con el tiempo y el esfuerzo que crean necesario.

Según (Shneiderman, Plaisant, Cohen, & Jacobs, 2009) (Preece, 1994), los principios a considerar para la creación de interfaces usables serían los siguientes:

- Estudiar la población de usuarios
- Reducir la carga cognitiva
- Aplicar técnicas de ingeniería para resolver la problemática del error humano
- Mantener consistencia y claridad.

### **2.2.1 Estándares relativos a la usabilidad**

En los últimos años se han desarrollado estándares relacionados con la disciplina de IHC en los comités ISO relativos a ergonomía, interfaces de usuario e ingeniería del software para establecer los requisitos mínimos de usabilidad para las interfaces y eliminar inconsistencias y variaciones. Expertos en usabilidad han trabajado con el subcomité de

ingeniería del software ISO/IEC JTC1/SC7 para integrar la usabilidad en la ingeniería y estándares de calidad del software. (Bevan, 1999)

Los estándares relativos a la usabilidad se refieren a los siguientes aspectos: uso del producto, interfaz de usuario e interacción, proceso llevado a cabo para el desarrollo del producto y capacidad de una organización para aplicar diseño centrado en el usuario.

Algunos de los estándares relevantes referentes a la usabilidad se citan a continuación:

- **ISO/IEC 9126 [ISO91]** Define la usabilidad como un atributo de la calidad del software, asociada al diseño y a la evaluación de la interfaz de usuario y la interacción. La usabilidad se analiza en términos de comprensibilidad, aprendizaje, operabilidad, atractividad y conformidad.
- **ISO/DIS 9241-11 [ISO93]** Este estándar define la usabilidad en términos de la calidad del trabajo de un sistema en uso, la cual depende de todos los factores que pueden influenciar el uso de un producto en el mundo real: factores de organización, diferencias individuales entre usuarios y experiencia. Para medirla se hace necesario identificar las metas y descomponer la efectividad, eficiencia y satisfacción, así como los componentes del contexto de uso en subcomponentes con atributos medibles y verificables.
- **ISO 13407 [ISO99]** Describe el diseño centrado en el usuario como una actividad multidisciplinar que incorpora factores humanos y el conocimiento de ergonomía y técnicas de trabajo con el objetivo de optimizar la eficacia y la productividad, mejorando las condiciones de trabajo y neutralizando los posibles efectos adversos del uso del sistema interactivo sobre la salud humana, la seguridad y el funcionamiento.
- **ISO TR 16982 [ISO02]** En este documento se presenta una lista de métodos ergonómicos que pueden ser aplicados a las diferentes etapas del ciclo de diseño, indicando sus ventajas y desventajas. Se presentan los métodos de evaluación tales como observación, cuestionarios, entrevistas, técnicas de diseño y evaluación participativa o métodos formales, que implican directamente a los usuarios finales.

### 2.2.2 Métodos de evaluación de usabilidad

La evaluación de la usabilidad, es una de las tareas más importantes que se emprende cuando se desarrolla una interfaz de usuario (Woodward, 1998). Se trata de un proceso que genera una medida de la facilidad de uso en el que intervienen el objeto a evaluar y un proceso a través del que se juzgan uno o más atributos (Karat & Helander, 1997). Para algunos autores como (Mayhew, 1999), la evaluación de la usabilidad es un estudio empírico con usuarios reales del sistema propuesto, con el propósito de dar retroalimentación en el desarrollo de software durante el ciclo de vida de desarrollo iterativo.

El propósito de evaluación de la usabilidad se resume como un proceso con los siguientes objetivos:

1. Proporcionar retroalimentación para mejorar el diseño
2. Valorar en qué medida se están consiguiendo cumplir los objetivos marcados frente a los usuarios y a la propia organización
3. Monitorear el uso a largo plazo de productos o sistemas

Existen diversas propuestas para la evaluación de la usabilidad y se han establecido clasificaciones de las mismas con base a diversos criterios. Algunos de estos métodos requieren un completo laboratorio de usabilidad con espacios independientes para el desarrollo de las pruebas y tecnología específica como cámaras de video y equipos especializados, y otros pueden llevarse a cabo con una interacción semiformal entre el grupo de desarrollo y los usuarios finales. Nielsen (Nielsen J. , 1993) sugiere que con una inversión pequeña en algún método de usabilidad puede obtenerse una mejora significativa para un sistema de software. Sin embargo, estos resultados pueden servir también como base para mejorar la experiencia de usuario (Hassan-Montero, 2006) (Paluch, 2006)

SUMI (Software Usability Measurement Inventory) y QUIS (Questionnaire for User Interaction Satisfaction) son estrictos cuestionarios utilizados para la usabilidad de un software desde el punto de vista del usuario final. Puede ser utilizado para evaluar nuevos productos, efectuar comparaciones con versiones previas y establecer objetivos para desarrollos futuros. (Kirakowski, 1994) (Norman, Shneiderman, & Harper, 1995). Por su parte, el cuestionario MUMMS (Measuring the Usability of Multi-Media) evalúa la medida en que el producto capta las respuestas emocionales del usuario, el grado de control con el que el usuario siente que él, y no el producto, va procediendo paso a paso; el grado de eficiencia con el que el usuario siente que puede conseguir los objetivos de su interacción con el producto, el nivel de ayuda y asistencia que el producto parece prestar al usuario y la facilidad de aprendizaje con la que un producto puede empezar y aprender nuevas características del producto (Kirakowski, 2004). El cuestionario SUS (System Usability Scale) desarrollado en 1986 sigue vigente hoy en día y su propósito consiste en establecer comparaciones cruzadas entre productos (Brook, 1998).

Por otro lado, WAMMI (Website Analysis and MeasureMent Inventory) es una herramienta de evaluación para sitios web, el cual permite predecir, monitorizar y obtener referencias sobre otros sitios similares (Claridge & Kirakowski, 1984). El proyecto SIRIUS propone un sistema de evaluación de la usabilidad Web orientado al usuario basado en la determinación de tareas críticas (Suárez-Torrente, 2011). IBM por su parte propone un método de evaluación subjetiva de interacción con un sistema en un escenario específico (Lewis, 1995).

## **2.3 Patrones de interacción**

Un patrón es un medio de comunicación que expresa una solución de interfaz en una forma textual y gráfica a un problema recurrente dentro de un contexto específico. Su especificación permite comunicar la experiencia y el conocimiento en un área específica (Gamma, Helm, Ralph, & Vlissides, 1995) (Borchers, 2001) Un patrón de interacción describe una solución exitosa a un problema recurrente relativo a la interfaz de usuario en un contexto dado (Hernández-Hernández, Alvarez-Carrión, & Muñoz-Arteaga, 2012). Sirve para describir relaciones visuales, estéticas y de satisfacción al mismo tiempo que define un problema, su contexto y solución. Esto facilita la comunicación entre miembros

de distintas disciplinas permitiendo registrar el conocimiento y la experiencia para construir prototipos de interfaz de usuario (Bayle, 1998) (Van-Welie, 2001) (Acosta & Zambrano, 2011) (Henninger, 2001).

### **2.3.1 Lenguaje de patrones de interacción**

Los lenguajes de patrones son representaciones que han sido usadas en diseño urbano y arquitectura desde los 70's para representar, de una forma generalizada, la interacción entre formas físicas y la conducta social (Bayle, 1998). Un lenguaje de patrones de interacción genera un diseño de espacio/tiempo que representa un modelo mental de las tareas de usuario con el objetivo de construir una interfaz humano-computadora lo más transparente posible. Se habla de un lenguaje de patrones cuando los patrones que forman la colección se encuentran conectados, cuando poseen relaciones asociativas entre sí que además posibiliten el uso de combinaciones de patrones para la solución de problemas complejos (Todd, Kemp, & Phillips, 2004).

La definición intencionalmente no se expresa para describir lo que es un solo patrón de interacción, pues la vinculación entre los patrones se considera tan importante como los propios patrones individuales. El objetivo de un lenguaje de patrones de interacción consiste en compartir soluciones de diseño IHC exitoso entre los profesionales de esta área y proporcionar un lenguaje común para cualquier persona involucrada en el desarrollo, evaluación, o el uso de sistemas interactivos (Borchers, 2001).

(Borchers, 2001) propone una estructura de patrón haciendo uso de un metapatrón, esto es, un patrón que permite describir patrones. En este metapatrón se definen los componentes requeridos en cualquier dominio de conocimiento. Es posible identificar a través de la literatura sobre el tema una serie de los elementos que los componen. (Moreno & Sánchez-Segura, 2003) (Hernández-Hernández, Alvarez-Carrión, & Muñoz-Arteaga, 2012) (Malone, Leacock, & Wheeler, 2005) (Varela-Tabuyo, 2005). No es necesario describir cada uno de los componentes para todos los patrones, salvo aquellos que son obligatorios: Nombre, Problema, Solución y Contexto. Asimismo, se propone una taxonomía que distingue tres dimensiones principales en las que se pueden clasificar los patrones de interacción:

1. Nivel de abstracción (objeto, estilo, tarea)
2. Función
  - a. Percepción (interfaz de salida)
  - b. Manipulación (interfaz de entrada)
  - c. Navegación
3. Dimensión física (espacio, secuencia, tiempo)

Mientras que las directrices de usabilidad describen reglas a seguir, los patrones de interacción además especifican el resultado deseado. (Spool, 2003) Es decir, una directriz de usabilidad representa una regla que si se cumple el diseño “estará bien”, y si no “estará mal”, mientras que un patrón especifica qué hacer para conseguir un objetivo concreto en un contexto determinado. Es decir, especifican cuándo, cómo y por qué la solución puede aplicarse (Welie, Veer, & Eliëns, 2000).

### 2.3.2 Colecciones significativas de patrones de interacción

Se realizaron búsquedas de patrones de interacción con los principales motores en Internet, hasta agotar las ligas que aportaban colecciones nuevas, desde el año 2009 hasta la fecha. Se evaluaron las colecciones encontradas para seleccionar las más significativas, entendiendo como “significativa” aquellas que demuestren algún grado de haber sido probadas, que abarquen algún área específica y que ha sido citada en otros trabajos. Enseguida se listan y describen aquellas que cumplen el criterio, y se deja al final la colección PrimeLife por ser ésta la más aproximada al presente trabajo.

Título: **Design for Quality**

Administrador: Elkee Folmer

URL: <http://www.designforquality.com/>

Descripción: Relación de patrones de usabilidad arquitectónicamente sensibles para aplicaciones software, es decir, propios del nivel estructural de la aplicación.

Idioma: Inglés

Título: **User Interface Design Patterns**

Administrador: Sari A. Laakso

URL: <http://www.cs.helsinki.fi/u/salaakso/patterns/>

Descripción: Patrones de interacción para el diseño de interfaces gráficas de usuario (GUIs).

Idioma: Inglés

Título: **Patterns in Interaction Design**

Administrador: Martijn van Welie

URL: <http://www.welie.com/>

Descripción: El sitio web presenta patrones de interacción para el Diseño Web, Interfaces Gráficas de Usuario (GUIs), e Interfaces de Dispositivos Móviles.

Idioma: Inglés

Título: **UI Patterns and Techniques**

Administrador: Jenifer Tidwell

URL: <http://time-tripper.com/uipatterns/>

Descripción: Patrones para Diseño de Interfaz.

Idioma: Inglés

Título: **HCI Pattern Collection – Version 2**

Administrador: Simone Fischer-Hübner

URL: [http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci\\_pattern\\_collection\\_v2-public.pdf](http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf)

Descripción: El documento presenta una colección para el manejo de la privacidad de datos personales en un contexto de leyes europeas

Idioma: Inglés

Título: **COPPEMA**

Publicación: (Murillo & Sánchez, Patrones de interacción y su aplicación a la privacidad en Internet, 2013)

Descripción: Colección para facilitar la percepción y manipulación de interfaces relativas a la privacidad de datos personales. Esta colección se sustenta en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

(Parlamentarios, 2010) y las relaciones entre la privacidad de datos personales e interfaz de usuario.

Idioma: Español

**Título: Privacy Patterns for Online Interactions**

Publicada por: Cranor, Lorrie Faith; Romanowsky, Sasha; Hong, Jason; Acquisti, Alessandro; y Friedman, Batya,

URL: <http://repository.cmu.edu/hcii/72>

Descripción: Publicación de tres patrones identificados para transacciones en sitios web: Consentimiento para transacciones web, Tráfico online enmascarado e Información mínima asimétrica.

**Colección PrimeLife**

Desde el 2008, el proyecto de investigación PrimeLife (Programme., 2010), sustentado por la Comunidad Europea, ha sido desarrollado para crear una colección de patrones de Interacción con el objetivo de definir directrices sobre cómo diseñar interfaces usables para mejorar la seguridad en los sistemas interactivos. Estas propuestas de IHC se estructuran en patrones relacionados con la privacidad, políticas de gestión, visualización de privacidad de información y flujos de trabajo, paradigmas de interacción, así como descripciones de maquetas interactivas de PET ( Privacy Enhancing Technologies). Sin embargo, estos son propuestos bajo un contexto de términos legales europeos y no existe evidencia de su implementación y uso en entornos latinoamericanos. En el Título de cada patrón se incluye una calificación de 5 estrellas (de 0 a 5 estrellas) para reflejar la cantidad de experiencia que se tiene de cada patrón. El esquema de calificación es el siguiente:

- 0 No hay ninguna prueba de usuario final.
- 1 Bajo nivel de conocimiento HCI incluido (en forma de principios de usabilidad)
- 2 Al menos se integró retroalimentación de dos usuarios.
- 3 Se han hecho más de dos evaluaciones de usuario.
- 4 Sólo necesita una ronda final de iteración.
- 5 Ha sido probado de manera exhaustiva y se considera una versión final.

Las cuatro categorías propuestas se listan a continuación:

- 1. PET patterns for privacy policies
  - a. Privacy Policy Display (\*\*\*)
  - b. Dynamic Privacy Policy Display (\*\*\*\*)
  - c. Policy Matching Display (\*\*)
- 2. PET Visualization
  - a. Privacy Icons (\*)
  - b. Icons for Privacy Policies
  - c. Privacy Awareness Panel in Collaborative Workspaces (\*\*\*\*)
- 3. PET Interaction
  - a. Secure Passwords (\*\*\*\*)
  - b. Informed Consent (\*\*\*\*)

- c. Privacy Aware Wording
  - d. Credential Selection (\*\*)
4. Descriptions of interactive PET Mock-ups
- a. Trust Evaluation of Services Sides (\*\*\*\*)
  - b. Data Track (\*\*\*)
  - c. Privacy Options in Social Networks
  - d. Selective Access Control in Forum Software (\*)
  - e. Privacy Enhanced Group Scheduling

Es relevante la propuesta de los patrones *Privacy Policy Display* y *Dynamic Privacy Policy Display*, cuyos modelos sugieren la representación mínima de un Aviso de Privacidad. Sin embargo ninguno de los dos propone un esquema para representar un Aviso de Privacidad extendido.

### 2.3.3 Impacto en el desarrollo de software

De acuerdo al trabajo de (Muñoz-Arteaga, Medina, Guerrero, & Muñoz-Lopez, 2010) se propone una clasificación de patrones especificando las mejores prácticas para diseñar la retroalimentación visual de un sitio web de manera que guíe y asista la tarea del usuario de una manera segura. Los patrones se han clasificado en función de los niveles de retroalimentación visual que tiene todo sitio web:

- **Nivel de Información:** Es el grupo de patrones de seguridad que describen al usuario de manera coherente y continua el estado en el que se encuentra el sitio web o alguno de sus procesos internos, necesarios en una transacción requerida por el usuario.
- **Nivel de Interacción:** Es el conjunto de patrones de seguridad que especifica el estado de diálogo entre el usuario y el sitio web por medio de la interacción con los elementos (servicios) de seguridad que se exponen en la interfaz.
- **Nivel de Interactividad:** Reagrupa los patrones de seguridad que especifican las acciones del usuario utilizando los dispositivos de entrada para manipular directamente los objetos de una aplicación.

El modelo teórico presentado por (Mendoza, 2009) propone un conjunto de conceptos para diseñar información de retroalimentación usable con respecto al área seguridad para aplicaciones web. Con esto se reconoce la importancia de disponer de un lenguaje común para proporcionar a los usuarios una interacción efectiva. Asimismo, esta categorización puntualiza la necesidad de disponer de una colección de patrones de interacción específica para el área de seguridad, hasta el momento inexistente en niveles consolidados de madurez. El trabajo de (Maurer, 2011) propuso un modelo de patrones gráficos interactivos para navegadores Firefox que alerta a los usuarios sobre las posibles consecuencias de ignorar advertencias para verificar la validez de un sitio web y descartar posible phishing. Los resultados de las pruebas aplicadas son alentadores al identificar interés en los usuarios por administrar la seguridad personal en un entorno gráfico.

Por su parte, (Acosta & Zambrano, 2011) describen un método para la construcción de la interfaz de usuario, basado en patrones de interacción. Este método puede integrarse en

un proceso de desarrollo de software orientado a objetos. Este método se inscribe en los modelos de desarrollo que incorporan el prototipado desde las primeras etapas del ciclo de vida de los sistemas. El objetivo principal de este método consiste en el desarrollo de un prototipo de la interfaz de usuario, generado a partir de los patrones de interacción. Este prototipo puede ser evaluado por otros expertos del grupo multidisciplinario y por el usuario y, así, el prototipo puede evolucionar hasta satisfacer los requerimientos del usuario, definiendo un proceso de ingeniería de requerimientos basado en patrones.

## **2.4 Seguridad y cultura informática**

La seguridad informática consiste en el aseguramiento de la integridad, autenticación, disponibilidad, no repudio, confidencialidad de la información y recursos que se usan para la entrada, almacenamiento, procesamiento y comunicación de los mismos sin dificultar las labores de los usuarios finales a un costo sustentable (Technology, 2000).

### **2.4.1 Cultura de seguridad informática en usuarios finales**

El número de usuarios de internet a nivel mundial continúa en aumento no así el índice de cultura de seguridad. En un estudio (AMIPCI, 2012) con usuarios de Internet mayores de edad, se observa que a nivel nacional el 13% de los internautas mayores de edad consideran que es responsabilidad de ellos mismos el debido tratamiento de su información, sin embargo, el 31% no pudo definir qué es un dato personal. El 11% de los evaluados ignora que el Derecho a la privacidad es un Derecho Constitucional. El 19% siempre lee el aviso de privacidad de un sitio en internet y al 62% de esta población le toma más de 4 minutos leerlo. El 61% de los internautas desconoce qué tratamiento le darán a sus datos personales en las redes sociales en las que se encuentran inscritos.

Estos datos revelan lo siguiente:

1. El creciente número de usuarios en internet carece de cultura de seguridad informática en el ámbito de la privacidad de datos.
2. Los internautas mayores de edad desconocen o no aplican medidas de seguridad en el tema.
3. Los mayores de edad son las personas responsables de educar a los jóvenes en estos temas.

### **2.4.2 Privacidad de datos**

El creciente uso de tecnologías de información ha provocado que los datos personales sean usados, en ocasiones, para fines distintos a los que fueron solicitados. Algunas veces, estos datos se transfieren a terceras instancias sin que el dueño de los mismos tenga conocimiento. El bajo índice de cultura de seguridad informática (AMIPCI, 2012) así como diseños de interfaz poco adecuados, hacen que el usuario promedio no aproveche las soluciones ofrecidas (Garfinkel & Faith, 2005). Desde la perspectiva de protección de

datos personales, el titular de dichos datos tiene el derecho y la libertad de decidir qué desea comunicar, cuándo y a quién, manteniendo el control sobre su información personal en todo momento (Datos, 2012).

La mayoría de los internautas acostumbran avanzar de forma rápida en todas las configuraciones previas al uso de un software sin leer los detalles (Murillo & Sánchez, 2013). Con ello, los sitios de Internet tienen registrado que los avisos de privacidad sí fueron leídos y se aceptaron los términos y condiciones del uso de los datos personales por parte de quien la recaba. Sin embargo, los usuarios suelen olvidar las consecuencias del compromiso aceptado consciente o inconscientemente. Cuando ya se lleva tiempo utilizando un software, los riesgos asociados a la información proporcionada en un inicio o durante el uso del mismo no son evidentes. Los usuarios interactúan con aplicaciones de forma cotidiana sin tener la certeza de qué puede suceder si un tercero hace mal uso de los datos capturados por ellos mismos.

Debido a lo anterior, cada vez más países han aprobado leyes que buscan proteger a las personas y no a los datos por sí mismos. Los primeros esfuerzos se dieron en Europa en 1967, con la Resolución 509 de la Asamblea del Consejo de Europa sobre los “derechos humanos y nuevos logros científicos y técnicos”. Al final de la década de los setentas Alemania, Francia, Dinamarca, Austria y Luxemburgo aprobaron leyes nacionales similares. Durante los años ochenta, el Consejo de Europa se pronunció sobre la protección de la intimidad frente a la potencial agresividad de las tecnologías, a través de la promulgación del Convenio No. 108 para proteger a las personas frente al tratamiento automatizado de sus datos. El propósito era garantizar a los ciudadanos de los Estados contratantes el respeto de sus derechos y libertades, en particular, el derecho a la vida privada. Todas estas disposiciones han planteado para los usuarios el derecho de acceder a su información y en caso de ser inexacta de rectificarla, el derecho a cancelar el dato cuando ya no es pertinente o ha perdido vigencia y el derecho a oponerse a su utilización por parte de un tercero (Programme., 2010) .

Algunos sistemas ofrecen opciones de manejo de privacidad en un lenguaje técnico o legal poco claro para un usuario promedio. Algunas personas, por curiosidad o necesidad, invierten tiempo en comprender los conceptos para fortalecer sus medidas de prevención o solucionar un problema. Sin embargo, cada software maneja los términos y simbología de forma distinta, lo que causa frustración y rechazo. En un trabajo publicado en 2011 (King, Lampinen, & Alex, 2011) se sugiere que hacer explícitos los riesgos de privacidad en una aplicación puede ayudar a los usuarios a tomar mejores decisiones con respecto a este tema. Esto, sin embargo, para cierto tipo de usuarios podría desalentar el uso de dichas aplicaciones pues tienen un diseño estático.

#### **2.4.2.1 Datos personales**

Se definen datos personales a cualquier información relacionada con una persona y forma parte de su identidad. Este tipo de datos permiten además, interactuar con otras personas, o con una o más organizaciones, así como que pueda ser sujeto de derechos. Le pertenecen a cada individuo y él decide a quién, para qué, cuándo y por qué los proporciona. Por ejemplo: nombre, teléfono, domicilio, fotografía o huellas dactilares, así como cualquier otro dato que pueda servir para identificarle (Parlamentarios, 2010).

Las principales categorías de datos definidos se presentan a continuación:

- Identificación (nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil)
- Laborales (puesto, domicilio, correo electrónico y teléfono del trabajo)
- Patrimoniales (información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos)
- Académicos (trayectoria educativa, título, número de cédula, certificados)
- Ideológicos (creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas)
- De salud (estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico)
- Características personales (tipo de sangre, ADN, huella digital)
- Características físicas (color de piel, iris y cabellos, señales particulares)
- Vida y hábitos sexuales, origen (étnico y racial)

### **Datos personales sensibles**

Son los datos que, de divulgarse de manera indebida, afectarían la esfera más íntima del ser humano. Ejemplos de este tipo de datos son: el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas y las preferencias sexuales.

#### **2.4.2.2 Ley federal de protección de datos personales en posesión de los particulares**

Esta ley regula la forma y condiciones en que deben utilizarse los datos personales por parte de personas físicas o morales en el ámbito privado. Tiene por objeto garantizar la protección de la información personal y a que se pueda ejercer el derecho a decidir, de manera libre e informada, sobre el uso que los entes privados darán a los datos. A esto se le conoce como "autodeterminación informativa" (Parlamentarios, 2010)

De acuerdo al Artículo 16 de esta ley se reconoce el derecho fundamental a que los datos personales sean protegidos. Por ello, todas las personas físicas o morales que cuenten con bases de datos están obligadas a seguir ciertas reglas que garanticen su uso adecuado y seguro.

Esta ley propone que el aviso de privacidad deberá contener, al menos, la siguiente información:

- I. La identidad y domicilio del responsable que los recaba;
- II. Las finalidades del tratamiento de datos;
- III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
- IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
- V. En su caso, las transferencias de datos que se efectúen, y

- VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

### **2.4.2.3 Aviso de privacidad e Interacción**

Cualquier empresa o entidad que solicite datos personales deberá elaborar y publicar un aviso de privacidad, documento a través del cual se podrá conocer la finalidad que tendrá la información que se pide al usuario. Este aviso debe proporcionar información que permita identificar a la empresa que recaba los datos y debe precisar la forma de hacer efectivos los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO). En el aviso de privacidad la empresa debe consultar si el usuario autoriza que se transfiera su información a terceros. La institución deberá notificar de cualquier cambio que se realice al mismo y pedir consentimiento para un nuevo uso que pretenda dar a los datos. Debe ponerse a disposición a través de medios físicos, digitales, visuales, sonoros o de cualquier otra tecnología.

Existen diversas guías (Datos, 2012) (Fácil, 2012) y herramientas que ayudan a generar un aviso de privacidad. Esto facilita la tarea de construirlo, cumpliendo el requisito de acuerdo a la ley. Sin embargo, la información generada mediante estos métodos no produce un documento claro para el usuario final. No existe un formato estándar, una definición clara de sus componentes o una forma de navegar a través de este documento que genere certidumbre y que esta experiencia se pueda trasladar a otros avisos de privacidad. Debido a esto y al bajo índice de cultura de seguridad informática, las personas no pueden reconocer y ejercer sus derechos en este rubro.

Algunos datos relevantes sobre la interacción con un aviso de privacidad se presentan a continuación (Mcdonald, Robert, Gage-Kelley, & Cranor, 2010):

- La gente esperaría ver una imagen, símbolo o ícono general que respalde el sitio en el cual está navegando sin tener que leer el extenso y ambiguo documento que lo avala.
- Algunos usuarios, ante la ambigüedad de los términos usados, están dispuestos a pagar por la protección de su privacidad, sin reconocer que esto es un derecho y responsabilidad de los mismos.
- Los usuarios no leen las políticas de privacidad si no se presentan en un formato corto
- Resulta difícil mapear conceptos simples a los términos usados en las políticas
- Formatos estándares reducen la libertad de acción por parte de las empresas
- Sería más efectivo educar a los usuarios para entender las consecuencias de la mala administración de su privacidad que educarlos para entender los formatos estándares de privacidad.

### **2.4.3 Visualización estandarizada de información personal**

Se han propuesto diversos lenguajes para expresar y automatizar las políticas de privacidad con propósitos informativos, de negociación y de cumplimiento. XACML y P3P

se presentan como dos lenguajes XML que sirven para construirlas y expresarlas de forma automática. (Cartas, 2008)

## **XACML**

De acuerdo a (Lockhart, 2013) y (Iervolino, 2013) el proyecto eXtensible Access Control Markup Language propone un estándar que proporciona la arquitectura, el protocolo y un lenguaje necesario para el intercambio de información basado en XML, éste permite la especificación tanto de políticas de control de acceso genéricas. Define cómo es la estructura de intercambio de mensajes de autorización y un modelo para organizar y almacenar la información de autorización. Dicho modelo impone una estructura base pero con flexibilidad suficiente para que cada sistema exprese las políticas de autorización de la forma más conveniente a su dominio de discurso (El-Aziz, 2013). Por ejemplo, un sistema podrá formar un modelo de autorización basado en usuarios, perfiles y páginas permitidas, mientras que otro podrá definirlo en términos de terminales, transacciones y tipos de producto. Diversos proyectos de investigación se han basado en este estándar para ofrecer soluciones técnicas para organizar la información desde la perspectiva de los administradores de la misma.

El trabajo presentado por (Esponda, 2007) propone una solución de autorización para servicios Web basado en XACML identificando situaciones en las cuales los sistemas de autorización pueden beneficiarse si adoptan un enfoque compatible con XACML. La investigación presentada por (Caviglione, 2013) analiza la situación actual del uso de políticas de control de acceso en redes sociales. Se identifican dos ideas esenciales: la interoperabilidad entre sistemas que usan lenguajes relativos a políticas de seguridad y la carencia de elementos en los lenguajes existentes al tratar de expresar términos de control de acceso en las mismas. Se propone XACML con un posible estándar.

## **GeoXACML**

GeoXACML (Geospatial eXtensible Access Control Markup Language) es una extensión geoespacial del estándar XACML para la declaración y aplicación de políticas de acceso a información geográfica. Uno de los principales organismos que desarrolla proyectos basado en este estándar es el Open Geospatial Consortium (Reed, 1994), consorcio de la industria internacional, agencias gubernamentales y universidades que soportan proyectos de soluciones interoperables de geoprocésamiento y servicios de localización basados en Tecnologías de Información. Por su parte, (Herrmann, 2010) propone un modelo de administración de capas que tiene la intención de apoyar una administración fácil, distribuida y jerárquica de las políticas de control de acceso espaciales complejas que se encuentran en las IDEs (Spatial Data Infrastructures). La Infraestructura de Datos Espaciales de Brasil (INDE) fue diseñada para difundir los datos geoespaciales producidos por organismos públicos, a excepción de los datos sensibles. Sin embargo, el Plan de Implementación de la INDE no especifica cómo utilizar las políticas de acceso a los datos disponibles. El proyecto propuesto por (Emerson & Wladimir, 2013) propone un sistema de control de acceso basado en GeoXACML como una solución para lograr este propósito, mejorando en 12% el tiempo de respuesta cuando se utiliza un servidor Web geoespacial. Por otro lado, el proyecto Certiloc (Gonzalez-Tablas, 2008) responde a la unión de los conceptos de “Certificación” y “Localización” y tiene como objetivo principal, la propuesta de un modelo teórico de un sistema informático respetuoso con la privacidad, que permita certificar digitalmente, la situación espacio-temporal de un dispositivo localizable mediante distintas tecnologías de localización.

## P3P

La Plataforma de Preferencias de Privacidad (Platform for Privacy Preferences) o P3P es un protocolo desarrollado por el World Wide Web Consortium (W3C) que permite a los sitios Web declarar las intenciones de uso de la información recopilada acerca de los usuarios que lo visitan y dar de esta forma un mayor control a éstos sobre su información personal cuando navegan, estableciendo un formato estándar para declarar la identidad y las prácticas sobre la información de los usuarios (Lindskog, 2003). Este formato basado en XML puede ser recuperado e interpretado por los navegadores de los usuarios. La especificación de P3P determina los siguientes tres puntos para definir la sintaxis y la semántica de las políticas de privacidad P3P:

- 1.- Un esquema de datos base de P3P, el cual es un esquema estándar de un amplio conjunto de datos que un sitio Web puede recolectar:
  - **Datos dinámicos:** describen el flujo de datos dinámicos que un usuario genera cuando visita un sitio Web. Por ejemplo, pueden describir el historial de artículos que un usuario revisó durante su visita al catálogo virtual de una tienda electrónica.
  - **Datos del usuario:** describen la información general de un usuario, por ejemplo, nombre, edad y domicilio.
  - **Datos de la empresa:** describen entidades legales y son usadas en interacciones usuario-empresa y empresa-empresa.
  - **Datos de terceros:** permiten a los usuarios y a las empresas informar sobre terceros, por ejemplo, los datos del cónyuge de alguien o de un socio.
- 2.- Un conjunto de usos, recipientes, categorías de datos y manifiestos de privacidad
- 3.- Un formato XML para expresar políticas de privacidad.

## Agentes lectores de políticas P3P

En esta sección se mencionan los principales prototipos de agentes lectores de políticas de privacidad basados en P3P.

### 1. W3C Prototype

W3C (Berners-Lee, 1997) desarrolló un prototipo de agente de P3P en el año 1997 para demostrar cómo los usuarios podrían especificar las preferencias de privacidad y recibir retroalimentación acerca de un sitio web. El prototipo, que era de dominio público, se demostró en una reunión de junio 1997 en la Comisión Federal de Comercio de Estados Unidos. Se evaluó la política de privacidad detrás de cada sitio que el usuario visitaba, y se hizo una comparación de la política del sitio con la configuración de las preferencias del usuario. En los sitios que no respondían a preferencias de un usuario, una ventana aparecía para notificar al usuario de la falta de correspondencia y dar a ella la opción de ignorar la desigualdad sólo por esta vez o cada vez que regresaba a la sitio. Presentaba noventa y ocho combinaciones de datos de en una matriz bidimensional. Su interfaz se consideró abrumadora y no prosperó.

## **2. Privacy Minder**

Este agente (Berners-Lee, 1997) basado en proxy utilizaba la versión de P3P desarrollado por AT&T. Este prototipo se basó enteramente en la configuración recomendada en forma de APPEL, que son conjuntos de reglas para especificar la preferencia de privacidad. Se consideró como un mejor diseño de interfaz con respecto al modelo de W3C, pero su uso tampoco prosperó.

## **3. Privacy bird**

Esta es una aplicación creada para el explorador Internet Explorer que informa al usuario sobre las políticas de seguridad que se maneja en la página web que visita (AT&T, 1999). Al ingresar a un sitio Web el motor de Privacy Bird se ejecuta buscando la declaración de políticas de seguridad y las compara con las preferencias que el usuario haya configurado al momento de la instalación o la última configuración. Este funciona como un el cuál funciona como un “objeto de ayuda para el navegador” (Esposito, 2011). La aplicación solo se puede utilizar desde la versión 6 hasta la versión 8 de Internet Explorer. La aplicación, al comparar las preferencias del usuario con las políticas de seguridad del sitio que se visita, mostrara iconos que van variando entre los colores verde, amarillo, rojo y gris. El verde indica confianza sobre el sitio. La imagen en amarillo, demuestra al usuario que el sitio Web no cuenta con políticas de seguridad en la plataforma P3P, en este caso el usuario queda expuesto a que el sitio haga con la información del usuario lo que sea (esto queda en duda ya que las políticas del sitio pueden ser expresadas en un documento “human-readable” y pueden ser atendidas por el usuario. La imagen en rojo, indica que las políticas de seguridad del sitio no coinciden con las preferencias del usuario.

El W3C y sus productos para estandarizar la verificación del uso de información privada en sitios web son una aportación valiosa en el sentido de que se mejora la seguridad del usuario final, exigiéndole a éste un conocimiento mínimo de todos los factores involucrados en los avisos de privacidad. Sin embargo, no abonan en el sentido de hacer eficiente el desarrollo de las aplicaciones ni la experiencia de usuario.

### **2.4.4 Administración de redes y seguridad**

El término *administración de redes* es definido como la suma total de todas las políticas y procedimientos que intervienen en la planeación, configuración, control y monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos; lo cual se verá reflejado en la calidad de los servicios ofrecidos. (Tanenbaum, 2010). El objetivo de la administración de la seguridad en una red consiste en ofrecer servicios de seguridad a cada uno de sus elementos así como a todo su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes (Dulaney, 2011)

#### **2.4.4.1 Herramientas de apoyo en la administración de redes**

Hoy en día, existen múltiples herramientas (Institute, 2000) que pueden ser implementadas en una red para administrar los principios básicos que un sistema seguro

debe cumplir: integridad, confidencialidad, disponibilidad y no repudio. En su mayoría este software cumple su objetivo técnico, sin embargo, ha sido desarrollado por expertos en seguridad, quienes no necesariamente lo son también en el área de interacción humano computadora, lo cual puede provocar que el diseño de la interfaz no sea lo más adecuado para todos los consumidores de esta tecnología. En algunos casos, esto causa frustración, pérdida de tiempo y hace que la experiencia adquirida por su uso no pueda aplicarse a otras herramientas de manera natural, obligando a que los usuarios se adapten a cada herramienta, y no viceversa; ahora cada usuario no solo debe ser experto en seguridad informática, sino también en manejo de interfaces. Con esto, los usuarios son los responsables de correlacionar y dar sentido a los resultados obtenidos por múltiples sistemas distribuidos, empleando diferentes técnicas, incluso manuales.

De acuerdo a (Foster & Vincent, 2006) más del 70% de los ataques contra las redes de las compañías vienen de la “Capa de aplicación” y no de la “Capa de red” de acuerdo al modelo de referencia OSI (Tanenbaum, 2010). Lo anterior indica que no se requiere un conocimiento profundo de programación, protocolos de ruteo o sistemas operativos, sino que se puede conseguir aplicaciones de fácil uso y causar daños severos. Contar con herramientas para predecir y mitigar los actos no deseados y detectar oportunamente “falsos positivos” dentro de una red es indispensable (Jackson, 2012) (Miller & Harris, 2011). De acuerdo a (Tipton & Micki, 2007), (Murillo, 2001) y (Systems, 2001) en cualquier organización es necesario contar con métodos centralizados para el control y acceso a la infraestructura de una red, sin embargo, con el paso de los años solo ha sido posible desarrollar aplicaciones de propósito específico y no resulta fácil su integración.

El control de acceso a la red basado en roles RBAC (Role Based Access Control) ofrece una alternativa al modelo de superusuario del tipo “todo o nada” (Peter, 2012) . Con RBAC, puede aplicar una política de seguridad en un nivel más específico. RBAC utiliza el principio de seguridad del **privilegio mínimo**. Privilegio mínimo significa que un usuario dispone exactamente de la cantidad de privilegios necesaria para realizar un trabajo. Los usuarios comunes tienen privilegios suficientes para utilizar sus aplicaciones, comprobar el estado de sus trabajos, imprimir o crear archivos. Las capacidades que van más allá de las propias se agrupan en perfiles de derechos. Los usuarios que realizarán trabajos que requieren algunas de las capacidades de superusuario asumen un rol que incluye el perfil de derechos adecuado. RBAC recopila las capacidades de superusuario en **perfiles de derechos** (Ferraiolo, 2007). Estos perfiles de derechos se asignan a cuentas de usuario especiales denominadas **roles**. Luego, un usuario puede asumir un rol para realizar un trabajo que requiere algunas de las capacidades de superusuario. Este esquema de personalización se refiere a las actividades que realizan las personas dentro del sistema definidas por un tercero, y no incluye otros factores de personalización como el gusto por hacer alguna tarea más que otra o asignación inteligente de tareas de acuerdo a desempeños previos.

Por su parte, las herramientas basadas en Command Line Interface (CLI) siguen siendo consideradas muy poderosas por permitir un manejo muy detallado de datos y parámetros, incluso sobre aquellas que cuentan con interfaz gráfica. Su uso exige que los usuarios conozcan la sintaxis de la sentencia que desean ejecutar, con el riesgo del error que se puede tener al teclear algo incorrecto (SANS, 2013) (Burns & Killion, 2007) (Ross, 2010). Según (Preece, 1994), se limitan las distracciones del usuario al no tener que estar atentos a mensajes de sistema, justificando así la alta carga cognitiva para el usuario. Durante años éstas han presentado este mismo formato y se sabe que para llegar a ser un experto en el área las personas deben adaptarse totalmente a ellas sin la

certeza de disponer de ambas versiones (versión gráfica y línea de comandos). Todas las categorías en las que se clasifican estas herramientas se basan en sus funciones técnicas sin considerar como básicos aspectos de interacción humano-computadora (INTECO, 2011)

#### **2.4.4.2 Usabilidad en herramientas de seguridad**

De acuerdo a (Tipton & Micki, 2007), (Murillo, 2001) y (Systems, 2001) en cualquier organización es necesario contar con métodos centralizados para el control y acceso a la infraestructura de una red, sin embargo, con el paso de los años solo ha sido posible desarrollar aplicaciones de propósito específico y no resulta fácil su integración. Las herramientas de seguridad deben cubrir de manera parcial o total las tareas de gestión de integridad, confidencialidad, disponibilidad, no repudio y autenticación (Dulaney, 2011) (Tanenbaum, 2010), sin considerar como básico el tópico de usabilidad.

Según (Nielsen, 1993) (ISO25010, 2011) la usabilidad está asociada con cinco atributos: facilidad para ser aprendido por nuevos usuarios, la eficiencia en su uso, la facilidad de recordar por usuarios ocasionales, la tolerancia a errores del usuario y la satisfacción subjetiva para el usuario. Sin embargo, de acuerdo a (Kandogan & Haber, 2005), una herramienta de apoyo a la seguridad tendría un alto grado de usabilidad si contara con formatos estándares que permitan una integración entre herramientas, aplicaciones de minería de datos, procesamiento automático de flujo de eventos, colaboración e intercambio de información, espacios de trabajo efectivos, escalables y personalizables con visualizaciones programables. Entre los administradores de seguridad, se considera que son usables si cumplen con su objetivo técnico específico para el cual fueron desarrolladas (Nemeth & Snyder, 2011). Por otro lado, (Marti, 2009) afirma que la presentación de informes, el análisis histórico y monitoreo en tiempo real son características de usabilidad relacionados con seguridad.

## **2.5 Factores humanos**

Sobre la conducta en los usuarios de tecnologías de información, se han detectado hechos que antes no existían. La investigación propuesta por (Madden & Lenhart, 2013) identificó que la proporción de jóvenes que usan redes sociales va en aumento y que los chicos de hoy comparten más información acerca de ellos mismos con personas desconocidas en estos sitios que las personas de la misma edad años atrás. Esto implica un cambio de cultura en temas de seguridad informática que no están siendo considerados. Se ha identificado por rangos de edades el tipo de información que se suele compartir. Sin embargo, sin importar el rango de edades, desconocen las malas consecuencias o actos indeseados de dichos actos. Se ha identificado que cierto sector de jóvenes deja en default todas las opciones que tienen que ver con el manejo de privacidad en los sitios que visita. Esto es alarmante, pues la curiosidad característica de estas edades no los invita a indagar los riesgos asociados a esta acción (King, Lampinen,

& Alex, 2011) . Tampoco muestran preocupación (ni sus padres) por quiénes y con qué frecuencia tienen acceso a la información que ellos mismos publican (Schlegel, 2011). Desde la Psicología y Diseño gráfico se ha buscado adaptar los factores de diseño de interfaces a las necesidades emergentes para mejorar la experiencia de usuario con aplicaciones interactivas. Algunos trabajos de investigación han comprobado que considerar estilos de aprendizaje en la creación de interfaces mejora la experiencia de usuario y su aplicación facilita la ergonomía cognitiva de los mismos. Las propuestas de (Velasco-Santos, Sánchez-Guerrero, & Laureano-Cruces, 2009) y de (Velasco-Santos, Laureano-Cruces, Mora-Torres, & Herrera-Bautista, 2011) presentan propuestas de combinaciones de colores para cada uno de los tipos de aprendizaje tomando en cuenta el tipo de inteligencia predominante en el usuario, aplicados todos ellos a un Sistema de Aprendizaje Inteligente.

En el trabajo presentado por (López, 2011) se hace un análisis de los resultados obtenidos en un estudio, comparando los promedios de aprovechamiento de un grupo de prueba que emplearon tres diferentes propuestas de interfaces educativas, llevado a cabo en condiciones experimentales controladas. Se emplearon principios teóricos de teoría del color, aprendizaje significativo, percepción visual y visualización de la información para construir las interfaces educativas. Los resultados indican que el uso inadecuado del color en las interfaces puede obstruir el aprendizaje. Estos resultados hacen evidente que las teorías del diseño, en este caso considerando el color como un factor crítico en la construcción de interfaces, pueden ser muy útiles para crear ambientes virtuales eficientes.

Algunos proyectos han estudiado la relación de factores humanos con el tema de seguridad informática. Se ha demostrado que las personas pueden generar contraseñas alfanuméricas seguras utilizando letras, números y símbolos asociados a alguna frase que solo tiene sentido para él mismo (Komanduri & Shay, 2011) (Schaub & Walch, 2013). Las contraseñas gráficas tienen un mayor grado de aceptación entre los usuarios de aplicaciones que aquellos muy seguros generados por complejos algoritmos, pues no se recuerdan con facilidad (Stobert & Biddle, 2013) y se escriben en sitios vulnerables a técnicas de ingeniería social aplicadas por personas con malas intenciones (Wiedenbeck & Birget, 2005).

Por su parte, el trabajo propuesto por (Colwill, 2009) reconoce que la seguridad informática en una empresa gira en torno a factores humanos, como lo es la confianza y la buena voluntad de las personas, pues el manejo de información sensible requiere conocimiento de la organización y ubicación de los activos valiosos. Los controles de seguridad tienen que ser viables en una variedad de entornos, teniendo en cuenta que el eslabón más débil de este control son las mismas personas que los usan.

De acuerdo a (Islam & Dong, 2008) diversos factores humanos pueden afectar profundamente los resultados y la eficiencia del desarrollo de software relativo a la seguridad de una red. El desarrollo incluye actividades como la identificación de activos, amenazas y riesgos, cuantificación y evaluación de consecuencias, presentación de informes y mitigación de riesgos. Este proceso es lento y costoso, y debe comenzar desde las primeras fases de la implementación del software. Los factores humanos involucrados en todo el proceso (individuales, del equipo de trabajo y de los socios de negocio) juegan un papel importante para lograr con éxito la gestión de la red en cuestión y se deben ver reflejados en la aplicación. Por su parte, (Hawkey & Botta, 2008) identifican cómo los factores humanos pueden estar relacionados con técnicas de

seguridad informática y los clasifican en nueve áreas: influencias externas, errores humanos, gestión, organización, funcionamiento y gestión de recursos, problemas de políticas, tecnología y capacitación. El trabajo de (Rajbhandari, 2013) determina que los métodos de análisis y gestión de riesgos (Risk Analysis and Management Methods) relativos a seguridad informática deben incluir los factores humanos, tales como la motivación, personalización de espacios y herramientas de trabajo, para mejorar el impacto en la organización.

Diversos factores humanos afectan de manera directa a actividades de generar (Miloslav, 2010) y recordar (Kraemer, 2006) una contraseña de acceso a un sistema, usabilidad de métodos de encriptación, implementación de políticas de seguridad y procedimientos de monitoreo en una red de cómputo y comunicaciones. Los principales factores humanos que afectan estas actividades son citadas en el trabajo de investigación presentado por (Gagne & Beznosov, 2008) :

- Carencia de entrenamiento en seguridad
- Carencia de cultura en seguridad
- Diferentes percepciones de los riesgos

## 2.6 Áreas de oportunidad

La problemática que se estudia en esta investigación se puede analizar desde distintos enfoques (Ver Fig. 1.3). Al finalizar la revisión de los trabajos previos se resumen los temas de impacto que pueden aportar los conceptos básicos para este trabajo. Ver de la Tabla 2.1 a la 2.5.



**Fig. 1.3** Enfoques de estudio

**Tabla 2.1** Trabajos relacionados y áreas de oportunidad sobre experiencia de usuario

| Área de conocimiento   | Antes de este trabajo                                                                                                                                                                                                                                                                                                                       | Área de oportunidad                                                                                                                                                                                                                        |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Experiencia de usuario | <ul style="list-style-type: none"> <li>Definición, alcances, limitaciones, (Ramírez-Barrera, 2012) (Nielsen &amp; Normand, 1998)</li> <li>Mejores prácticas (Rusu, 2014) (Morville, 2004)</li> <li>Métodos de evaluación (Arhippainen L., 2003) (Irons, 2003) (Laugwitz, 2008)</li> <li>Métodos de documentación (Hekkert, 2001)</li> </ul> | <ul style="list-style-type: none"> <li>Se carece de documentación de su aplicación en entornos de seguridad informática.</li> <li>Se desconoce la percepción de las personas al interactuar con factores críticos de seguridad.</li> </ul> |

**Tabla 2.2** Trabajos relacionados y áreas de oportunidad sobre usabilidad

| Área de conocimiento | Antes de este trabajo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Área de oportunidad                                                                                                                                                                       |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usabilidad           | <ul style="list-style-type: none"> <li>Definición, alcances, limitaciones (Nielsen J. , 1993) (Bevan, Kirakowsky, &amp; Maissel, 1991) (Rosson &amp; Carroll, 2002) (Krug, 2006)</li> <li>Principios de interfaces usables (Shneiderman, Plaisant, Cohen, &amp; Jacobs, 2009) (Preece, 1994)</li> <li>Retroalimentación usable en web (Mendoza, 2009)</li> <li>Estándares (Bevan, 1999)</li> <li>Métodos de evaluación (Woodward, 1998) (Karat &amp; Helander, 1997) (Mayhew, 1999) <ul style="list-style-type: none"> <li>SUMI, QUIS (Mayhew, 1999)</li> <li>(Norman, Shneiderman, &amp; Harper, 1995) MUMMS (Kirakowski, 2004)</li> <li>SUS (Brook, 1998)</li> <li>WAMMI (Claridge &amp; Kirakowski, 1984)</li> </ul> </li> <li>Usabilidad para administradores de seguridad (Tipton &amp; Micki, 2007) (Kandogan &amp; Haber, 2005) (Marti, 2009) (Nemeth &amp; Snyder, 2011)</li> </ul> | <ul style="list-style-type: none"> <li>Se carece de documentación de su aplicación en entornos de administración de privacidad de datos personales y administración de una red</li> </ul> |

**Tabla 2.3** Trabajos relacionados y áreas de oportunidad sobre patrones de interacción

| Área de conocimiento    | Antes de este trabajo                                                                                                                                                                                                                          | Área de oportunidad                                                                                                              |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Patrones de interacción | <ul style="list-style-type: none"> <li>Definición (Borchers, 2001) (Gamma, Helm, Ralph, &amp; Vlissides, 1995)</li> <li>Lenguajes de patrones (Todd, Kemp, &amp; Phillips, 2004)</li> <li>Colecciones existentes (Programme., 2010)</li> </ul> | Definir elementos y métodos para construir patrones de interacción que mejoren la interacción con factores críticos de seguridad |

**Tabla 2.4** Trabajos relacionados y áreas de oportunidad sobre seguridad informática

| Área de conocimiento  | Antes de este trabajo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Área de oportunidad                                                                                                                                                                                                                                                                                                                               |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Seguridad informática | <ul style="list-style-type: none"> <li>Estadísticas nacionales               <ul style="list-style-type: none"> <li>Uso de internet (AMIPCI A. M., 2012)</li> <li>Cultura de seguridad informática (AMIPCI A. M., 2012)</li> </ul> </li> <li>Responsabilidades, buenas prácticas, procedimientos, alcances y limitaciones que se ofrece desde la perspectiva técnica (Technology, 2000)</li> <li>Situación actual sobre Privacidad de información (Murillo &amp; Sánchez, 2013) (King, Lampinen, &amp; Alex, 2011) (Parlamentarios, 2010) (Datos, 2012)</li> <li>Estudios sobre visualización de Avisos de privacidad (Mcdonald, Robert, Gage-Kelley, &amp; Cranor, 2010), (Cartas, 2008)</li> <li>Herramientas para construir aplicaciones de privacidad (El-Aziz, 2013) (Reed, 1994) (Lindskog H. , 2003)</li> <li>Situación actual sobre Administración de redes (Dulaney, 2011)</li> <li>Herramientas para Administración de redes (Institute, 2000) (Foster &amp; Vincent, 2006) (Tipton &amp; Micki, 2007) (Murillo S. , 2001)</li> <li>Las herramientas cumplen sus objetivos técnicos y son diseñadas, construidas y operadas por expertos del área de seguridad. (Garfinkel &amp; Faith, 2005) (Systems, 2001)</li> <li>Herramientas basadas en línea de comandos (SANS, 2013) (Burns &amp; Killion, 2007) (Ross, 2010)</li> </ul> | <ul style="list-style-type: none"> <li>Se desconocen cuáles son los factores críticos para la óptima administración de privacidad de datos personales y administración de una red y sus correlaciones con otros factores humanos y de interfaz.</li> <li>Se carece de herramientas que faciliten el desarrollo de aplicaciones usables</li> </ul> |

**Tabla 2.5** Resumen de trabajos relacionados y áreas de oportunidad sobre factores humanos

| Área de conocimiento | Antes de este trabajo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Área de oportunidad                                                                                                                                                               |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Factores humanos     | <ul style="list-style-type: none"> <li>• Impacto social de redes sociales (Madden &amp; Lenhart, 2013)</li> <li>• Riesgos asociados a la privacidad (King, Lampinen, &amp; Alex, 2011) (Schlegel, 2011)</li> <li>• Estilos de aprendizaje en interfaces mejora la experiencia de usuario (Velasco-Santos, Sánchez-Guerrero, &amp; Laureano-Cruces, 2009) (Velasco-Santos, Laureano-Cruces, Mora-Torres, &amp; Herrera-Bautista, 2011) (López, 2011)</li> <li>• Factores humanos aplicados a la generación de passwords seguros (Komanduri &amp; Shay, 2011) (Schaub &amp; Walch, 2013) (Miloslav, 2010)</li> <li>• Ingeniería social (Stobert &amp; Biddle, 2013) (Wiedenbeck &amp; Birget, 2005)</li> <li>• Se ha estudiado la relación de las personas con la seguridad dentro de empresas como individuo y como parte de un equipo de trabajo (Colwill, 2009)</li> <li>• Factores humanos determinan eficiencia del desarrollo de software (Islam &amp; Dong, 2008)</li> <li>• Factores humanos y su relación con Seguridad informática (Hawkey &amp; Botta, 2008)</li> <li>• Factores humanos y análisis de riesgos (Rajbhandari, 2013)</li> <li>• Factores humanos y monitoreo de una red (Gagne &amp; Beznosov, 2008)</li> </ul> | Se desconoce cuáles son los factores críticos humanos que se relacionen con la seguridad para sugerir esquemas de desarrollo de interfaces que mejoren la experiencia de usuario. |

### Capítulo 3. Administración de datos personales e Interfaz de Usuario

---

*“El fin jamás justificará los medios para violar la privacidad y confidencialidad de otros”*

*Gabriel Carrillo Navas*

En este capítulo se identifican las correlaciones significativas entre factores críticos de administración de datos personales, factores humanos e interfaz de usuario mediante un análisis de la estructura actual de dichos avisos conforme los parámetros que exige la ley, la percepción que se tiene de la información dentro del mismo y un estudio etnográfico.

### 3. Administración de datos personales e Interfaz de usuario

Dado que la administración de datos personales en las aplicaciones en internet es un proceso importante para los usuarios finales, se hace mandatorio investigar en México la percepción que se tiene de la información en un aviso de privacidad y también si la estructura de dichos avisos está completa de acuerdo a lo que exige la ley y que cumple las expectativas de los usuarios.

#### 3.1 Elementos de un aviso de privacidad y su relación con el usuario de Internet

Como se ha mencionado en el apartado **2.4.2 Privacidad de datos**, la interacción con un aviso de privacidad determina para los usuarios de internet niveles de seguridad en torno a sus datos personales para el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición). En este capítulo se identifica la percepción general del usuario ante la tarea de reconocer en las páginas de Internet los elementos para ejercer los derechos ARCO. Para esto, se investiga si los avisos de privacidad cumplen con los elementos requeridos por la ley y se documentan factores humanos de interacción.

##### 3.1.1 Metodología

Durante el periodo académico Otoño 2012 quince personas consultaron quince páginas de Internet entre los meses de noviembre y diciembre de 2012:

- |                           |                          |                                  |
|---------------------------|--------------------------|----------------------------------|
| 1. Telmex.com.mx          | 6. Iusacell.com.mx       | 11. Hospitalbetania.com.mx       |
| 2. Esmas.com.mx           | 7. Unefon.com.mx         | 12. Beneficienciaespanola.com.mx |
| 3. Seccionamarilla.com.mx | 8. Mecagable.com.mx      | 13. Upaep.mx                     |
| 4. Tvazteca.com.mx        | 9. Hospitalpuebla.com.mx | 14. Itesm.mx                     |
| 5. Telcel.com.mx          | 10. Sanatorio.com.mx     | 15. Cemexmexico.com              |

Las personas participaron de manera voluntaria y no se ofreció algún tipo de recompensa por su actividad. Fueron 8 hombres y 7 mujeres. Se les explicó la función de un aviso de privacidad y sus componentes. Se trabajó en sesiones de una hora diaria con un descanso de cinco minutos entre cada aviso de privacidad. Cada consulta se hizo directamente en una computadora y se les pidió que al encontrar cada elemento del aviso de privacidad, la reportaran en un formato electrónico predefinido, permitiéndoles hacer anotaciones adicionales en papel. Al finalizar, se les pidió a los participantes que con base a una escala Likert calificaran cada uno de los siguientes seis enunciados:

“En relación a los avisos de privacidad de las páginas de internet y mi seguridad:”

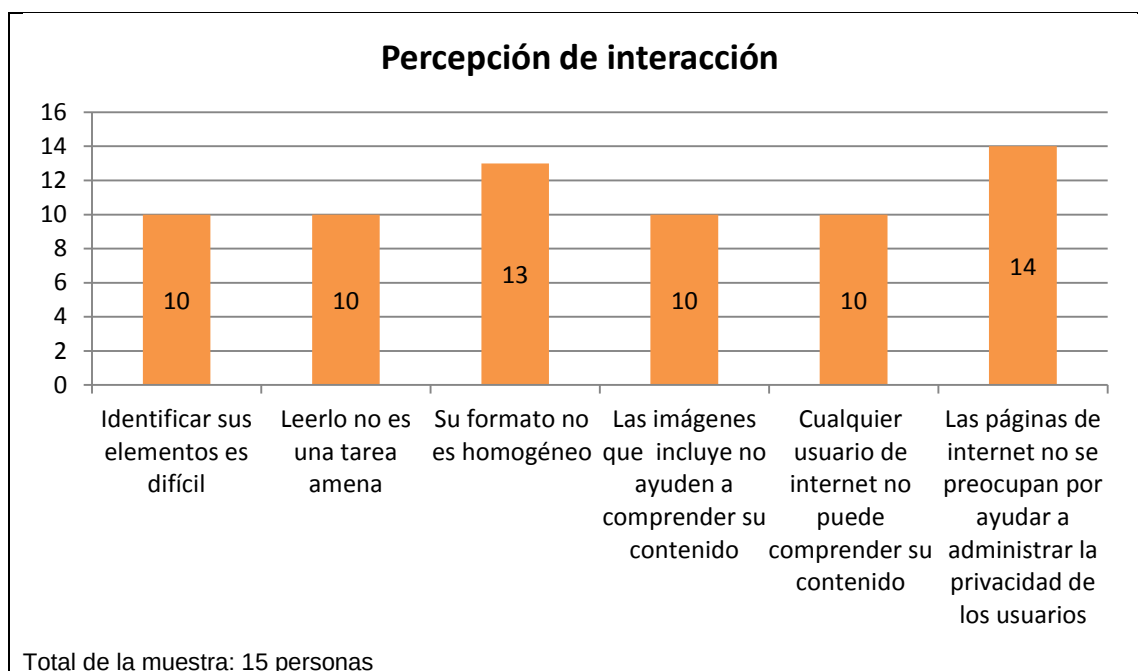
1. Es muy fácil identificar los elementos de un aviso de privacidad
2. Es una tarea muy amena leer un aviso de privacidad
3. Percibo que las páginas de internet se preocupan por ayudarme a administrar mi privacidad
4. El formato general de un aviso de privacidad es homogéneo en todas las páginas que visito

5. Las imágenes que se incluyen en los avisos de privacidad me ayudan a comprender su contenido
6. Considero que cualquier usuario de internet puede comprender el contenido de un aviso de privacidad.

### 3.1.2 Resultados acerca de la percepción de interacción

Al finalizar el estudio dirigido, se observó lo siguiente:

1. 10 personas estuvieron totalmente en desacuerdo que identificar los elementos de un aviso de privacidad fuera fácil.
2. 10 personas estuvieron en desacuerdo que leer un aviso de privacidad fuera una tarea amena.
3. 14 personas perciben que las páginas de internet no se preocupan por ayudar a administrar la privacidad de sus usuarios.
4. 13 personas consideran que el formato no es homogéneo en las páginas de Internet que visita.
5. 10 personas está en total desacuerdo respecto a que las imágenes que actualmente se incluyen en los avisos de privacidad ayuden a comprender su contenido.
6. 10 personas no está de acuerdo en que cualquier usuario de internet puede comprender el contenido de un aviso de privacidad.

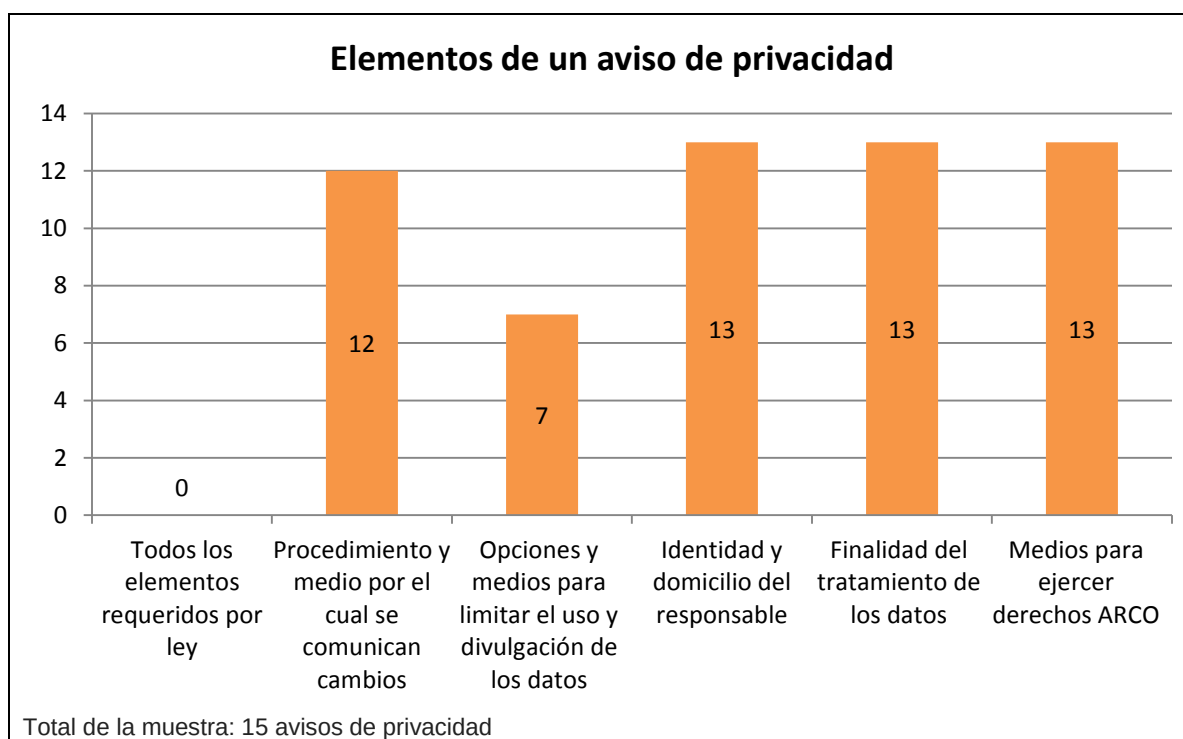


**Fig. 3.1** Percepción de interacción con un aviso de privacidad

### 3.1.3 Resultados acerca de la estructura de un aviso de privacidad

Al finalizar el estudio dirigido, se observó lo siguiente (Ver Fig. 3.2):

1. Ningún aviso de privacidad mostró todos los elementos requeridos por ley.
2. Los elementos obligatorios *Identidad y domicilio del responsable*, *Finalidad del tratamiento de los datos* y *Medios para ejercer derechos ARCO* se encontraron en 13 elementos del total de la muestra
3. El elemento obligatorio *Procedimiento y medio por el cual se comunican cambios en el Aviso de Privacidad* se encontró en un 12 elementos del total de la muestra
4. El elemento obligatorio *Opciones y medios para limitar el uso y divulgación de los datos* se encontró en 7 elementos del total de la muestra
5. Dos elementos de la muestra presentan de 2 a 3 (de los 6 que son obligatorio) elementos de un aviso de privacidad.



**Fig. 3.2** Elementos presentes en los avisos de privacidad

### 3.1.4 Discusión sobre la interacción con un aviso de privacidad

Para proteger a los usuarios de Internet la ley actual exige la presencia de un aviso de privacidad en todas las páginas de Internet albergadas en dominios nacionales. Para evitar la multa correspondiente por no tenerlo, las empresas lo generan utilizando

cualquier mecanismo y lo hacen público, sin embargo, el usuario final no dispone de una interfaz homogénea para ejercer sus derechos relativos a este tema y tener el impacto esperado.

La mayoría de las personas desconocen lo qué es un aviso de privacidad, sus elementos y los derechos y obligaciones asociados. Las pocas personas que hacen un esfuerzo por comprenderlo no pueden trasladar su experiencia de uso a otras páginas debido a las inconsistencias de formatos. Además, se percibe que las mismas páginas no muestran intención de ayudar al usuario.

Los avisos actuales solo generan frustración, aburrición o indiferencia y esto es preocupante, pues no se está fomentando la mejora de la cultura de la seguridad informática. Si esto sucede con personas de educación superior, no se esperarían mejores resultados al encuestar a adolescentes o adultos poco preocupados por su integridad cibernética.

### **3.1.5 Conclusión**

Las personas y las aplicaciones de generación automática que construyen los avisos de privacidad no disponen de herramientas, patrones, íconos y formatos universales que ayuden al usuario final en su correcta identificación, lectura y comprensión de elementos básicos de privacidad. Si existiera un formato estándar para presentar la información, los usuarios podrían identificar cada elemento de manera sencilla y oportuna. A los usuarios se les exige que conozcan términos de seguridad informática que no están claramente definidos en un lenguaje de seguridad experto y pueden tener diversas interpretaciones al momento de su implementación, lo que causa confusión. A partir de esto, se sugieren dos cosas. La primera, estudiar las relaciones entre la interfaz de usuario y factores (técnicos y humanos) de privacidad para proponer esquemas que mejoren la experiencia de navegación. Y por otro lado, estudiar si los responsables de construir aplicaciones que involucran temas de privacidad tienen a su disposición herramientas de software que faciliten esta tarea. Ambos aspectos se han estudiado como parte del presente proyecto y se discuten a continuación.

## **3.2 Privacidad en Internet: factores técnicos y humanos**

En este capítulo se presenta la relación actual entre factores críticos de privacidad de los datos personales y la interfaz de usuario a través de un estudio etnográfico. Dado que cada persona cuenta de manera individual con un perfil de aprendizaje (factor humano), se hace lógico identificar la relación de dicho perfil con la administración de privacidad de datos en el contexto del Internet. Se persiguen los siguientes objetivos específicos:

1. Identificar la relación actual de factores (técnicos y humanos) involucrados en el uso de Internet y la privacidad de su información.
2. Establecer una relación entre la administración de la privacidad y estilos de aprendizaje de los usuarios de Internet como posible aportación a esta investigación.
3. Reconocer los factores críticos considerados por los usuarios para administrar su privacidad.

### **3.2.1 Estilos de aprendizaje e Interfaz de usuario**

A la luz de la neurofisiología y psicología, se han propuesto modelos de rasgos cognitivos, afectivos y fisiológicos que sirven como indicadores de cómo las personas perciben interacciones y responden a sus ambientes de aprendizaje (México, 2012). Se les denomina estilos de aprendizaje y han contribuido al proceso educativo en los últimos años (Lindskog, 2003). Algunos proyectos de investigación han sugerido su aplicación para generar interfaces que faciliten la ergonomía cognitiva de los usuarios (Malhortra, 2008) (Vélez, y otros, 2005). En este capítulo se explora la posibilidad de considerar el estilo de aprendizaje basado en la topología de (CHAEA, 2002) como un factor determinante en la experiencia de usuario con factores de seguridad.

### **3.2.2 Metodología**

Se realizó un análisis cuantitativo de datos mediante un análisis paramétrico utilizando frecuencias y coeficientes de correlación (Malhortra, 2008). Se aplicó Análisis de Frecuencias y método de Correlación de Pearson utilizando el software SPSS para identificar las relaciones entre las variables.

En se aplicó una encuesta a 280 alumnos dentro de una universidad en la ciudad de Puebla, México, cuya población total a ese momento era de 8157 estudiantes. Para que el muestreo fuera significativo, el número de encuestados fue proporcional a la cantidad total de alumnos por cada carrera. Solo 275 encuestas fueron útiles para el estudio. Esto presenta un nivel de confianza del 95% con un error de 5.81%.

#### **Datos demográficos del análisis**

Los factores demográficos se consideraron son: Carrera, Semestre, Sexo y Edad como se ve en la Tablas 3.1, 3.2, 3.3 y 3. 4.

Se indagó sobre el estilo de aprendizaje predominante de los participantes. Se reconoce la presencia significativa de los cuatro estilos en toda la muestra (Ver Tabla 3.5)

**Tabla 3.1 Carrera**

| Válidos                          | Frecuencia | Porcentaje |
|----------------------------------|------------|------------|
| Admón. Bursátil                  | 1          | .4         |
| Admón. de Empresas               | 5          | 1.8        |
| Agronomía                        | 3          | 1.1        |
| Ambiental                        | 11         | 4.0        |
| Arquitectura                     | 10         | 3.6        |
| Autopartes                       | 2          | .7         |
| Banca y finanzas                 | 1          | .4         |
| Biónica                          | 5          | 1.8        |
| Biología                         | 2          | .7         |
| Ciencias políticas               | 1          | .4         |
| Cine                             | 7          | 2.5        |
| Comercio Exterior                | 4          | 1.5        |
| Comercio Internacional           | 6          | 2.2        |
| Computación y Sistemas           | 3          | 1.1        |
| Comunicación                     | 6          | 2.2        |
| Contaduría y Alta dirección      | 5          | 1.9        |
| Derecho                          | 6          | 2.2        |
| Diseño Automotriz                | 6          | 2.2        |
| Diseño Gráfico                   | 2          | .7         |
| Diseño y Producción Publicitaria | 11         | 4.0        |
| Economía                         | 1          | .4         |
| Electrónica                      | 4          | 1.5        |
| Enfermería                       | 7          | 2.5        |
| Filosofía                        | 3          | 1.1        |
| Fisioterapia                     | 5          | 1.8        |
| Gastronomía                      | 9          | 3.3        |
| Humanidades                      | 2          | .7         |
| Civil                            | 5          | 1.8        |
| Software                         | 2          | .7         |
| Industrial                       | 11         | 4.0        |
| Química                          | 2          | .7         |
| Instituciones                    | 5          | 1.8        |
| Inteligencia y Dslo. de Negocios | 4          | 1.5        |
| Tecnologías de Información       | 1          | .4         |
| Manufactura de Autopartes        | 2          | .7         |
| Mecatrónica                      | 9          | 3.3        |
| Medicina                         | 71         | 25.8       |
| Mercadotecnia                    | 5          | 1.8        |
| Nutrición                        | 4          | 1.5        |
| Odontología                      | 9          | 2.9        |
| Pedagogía                        | 2          | .7         |
| Periodismo                       | 1          | .4         |
| Psicología                       | 5          | 1.8        |
| Psicopedagogía                   | 2          | .7         |
| Relaciones internacionales       | 3          | 1.1        |
| Veterinaria                      | 4          | 1.5        |
| Total                            | 275        | 100.0      |

**Tabla 3.2 Semestre**

| Válidos  | Frecuencia | Porcentaje |
|----------|------------|------------|
| 1        | 46         | 16.7       |
| 2        | 8          | 2.9        |
| 3        | 47         | 17.1       |
| 4        | 15         | 5.5        |
| 5        | 57         | 20.7       |
| 6        | 17         | 6.2        |
| 7        | 48         | 17.5       |
| 8        | 12         | 4.4        |
| 9        | 18         | 6.5        |
| 10       | 5          | 1.8        |
| 11       | 1          | .4         |
| 11 o más | 1          | .4         |
| Total    | 275        | 100.0      |

**Tabla 3.3 Sexo**

| Válidos | Frecuencia | Porcentaje |
|---------|------------|------------|
| Hombre  | 136        | 49.5       |
| Mujer   | 138        | 50.5       |
| Total   | 275        | 100.0      |

**Tabla 3.4 Edad**

| Válidos | Frecuencia | Porcentaje |
|---------|------------|------------|
| 17      | 4          | 1.5        |
| 18      | 26         | 9.5        |
| 19      | 50         | 18.2       |
| 20      | 63         | 22.9       |
| 21      | 56         | 20.4       |
| 22      | 35         | 12.7       |
| 23      | 29         | 10.5       |
| 24      | 7          | 2.5        |
| 25      | 5          | 1.8        |
| Total   | 275        | 100.0      |

**Tabla 3.5** Estilos de aprendizaje en la muestra

| Válidos           | Frecuencia | Porcentaje |
|-------------------|------------|------------|
| Activo            | 78         | 28.4       |
| Reflexivo         | 73         | 26.5       |
| Teórico           | 56         | 20.4       |
| Pragmático        | 68         | 24.7       |
| Total encuestados | 275        | 100.0      |

### 3.2.4 Factores críticos de privacidad e interfaz

En una tercera versión de la encuesta (Ver Appendix F) se usaron siete puntos Likert (0: nada importante, 6: extremadamente importante) para indagar la relación de los usuarios con los elementos de un aviso de privacidad. Mediante el programa estadístico SPSS (Malhortra, 2008) se analizó la relación de esas variables. Se validó la confiabilidad del instrumento mediante un Alfa de Cronbach de 0.863 como se muestra en las Tabla 3.6 y Tabla 3.7.

**Tabla 3.6** Resumen del procesamiento de los casos

|       |                        | N   | %     |
|-------|------------------------|-----|-------|
| Casos | Válidos                | 275 | 100.0 |
|       | Excluidos <sup>a</sup> | 0   | .0    |
|       | Total                  | 275 | 100.0 |

a. Eliminación por lista basada en todas las variables del procedimiento.

**Tabla 3.7** Estadísticos de fiabilidad

| Alfa de Cronbach | N de elementos |
|------------------|----------------|
| .863             | 6              |

Las variables a analizar fueron las siguientes:

1) Con respecto a la privacidad

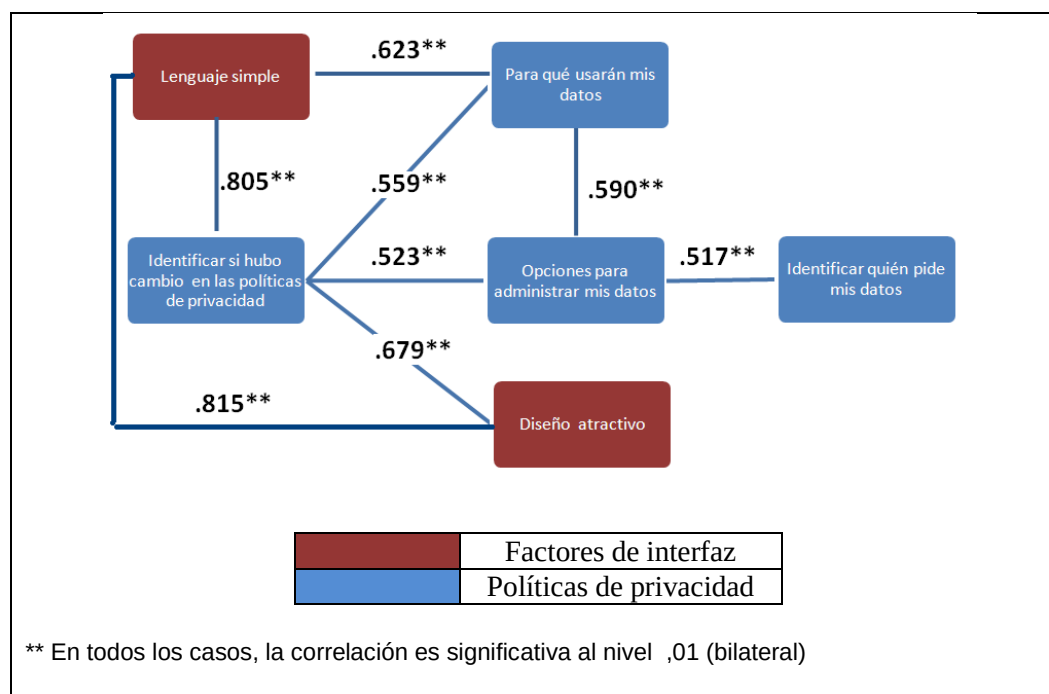
- Medidas de protección.
- Identificar datos personales.
- Identificar quién los recaba.
- Saber para qué los van a usar.
- Identificar cómo me avisarán de los cambios en las políticas de privacidad del sitio.
- Identificar cómo puedo consultar, modificar o cancelar mis datos.
- Existencia de leyes internacionales.

2) Con respecto a la interfaz

- Lenguaje simple.
- Diseño atractivo.
- Personalización del navegador.

### 3.2.4 Correlación entre los factores de estudio

Con base a los resultados obtenidos por el Coeficiente de Correlación de Pearson, se resumen las relaciones más significativas de los factores que los usuarios consideran importantes los para administrar la privacidad de los datos personales cuando se navega en cualquier página de Internet de acuerdo a la Fig. 3.3



**Fig. 3.3** Relaciones significativas basadas en Coeficiente de Correlación de Pearson

Las cuatro correlaciones más significativas de acuerdo al coeficiente de correlación de Pearson son las siguientes:

1. Las interfaces deben tener un diseño atractivo y un lenguaje simple ( $.815^{**}$ )
2. Los cambios en las políticas de privacidad se deben mostrar en un lenguaje simple ( $.805^{**}$ )
3. Los cambios en las políticas de privacidad se deben mostrar en un diseño atractivo ( $.679^{**}$ )
4. Saber para qué se usarán los datos personales debe mostrarse en un lenguaje simple ( $.623^{**}$ )

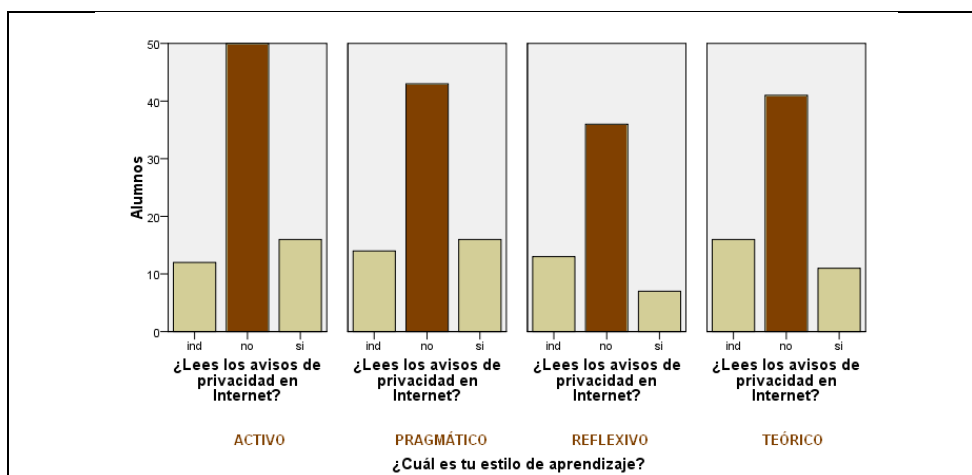
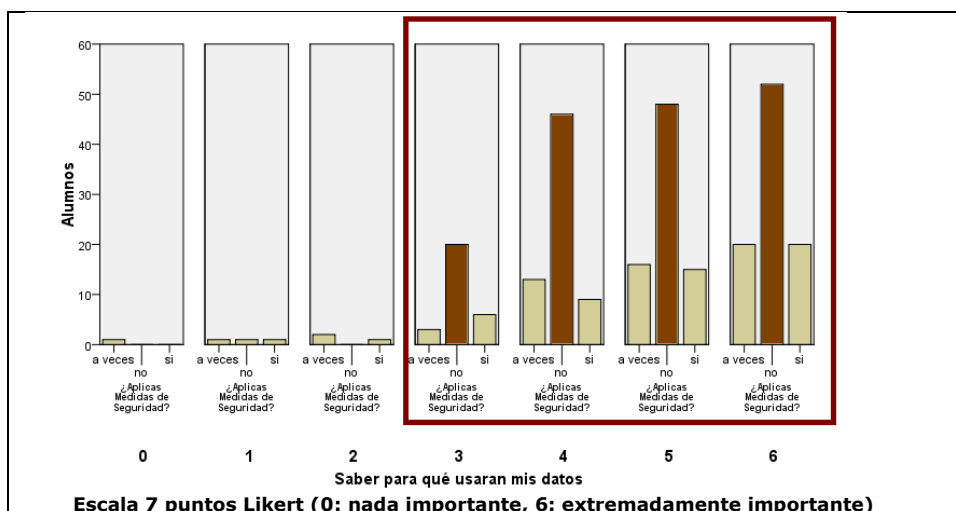
Lo anterior demuestra que los factores de diseño de interfaz en un contexto de privacidad de información son determinantes para los usuarios.

Los tres factores críticos más importantes para los usuarios son:

1. Identificar si harán transferencia de los datos a otras entidades (43.3%)
2. Diseño atractivo en la interfaz (42.5%)
3. Identificar las opciones para consultar, modificar o cancelar los mismos (39.6%)

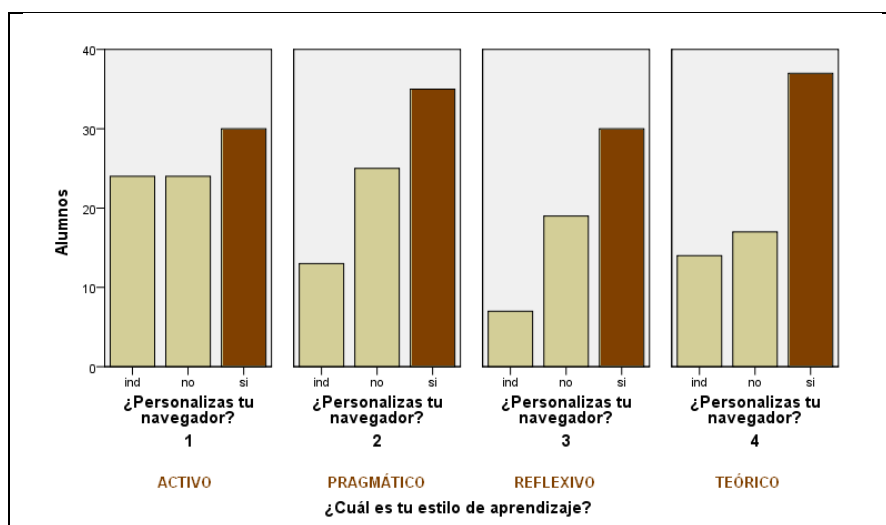
### 3.2.5 Resultados acerca de los factores críticos de privacidad

- 85.8% Identifican sus datos personales.
- 56.7 % Saben qué es un Aviso de Privacidad.
- 87.6% Desconoce la existencia de leyes federales sobre Protección de Datos Personales en Posesión de los Particulares.
- 18.9% Aplica medidas para mantener la privacidad de sus datos personales cuando navega en Internet.
- La mayoría reconoce que es importante saber qué harán con sus datos personales, sin embargo no aplican medidas de seguridad (Fig. 3.4)
- 18.2% Lee los avisos de privacidad de las páginas que visita en Internet y les toma entre uno y cuatro minutos leerlos. (Fig. 3.5)

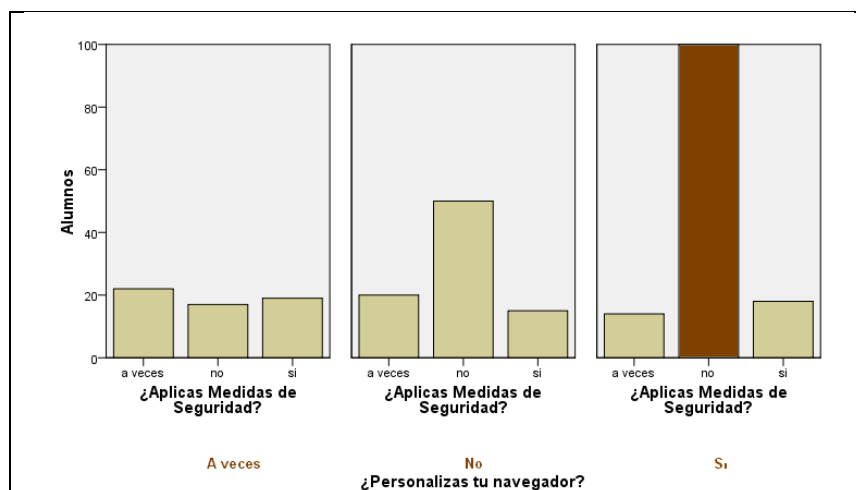


### 3.2.6 Resultados acerca de factores humanos y de interfaz

- La mayoría de los usuarios, sin importar su estilo de aprendizaje, presentan un manejo similar de su privacidad. (Fig. 3.5)
- El 48% personaliza su navegador (Fig. 3.6 y 3.7)
- Al 81.5% le gustaría que consideren sus gustos de personalización para administrar su privacidad.
- 81.5% Espera un formato simple y un diseño atractivo en un aviso de privacidad.



**Fig. 3.6** Estilo de aprendizaje y personalización de navegador



**Fig. 3.7** Personalización de navegador y medidas de seguridad

- Al final de la encuesta, se identificó el índice general de satisfacción de las personas sobre las decisiones que involucran privacidad de datos (donde 0 es ninguna satisfacción y 10 es satisfacción completa). Los 4 grupos de encuestados más grandes son aquellos que califican su grado de satisfacción con valores entre 5 y 8, es decir, satisfacción media-alta. Sin embargo, estas mismas personas pertenecen al grupo que no conoce la Ley de protección de datos personales en posesión de los particulares. Ver (Fig. 3.8).

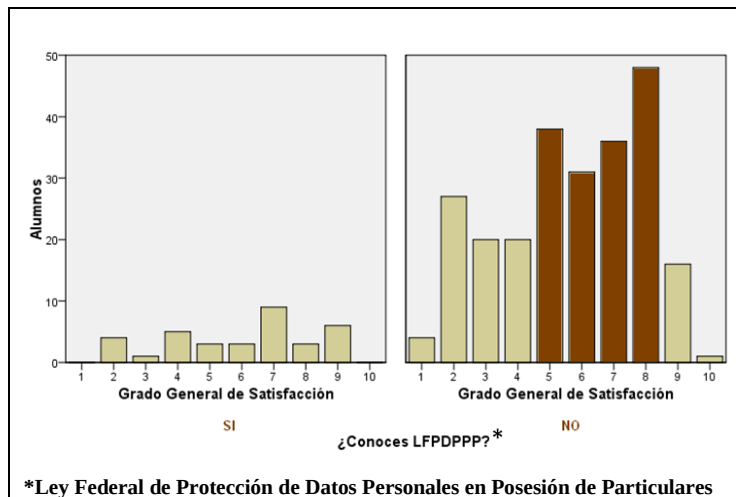


Fig. 3.8 Satisfacción general sobre el tema

### 3.2.7 Método sugerido para construir interfaces basado en correlaciones

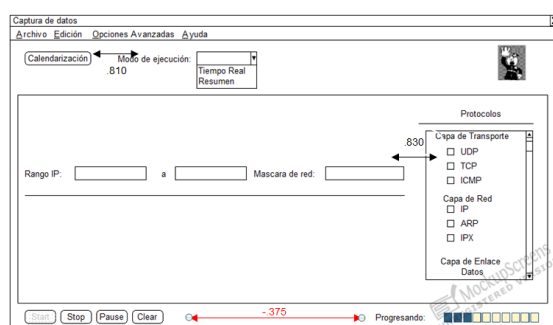
El coeficiente de correlación de Pearson (Malhortra, 2008) es un índice que mide el grado de variación entre distintas variables relacionadas, esto significa que puede ver variables fuertemente relacionadas. Sus valores absolutos oscilan entre 0 y 1, es decir, si se tienen dos variables **XY** y se define el coeficiente de correlación de Pearson entre estas dos variables como  $r_{XY}$  entonces:

$$-1 \leq r_{xy} \leq 1$$

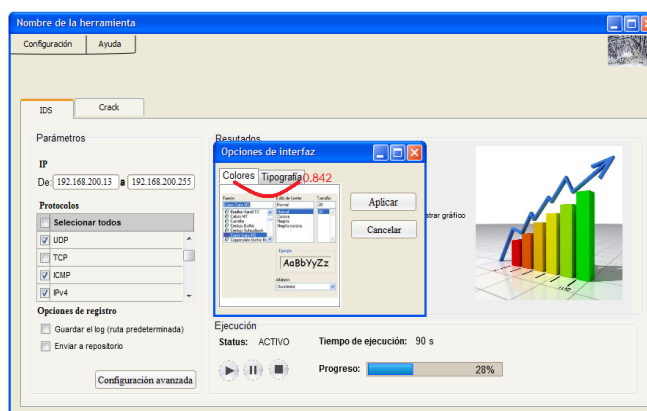
No obstante, ha de indicarse que la magnitud de la relación viene especificada por el valor numérico del coeficiente, reflejando el signo de la dirección de tal valor. En este sentido, tan fuerte es una relación +1 como de -1. En el primer caso la relación es perfecta positiva y en el segundo perfecta negativa. Se dice que la correlación entre dos variables **XY** es perfecta positiva cuando a medida que aumenta una variable también aumenta la otra, al contrario de una relación perfecta negativa que se lleva acabo cuando a medida que aumenta una variable disminuye la otra. Los coeficientes de correlación significativos al nivel 0.05 se identifican por medio de un solo asterisco, mientras que los significativos al nivel 0.01 mediante dos asteriscos.

El método de construcción de interfaces propuesto, sugiere una distribución de elementos sobre el espacio de interacción basado en los valores de las correlaciones obtenidos. La distancia que debe existir entre los elementos está determinada por dicho valor. Las correlaciones altas sugieren cercanía de elementos por la alta relación que tiene para el usuario, los valores bajos sugieren distanciamiento, El alcance de este proyecto no incluye formalizar y evaluar este método. Esto se sugiere como futura línea de investigación.

Durante el año 2012 se sugirió este método en la construcción de prototipos de herramientas de apoyo a la administración de una red de computadoras para dos cursos de Seguridad Informática a nivel licenciatura de alumnos en Ingeniería en Computación para observar resultados preliminares. En la Fig. 3.9 se observa que los factores técnicos con alto grado de correlación están cerca uno de otro, y los que tienen valor bajo están distantes. En la Fig. 3.10 se observa que los elementos de interfaz con alto grado de correlación están cerca uno de otro.



**Fig. 3.9** Correlaciones de factores técnicos en un prototipo



**Fig. 3.10** Correlaciones de elementos de interfaz en un prototipo

Después de identificar los factores críticos de privacidad de datos personales y sus correlaciones más significativas con factores de interfaz, se implementaron 2 prototipos bajo el mismo método, los cuales se presentaron durante una Feria de Ciencias en una Facultad de Tecnologías de Información en diciembre de 2013 (Ver Fig. 3.11). En este

trabajo, participaron de forma conjunta un alumno de Ingeniería de Software y otro de Diseño y Dirección Publicitaria. Los prototipos generados fueron:

1. Aviso de privacidad
2. Ejercicio de derechos ARCO



**Fig. 3.11** Presentación de patrones de interacción

Se documentó la retroalimentación por parte de alumnos y profesores para mejoras futuras.

### **3.2.8 Conclusión**

Se ha demostrado que los factores relacionados con la interfaz de usuario deben ser considerados desde la perspectiva de la seguridad informática. Los valores de las correlaciones entre factores de manejo de privacidad, factores de interfaz y factores humanos son significativos y deben ser consideradas al momento de implementar una interfaz. Sería deseable contar con un modelo que relacione los factores críticos de privacidad de información con tópicos de diseño de interfaz. El modelo propuesto en el apartado 3.2.7 debe ser implementado y evaluado para verificar su validez. Todos los estilos de aprendizaje muestran un comportamiento similar ante las interfaces de administración de la privacidad actuales. Aplicar los rasgos distintivos de cómo las personas perciben interacciones y responden a sus ambientes de aprendizaje, podría beneficiar a los usuarios para mejorar su privacidad y a los desarrolladores para contar con un marco de referencia que mejore la experiencia de usuario y la usabilidad de un sistema. Para delimitar el alcance de este trabajo, no se explorará la implementación de los mismos. Hasta el momento se ha estudiado la interacción del usuario final y las aplicaciones de Internet, ahora sería deseable desde el punto de vista de los administradores de seguridad de redes y las herramientas que permiten esta tarea.

## Capítulo 4. Administración de Seguridad de Red e Interfaz de Usuario

---

*“Internet es un gran avance para la humanidad, pero también un gran problema”*

*Pedro Ramírez*

En este capítulo se presentan las correlaciones significativas entre factores críticos de administración de seguridad en una red e interfaz de usuario tomando como base un estudio de usabilidad de herramientas básicas y al identificar los elementos técnicos y humanos comunes a dichas aplicaciones.

## 4. Administración de seguridad de red e interfaz de usuario

Este capítulo presenta la relación de los elementos comunes en las herramientas de administración de seguridad en una red basadas en línea de comandos y la interfaz de usuario. Se persiguen los siguientes objetivos específicos:

- Determinar el grado actual de usabilidad de aplicaciones de seguridad basadas en línea de comandos.
- Identificar los elementos comunes en las herramientas de administración de seguridad.
- Determinar la correlación de dichos elementos con la interface de usuario.

### 4.1 Metodología

Se realizó un análisis cuantitativo de datos mediante un análisis paramétrico utilizando frecuencias y coeficientes de correlación (Malhortra, 2008). Se aplicó Análisis de Frecuencias y método de Correlación de Pearson utilizando el software SPSS para identificar las relaciones entre las variables. Se aplicó una prueba de usabilidad y una encuesta particular a estudiantes y maestros de UPAEP (Ver Tabla 4.1). Su participación fue voluntaria y no se ofreció algún tipo de compensación. Se llevaron a cabo 3 sesiones de trabajo.

**Tabla 4.1** Demográficos

| Edad    | Cantidad | Sexo   | Profesión  |
|---------|----------|--------|------------|
| [22-23] | 4        | Mujer  | Estudiante |
| [35-40] | 2        | Mujer  | Maestro    |
| [22-24] | 7        | Hombre | Estudiante |
| [40-49] | 2        | Hombre | Maestro    |

En la primera sesión, se les pidió a los participantes mencionar las 20 herramientas básicas en su tarea administrar la seguridad de una red. De este listado inicial, por límite de tiempo y de acuerdo al mayor número de incidencias, se seleccionaron sólo cuatro herramientas basadas en línea de comandos : Un IDS (Intrusion - Detection System, caso Snort), un Password Crack (caso John the Ripper), un Administrador de políticas para correo electrónico (caso Procmail) y un Administrador de dispositivos en la red ( caso SNMP: Simple Network Management Protocol) (Sourcefire, 2000) (Openwall, 2001) (Van den Berg, 2000) (Research, 2001). El listado inicial incluía el siguiente software:

- IDS
- Password Crack
- Procmail
- SNMP
- Samba
- IPsec
- SSH Server
- HTTPS Server
- Retina
- Nessus
- VPN
- Firewall
- Access Lists
- Nmap
- Tripwire

## System Usability Scale

Seleccionadas las cuatro herramientas, se les pidió evaluar en papel (Ver Fig. 4.1) con base en su experiencia previa, la usabilidad de las cuatro herramientas usando el cuestionario sugerido por la metodología de SUS (System Usability Scale) (Brook, 1998).



**Fig. 4.1** Evaluando herramientas con SUS

Los resultados promedio obtenidos por los 15 participantes se muestran en la Tabla 4.2.

**Tabla 4.2** Resultados evaluación SUS

| Herramienta evaluada | Resultado SUS |
|----------------------|---------------|
| Snort                | 22            |
| John the Ripper      | 28.3          |
| Procmail             | 20.5          |
| SNMP                 | 23.3          |

(Brook, 1998) indica que una nota media dada por SUS es de 68. Un resultado más alto significa un nivel de usabilidad mejor que el promedio. Para este trabajo, las herramientas evaluadas mostraron valores entre 20.5 y 28.3, lo que sugiere niveles de usabilidad menores al promedio esperado.

## 4.2 Elementos técnicos y elementos de interfaz

En la segunda sesión, en una tercera versión de encuesta, se les pidió a los participantes que indicaran cuales son los elementos técnicos y los elementos relativos a la interfaz que deberían tener una representación consistente y común en las cuatro herramientas seleccionadas para el estudio. Los elementos técnicos, sin importar el orden en que se citan, que se esperaba encontrar en forma consistente en las herramientas de administración de seguridad informática en una red son los siguientes:

1. Rangos de direcciones IP
2. Menú de puertos
3. Menú de protocolos
4. Menú de tarjetas de red
5. Grupos de trabajo

6. Status de la aplicación (Activo / inactivo)
7. Calendarización de tareas
8. Funciones Básicas (Botón de Inicio, Pausa, Fin, Reset)
9. Menú de administración (Agregar, quitar componentes)
10. Lista de elementos (usuarios, nodos de red)
11. Porcentaje de Avance
12. Barra de "Procesando" (Estoy trabajando)
13. Tiempo de Ejecución (Horas, minutos para terminar la tarea)
14. Modos de Ejecución (online, offline)
15. Log en Tiempo Real
16. Resultados finales esperados
17. Opciones Avanzadas
18. Guardar/Enviar el Log (local, repositorio remoto, email)
19. Guardar/Enviar resultado parcial (local, repositorio remoto, email)
20. Guardar/Enviar resultado final (local, repositorio remoto, email)
21. Ventana de log

Los elementos relativos a la interface, sin importar el orden en que se citan, que se esperaba encontrar en las herramientas de administración de seguridad en una red son:

1. Cambiar colores de la herramienta
2. Cambiar tipografía de la herramienta
3. Iconos representativos
4. Cambiar posición de las opciones dentro de la interfaz
5. Disponer de versión gráfica
6. Disponer de versión de línea de comandos

### **Análisis de variables**

En la tercera sesión se presentaron cuatro encuestas en papel (una por cada herramienta) con 5 puntos en escala Likert (1: nada importante, 5: extremadamente importante) para determinar la importancia cada uno de los elementos dentro de la herramienta.

La pregunta que se presentó a los participantes fue la siguiente:

¿Qué tan importante es para usted disponer de manera oportuna de cada uno de los siguientes elementos para operar de forma cotidiana la herramienta ( Snort / John the Ripper / Procmil / SNMP )?

La relación de las variables fue analizada usando SPSS (Malhortra, 2008) . La confiabilidad del instrumento fue validada a través del valor Alpha de Cronbach (Ver Tabla 4.3).

**Tabla 4.3** Validez de instrumento

| <b>Tool</b>     | <b>Cronbach's Alpha</b> | <b>N of Items</b> |
|-----------------|-------------------------|-------------------|
| Snort           | .809                    | 27                |
| John the Ripper | .863                    | 27                |
| SNMP            | .800                    | 27                |
| Procmal         | .812                    | 27                |

### 4.3 Importancia de factores críticos en herramientas de estudio

A continuación se muestran los porcentajes individuales más significativos respecto a la importancia (1: Nada importante, 5: Muy importante) que los administradores asignaron a los elementos técnicos y de interfaz necesarios para operar de forma cotidiana cada herramienta. (Ver Tabla de la 4.4 a la 4.7). Estos resultados se discuten en la sección **4.5 Discusión sobre la percepción de la línea de comandos**.

- 1 = Nada importante
- 2 = Poco importante
- 3 = Moderadamente importante
- 4 = Importante
- 5 = Muy importante

**Tabla 4.4** Colores, tipografía e íconos

| <b>Herramienta</b> | <b>Cambiar colores</b>         | <b>Cambiar tipografía</b>      | <b>Incluir íconos</b> |
|--------------------|--------------------------------|--------------------------------|-----------------------|
| Snort              | 71.4% Importante               | 28.6% Moderadamente importante | 57.1% Importante      |
| John the Ripper    | 42.9% Moderadamente importante | 42.9% Nada importante          | 57.1% Importante      |
| SNMP               | 57.1% Moderadamente importante | 42.9% Poco importante          | 42.9% Importante      |
| Procmal            | 57.1% Moderadamente importante | 42.9% Moderadamente importante | 57.1% Importante      |

**Tabla 4.5** Elegir posición y versión gráfica

| <b>Herramienta</b> | <b>Cambiar elementos de posición</b> | <b>Versión gráfica</b>         |
|--------------------|--------------------------------------|--------------------------------|
| Snort              | 42.9% Importante                     | 42.9% Importante               |
| John the Ripper    | 42.9% Importante                     | 42.9% Moderadamente importante |
| SNMP               | 57.1% Importante                     | 71.4% Moderadamente importante |
| Procmal            | 42.9% Importante                     | 57.1% Moderadamente importante |

**Tabla 4.6** Básicos, avanzados, esperados

| Herramienta     | Funciones básicas    | Funciones avanzadas            | Resultados esperados           |
|-----------------|----------------------|--------------------------------|--------------------------------|
| Snort           | 42.9% Muy importante | 57.1% Muy importante           | 57.1% Importante               |
| John the Ripper | 57.1% Importante     | 57.1% Muy importante           | 71.4% Importante               |
| SNMP            | 57.1% Important      | 57.1% Muy importante           | 42.9% Moderadamente importante |
| Procmal         | 57.1% Importante     | 57.1% Moderadamente importante | 42.9% Importante               |

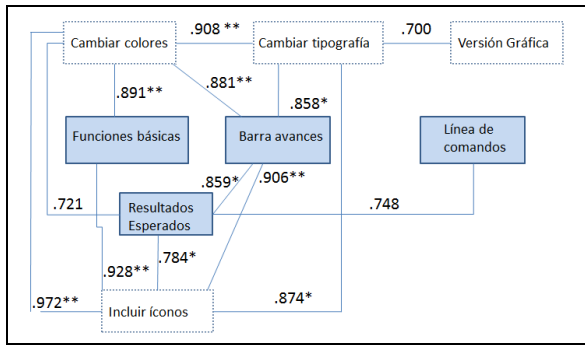
**Tabla 4.7** CLI y menú de administración

| Herramienta     | Línea de comandos              | Barra de avances               | Menú de administración         |
|-----------------|--------------------------------|--------------------------------|--------------------------------|
| Snort           | 57.1% Moderadamente importante | 28.3% Moderadamente importante | 71.4% Importante               |
| John the Ripper | 42.9% Poco importante          | 57.1% Moderadamente importante | 57.1% Importante               |
| SNMP            | 57.1% Poco importante          | 57.1% Moderadamente importante | 57.1% Importante               |
| Procmal         | 71.4% Poco importante          | 42.9% Nada importante          | 85.7% Moderadamente importante |

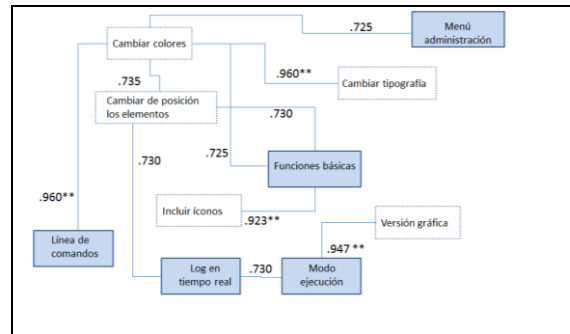
#### 4.4 Correlación de factores críticos de administración de seguridad en una red y elementos de Interfaz

Basado en los resultados obtenidos por el Coeficiente de Correlación de Pearson, las relaciones más significativas (iguales o mayores a .700, valor definido para este trabajo) de los factores básicos que los administradores de una red requieren para utilizar la herramienta estudiada, se sumarizan en las Figuras de la 4.2 a la 4.5.

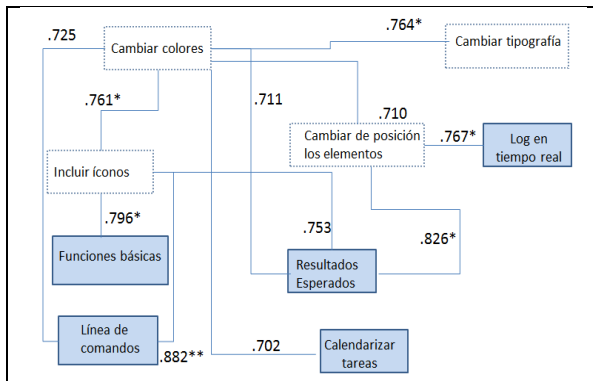
Los tópicos representados con líneas punteadas representan factores relativos a la interfaz, y los tópicos señalados con líneas continuas representan factores técnicos. Se distingue para las cuatro herramientas altas correlaciones entre los dos tipos de factores evaluados. No se puede construir una interfaz basada solo en funciones técnicas sin considerar las preferencias de los usuarios.



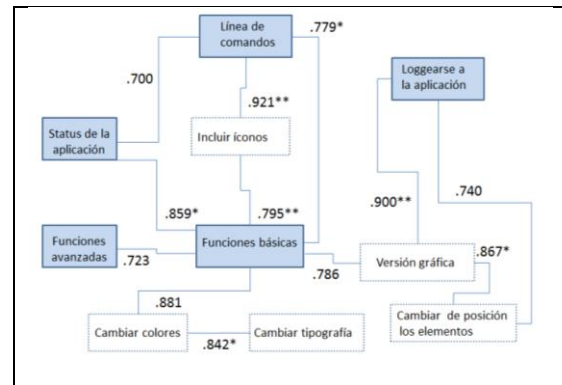
**Fig. 4.2** Correlaciones Snort



**Fig. 4.3** Correlaciones Crack



**Fig. 4.4** Correlaciones SNMP



**Fig. 4.5** Correlaciones SNMP

Al final de la encuesta, se les preguntó a los participantes sobre su índice general de satisfacción con respecto a que la interfaz actual de las herramientas estudiadas le ayuden a cumplir con el objetivo para el que fue desarrollada (0 es ninguna satisfacción y 10 es satisfacción completa). Ninguna persona calificó su percepción con valores de 9 o 10. De los 15 encuestados, 14 dieron una calificación entre 3 y 8 donde 5 de ellos asignaron 6 como respuesta, lo que indica que los administradores tienen un nivel medio de satisfacción con el uso de las interfaces de herramientas de administración de seguridad. Los resultados se presentan en la Tabla 4.8

**Tabla 4.8** Satisfacción General

|         |   | <b>Frecuencia</b> | <b>Porcentaje</b> |
|---------|---|-------------------|-------------------|
| Válidos | 3 | 3                 | 20.0              |
|         | 4 | 2                 | 13.3              |
|         | 5 | 2                 | 13.3              |
|         | 6 | 5                 | 33.3              |
|         | 7 | 2                 | 13.3              |
|         | 8 | 1                 | 6.7               |
| Total   |   | 15                | 100.0             |

## 4.5 Discusión sobre la percepción de la línea de comandos

El estudio fue conducido con personas de distintas edades: estudiantes de los últimos semestres de una Facultad de Tecnologías de Información de la especialidad de Seguridad Informática y profesores con más de 15 años de experiencia en docencia y en consultorías en el área de seguridad informática. Futuros estudios podrían considerar incluir personas expertas en seguridad de otros puntos geográficos y culturales para comparar los resultados. Para realizar la prueba SUS este estudio consideró la experiencia previa de los encuestados sin tener acceso a las herramientas en ese momento. En un futuro se podrían incluir otras pruebas de usabilidad en un laboratorio explícitamente preparado para ello. Se sugiere también incluir más herramientas para su análisis. Ninguno de los participantes se siente satisfecho con la idea de que las interfaces de las herramientas actuales faciliten su uso para alcanzar los resultados esperados. La mayoría indica estar de poco a medianamente satisfecho, abriendo oportunidades de explorar mejoras en la interacción.

Los resultados iniciales obtenidos de la evaluación basada en SUS (entre 20.5 y 28.3) indican que el grado de usabilidad de las herramientas estudiadas es muy bajo y no satisface a quienes las usan de forma cotidiana (Ver Tabla 4.2). Sería deseable proponer algunos esquemas de uso basado en interfaces gráficas y repetir la para identificar preferencias.

Tener íconos representativos así como la opción de cambiar colores es muy importante para los usuarios de las cuatro herramientas evaluadas (Ver Tabla 4.4), de esta última opción se desprenden correlaciones significativas con otros factores de manejo de interfaz y factores. Por ejemplo, en las cuatro herramientas se encontró una alta correlación con la opción cambiar tipografía; esto implica que deberían situarse cerca una de otra en la interfaz (Ver de la Fig. 4.2 a la Fig. 4.5). Definir un conjunto universal de íconos de seguridad podría incrementar el nivel de usabilidad de las herramientas y mejorar el desempeño del usuario.

Disponer de la opción de cambiar tipografía solo fue importante para dos de las cuatro herramientas evaluadas (Ver Tabla 4.4). Esto puede implicar que no es un factor determinante para el usuario, sino que solo es deseable.

Cambiar de posición los elementos dentro de la interfaz y disponer de una versión gráfica adicional a la línea de comandos son opciones importantes para los usuarios de estas herramientas (Ver Tabla 4.5). Esto sugiere que la personalización de los espacios de trabajo podría mejorar el uso de las mismas. Las funciones básicas, las opciones avanzadas y los resultados esperados, son elementos técnicos muy importantes para los usuarios de las cuatro herramientas y se esperaría una presencia relevante dentro de una interfaz basada en las opiniones directas de los administradores (Ver Tabla 4.6).

El usuario espera encontrar las opciones de las que dispone para trabajar en un lenguaje gráfico y consistente. Esta característica presentó una alta correlación con las funciones básicas de una aplicación para los cuatro casos de estudio (Ver Figuras de la 4.2 a la 4.5).

Es probable que para algunas personas trabajar con línea de comandos sea la mejor opción, sin embargo existen otros perfiles de usuario cuyas habilidades son distintas y no se ofrecen alternativas que faciliten su trabajo.

## 4.6 Implementación

Las correlaciones obtenidas en este estudio, se implementaron en ejemplos de interacción y se comparó su grado de usabilidad, mediante las metodologías SUS (Brook, 1998) y SIRIUS (Suárez-Torrente, 2011), con respecto a las herramientas originales basadas en línea de comandos. Los resultados demuestran una mejora significativa en sus evaluaciones de usabilidad desde ambas metodologías. Estos resultados se observan en las Tablas 4.9 y 4.10. Este trabajo se desarrolló como parte de una Tesis de Ingeniería en Computación y Sistemas con el título: “BLU: Un modelo de construcción de patrones de interacción para mejorar el desempeño de los administradores de una red de cómputo basados en las correlaciones de factores humanos, de seguridad y de interfaz”.

**Tabla 4.9** Comparación de resultados IDS

| Herramienta evaluada                  | Resultado SUS | Resultado SIRIUS |
|---------------------------------------|---------------|------------------|
| Intrusion Detection System (original) | 22            | 30               |
| Intrusion Detection System BLU        | 60            | 72               |

**Tabla 4.10** Comparación de resultados Cracker

| Herramienta evaluada | Resultado SUS | Resultado SIRIUS |
|----------------------|---------------|------------------|
| Cracker (original)   | 28.3          | 29               |
| Cracker BLU          | 65            | 70               |

## 4.7 Conclusión

Los resultados de este estudio sugieren que el desempeño del administrador podría mejorar si se implementan tópicos de usabilidad en interfaces de administración de seguridad. Los valores de las correlaciones entre factores de administración de una red, factores de interfaz y factores humanos son significativos y deben ser consideradas al momento de implementar una interfaz. Esto no limita a desaparecer las herramientas basadas en línea de comandos, pues tienen una funcionalidad muy poderosa, sino que las interfaces gráficas podrían ser un complemento que mejore la experiencia de usuario. Los usuarios expertos reconocen que se debe dominar el uso de la línea de comandos pues durante muchos años la mayoría de las herramientas más poderosas se han desarrollado en este ambiente, sin embargo, cada vez son más las personas del área tecnologías de información que han crecido interactuando en su mayoría con ambientes gráficos y no resulta natural trabajar con espacios limitados sin opciones de personalización.

## Capítulo 5. Patrones de interacción y diseño de interfaces

---

*“No solo los diseñadores han mejorado, los usuarios se han acostumbrado a los entornos interactivos”*

*Jacob Nielsen*

En este capítulo se investiga cuáles zonas las herramientas que usan los desarrolladores para construir software relativo a seguridad y se propone un conjunto de patrones de interacción basado en factores humanos para resolver un conjunto de tareas específicas relativas a seguridad evaluando su impacto.

## 5. Patrones de interacción y diseño de interfaces

Basado en los temas analizados del Capítulo 1 al Capítulo 4, se hace evidente que el aplicar patrones de interacción en el diseño de interfaces podría mejorar la usabilidad y la experiencia de usuario y disminuir el tiempo invertido en el diseño de interfaces relativas a seguridad. En este capítulo se investiga cuáles son las herramientas que usan los desarrolladores para construir software de privacidad y se propone un patrón basado en la interacción con elementos de un aviso de privacidad como medio para reducir las brechas de comunicación existentes. Se persiguen los siguientes objetivos específicos:

1. Identificar las herramientas que usan los desarrolladores para construir aplicaciones con funciones relativas a privacidad de usuario final.
2. Evaluar por parte de los desarrolladores la utilidad de las herramientas citadas del punto anterior.
3. Evaluar la pertinencia de un conjunto de patrones de interacción relativos a privacidad para la construcción de interfaces.

### 5.1 Metodología

Se definieron los requerimientos funcionales de cinco aplicaciones que involucran temas de privacidad de información de usuarios finales. Durante otoño 2012 se dirigió a un grupo de once estudiantes de séptimo semestre de Ingeniería en Computación e Ingeniería de Software con el objetivo de identificar los elementos de software que utilizaron para construir aplicaciones relativas a privacidad. Se les permitió seleccionar libremente las herramientas que consideran adecuadas para su diseño e implementación. Al finalizar este curso y después de evaluar la funcionalidad de sus aplicaciones, se presentó a los alumnos un conjunto de patrones de interacción (COPEMMA (Murillo & Sánchez, 2013) y el Aviso de privacidad que se describirá más adelante) y a cada equipo se le pidió que estimara el impacto en el desarrollo de su trabajo concluido si hubieran contado con dichos patrones desde el inicio del curso.

Los estudiantes participaron bajo la premisa de que solo se evaluaría el cumplimiento de los requerimientos funcionales solicitados. En los equipos de desarrollo no contaron con ayuda de expertos legales ni diseñadores gráficos (o afín). Se presentó para cada equipo los requerimientos funcionales de su aplicación sin mencionarles el objetivo de este estudio. Cada equipo seleccionó su metodología de desarrollo de software, lenguaje de programación, íconos, imagen y organización de información en pantalla. Para obtener sus comentarios finales, se les invitó a participar de manera voluntaria sin algún tipo de retribución.

A continuación se listan los cinco proyectos solicitados a los participantes de este estudio. Estos trabajos se presentaron en la exposición de proyectos finales que organiza la facultad de tecnologías de información a la cuál pertenecen los alumnos. En los cinco casos, los evaluadores y otros alumnos que interactuaron con los proyectos comentaron que estas herramientas hacían más fácil la comprensión de las políticas de privacidad.

1. Prototipo de Navegación para un Aviso de Privacidad en un dispositivo móvil basado en Android. (Ver Fig. 5.1)

2. Elementos gráficos de visualización web de un Aviso de Privacidad para Universitarios. (Ver Fig. 5.2)
3. Visualización de un Aviso de Privacidad simplificado en Android basada en estilos de aprendizaje. (Ver Fig.5.3 )
4. Realidad Aumentada aplicada a la visualización de elementos de privacidad (Ver Fig. 5.4)
5. Visualización de políticas de privacidad basadas en P3P (Platform for Privacy Preferences) para el navegador Chrome. (Ver Fig. 5.5)

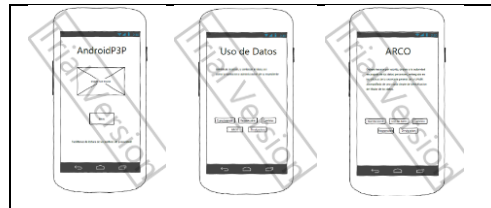


Fig. 5.1 Prototipo de Navegación



Fig. 5.2 Elementos gráficos de visualización



Fig. 5.3 Visualización de un Aviso de Privacidad simplificado basada en estilos de aprendizaje



Fig. 5.4 Realidad aumentada

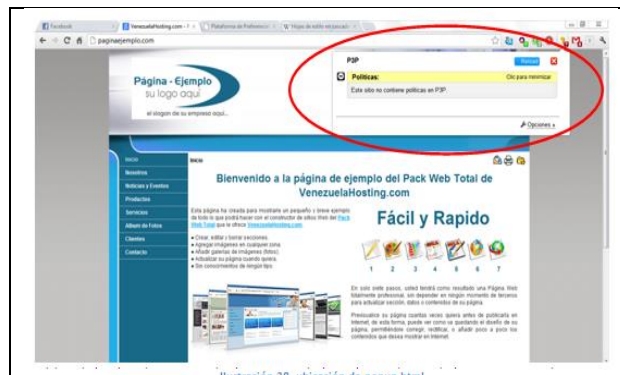


Fig. 5.5 Visualización basada en P3P

## 5.2 Herramientas tradicionales de desarrollo para aplicaciones de seguridad

En las tres sesiones parciales de evaluación de requerimientos funcionales de cada aplicación, se les preguntó de forma abierta a los desarrolladores sobre todas las herramientas, guías y estándares que les sirvieron de base en la construcción de cada proyecto resumiendo lo siguiente: (Ver Tabla 5.1)

Tabla 5.1 Herramientas de programación, guías y estándares

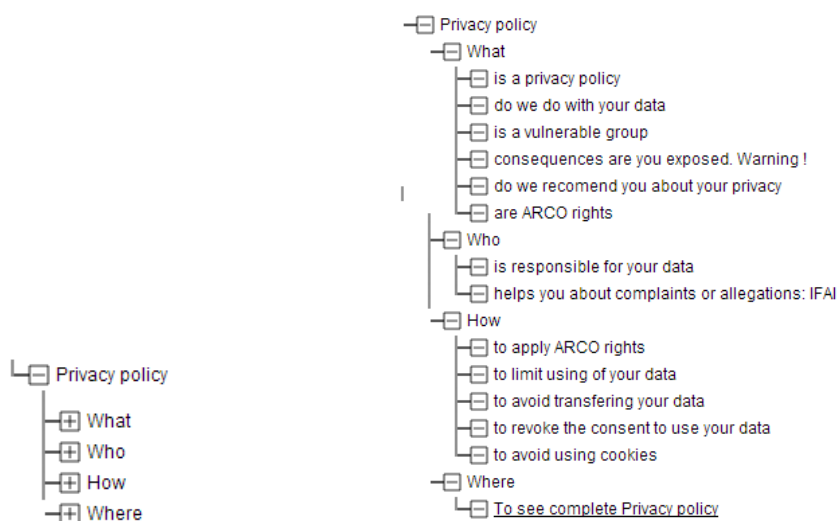
| Proyecto | Herramientas  | Metodologías                 | Estándares de seguridad                                                                                                                                                            |
|----------|---------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | Eclipse       | Modelado ágil. Scrum         | Leyes sobre protecciones de datos personales, colecciones de íconos, campos de captura de password.                                                                                |
| 2        | PHP y Eclipse | Modelado orientado a objetos | Resúmenes de leyes sobre protecciones de datos personales, Privacy Bird, Función de cifrado de datos, Campos de captura de password.                                               |
| 3        | Eclipse       | Modelado orientado a objetos | Leyes sobre protecciones de datos personales, Colecciones de íconos, Campos de captura de password.                                                                                |
| 4        | Java          | Modelado orientado a objetos | Leyes sobre protecciones de datos personales, APIs de desarrollo.                                                                                                                  |
| 5        | PHP           | Modelado orientado a objetos | Privacy Bird, P3P*, Xacml**<br>* <a href="http://www.w3.org/P3P/">http://www.w3.org/P3P/</a><br>** <a href="http://sunxacml.sourceforge.net/">http://sunxacml.sourceforge.net/</a> |

### 5.3 Patrones de interacción: una propuesta para un aviso de privacidad

Para este proyecto se diseñó un patrón de interacción basado en los resultados de los capítulos 3 y 4 presentados anteriormente y los trabajos previos publicados (Murillo & Sánchez, 2013) (Murillo & Sánchez, 2013).el cuál se describe a continuación.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nombre</b><br>Aviso de privacidad integral                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Problema</b><br>El Aviso de privacidad es un documento generado por la persona física o moral responsable de la <b>recopilación y tratamiento adecuado de datos personales</b> y debe ser puesto a disposición del titular de los datos. Este documento no tiene una estructura definida y queda a juicio de cada entidad el formato que le dará. El documento está escrito en lenguaje legal, poco claro para el usuario final y es difícil identificar sus partes. Es ignorado por el usuario común debido a su extensión.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Solución</b><br>Se propone una jerarquía de datos, una distribución y navegación de información basada en reglas de usabilidad. Al usuario se le indica el procedimiento para identificar los elementos de un Aviso de privacidad y la función de cada uno de ellos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Contexto</b><br>De acuerdo al artículo 16 de la FPDPPP ( <i>Ley Federal de Protección de Datos Personales en Posesión de los Particulares</i> ) se exige para México que el formato integral incluya de manera explícita:<br><br><ol style="list-style-type: none"><li>1. El tratamiento que se da a los datos recabados</li><li>2. Quién es el responsable de almacenar los datos</li><li>3. Cómo ejercer los derechos ARCO</li><li>4. Cómo se darán a conocer los cambios en el Aviso de Privacidad</li><li>5. Cómo limitar el uso de los datos</li><li>6. Consentimiento para transferir datos</li><li>7. Revocar el consentimiento al tratamiento de los datos almacenados para el cuál fueron capturados</li><li>8. Revocar el consentimiento de transferir los datos a terceros</li><li>9. Información explícita sobre grupos vulnerables</li><li>10. Uso de cookies y tecnologías de recolección adicional de información</li><li>11. Indicar las consecuencias del posible mal uso de los datos</li><li>12. Sugerencias para prevenir malos actos</li></ol> |
| <b>Usabilidad</b><br>Auxilia al usuario para identificar los elementos de un Aviso de Privacidad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Consecuencias</b><br>El usuario puede identificar las partes de un Aviso de Privacidad, reconocer su importancia y ejercer sus derechos ARCO de manera oportuna.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Patrones relacionados</b> <ul style="list-style-type: none"><li>• Datos personales</li><li>• Datos personales sensibles</li><li>• Ejercicio de derechos ARCO</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

### Ejemplo A



## 5.4 Utilidad de las herramientas tradicionales de desarrollo en aplicaciones de seguridad

En la última sesión de revisión se les pidió a los participantes que evaluaran las herramientas utilizadas con base a la siguiente escala Likert:

- 1.- Totalmente en desacuerdo
- 2.- En desacuerdo
- 3.- Ni de acuerdo ni en desacuerdo
- 4.- De acuerdo
- 5.- Totalmente de acuerdo

Pregunta de investigación: “Las herramientas, guías y estándares que utilizó en su proyecto facilitan de forma significativa las siguientes tareas”. (Ver Tabla 5.2)

**Tabla 5.2** Utilidad de herramientas

| Proyecto                                         | Programación de APPs | GUIs de diseño de privacidad | Colecciones de íconos de privacidad |
|--------------------------------------------------|----------------------|------------------------------|-------------------------------------|
| 1                                                | 3                    | 2                            | 3                                   |
| 2                                                | 3                    | 2                            | 3                                   |
| 3                                                | 4                    | 3                            | 4                                   |
| 4                                                | 3                    | 3                            | 3                                   |
| 5                                                | 2                    | 2                            | 3                                   |
| Promedio                                         | 3                    | 2.4                          | 3.2                                 |
| Utilidad de la herramienta para el desarrollador | 3/5 = 60%            | 2.4/5 = 48%                  | 3.2/5 = 64%                         |

También se les pidió respondieran como equipo las siguientes preguntas:

1. ¿Existe un lenguaje universal que represente temas de seguridad informática y privacidad?

2. ¿Es oportuna la participación del área de diseño gráfico en la construcción de estas interfaces?

Se obtuvieron las respuestas presentadas en la Tabla 5.3.

**Tabla 5.3** Elementos adicionales

| Proyecto | Existencia de un lenguaje universal | Participación de Diseñadores |
|----------|-------------------------------------|------------------------------|
| 1        | Solo elementos aislados             | Si                           |
| 2        | No                                  | Si                           |
| 3        | No                                  | Si                           |
| 4        | No                                  | Si                           |
| 5        | No                                  | Si                           |

## 5.5 Impacto del uso de patrones de interacción en aplicaciones de seguridad

Durante el periodo de Verano 2013, a los alumnos que desarrollaron las Aplicaciones 1, 2, 3 y 4 se les explicó el concepto de Patrón de Interacción, desconocido hasta ese momento por los estudiantes, se les presentó la colección COPPEMA (Murillo, Sánchez, & Alfredo, 2013) y adicionalmente el patrón de Aviso de Privacidad (5.3.2) y se les pidió que estimaran cómo hubiera influido en sus proyectos realizados durante Otoño 2012 si hubieran tenido acceso a ellos desde el inicio de sus proyectos con base a la siguiente escala Likert:

1. Totalmente en desacuerdo
2. En desacuerdo
3. Ni de acuerdo ni en desacuerdo
4. De acuerdo
5. Totalmente de acuerdo

Pregunta de estudio: “¿Disponer de una colección de patrones de interacción relativa a privacidad facilitaría de forma significativa las tareas asociadas al desarrollo de la aplicación presentada en el periodo Otoño 2012?”. (Ver Tabla 5.4)

**Tabla 5.4** Tareas asociadas y calificación

| Proyecto                                      | Programar una aplicación sobre privacidad | Diseñar GUIs sobre privacidad | Consultar colecciones de íconos sobre privacidad |
|-----------------------------------------------|-------------------------------------------|-------------------------------|--------------------------------------------------|
| 1                                             | 4                                         | 5                             | 4                                                |
| 2                                             | 4                                         | 5                             | 5                                                |
| 3                                             | 4                                         | 5                             | 4                                                |
| 4                                             | 4                                         | 4                             | 4                                                |
| Promedio                                      | 4                                         | 4.75                          | 4.5                                              |
| Utilidad de herramientas para desarrolladores | 4/5 = 80%                                 | 4.75/5 = 95%                  | 4.5/5 = 90%                                      |

Finalmente, se les pidió que estimaran un promedio de horas ahorradas si hubieran contado con los patrones de interacción desde el inicio de su proyecto. (Ver Tabla 5.5)

**Tabla 5.5** Estimación de impacto de patrones de interacción en diseño de aplicaciones

| Proyecto       | Horas promedio reales invertidas | Horas promedio estimadas si se hubiera contado con los patrones de interacción |
|----------------|----------------------------------|--------------------------------------------------------------------------------|
| 1              | 20                               | 15                                                                             |
| 2              | 10                               | 7                                                                              |
| 3              | 12                               | 7                                                                              |
| 4              | 28                               | 23                                                                             |
| Total de horas | 70 horas                         | 52 horas                                                                       |

A continuación se muestra un comparativo de los valores obtenidos de utilidad para los desarrolladores al usar herramientas generales de desarrollo versus los patrones de interacción (Ver Tabla 5.6)

**Tabla 5.6** Herramientas generales versus Patrones de Interacción

|                                          | Programar una aplicación sobre privacidad | Diseñar GUIs sobre privacidad | Consultar colecciones de íconos sobre privacidad |
|------------------------------------------|-------------------------------------------|-------------------------------|--------------------------------------------------|
| Herramientas de desarrollo tradicionales | 60%                                       | 48%                           | 64%                                              |
| Patrones de Interacción                  | 80%                                       | 95%                           | 90%                                              |

Ningún equipo utilizó herramientas para construir prototipos previos ni se identificó alguna colección integral de elementos especializados que los ayudara en sus procesos de diseño y desarrollo. Se encontraron elementos de apoyo (clases en java, extensiones para tipos particulares de navegadores) que desde el punto de vista técnico apoyan al desarrollador de cualquier tipo de aplicación. (Ver Tabla 5.1).

Las herramientas utilizadas se consideran, de forma general, 60% útiles para el diseño de una aplicación relativa a privacidad (Ver Tabla 5.2), comparado con 80% del uso de patrones de interacción (Ver Tabla 5.4).

No se reconoce la existencia de un lenguaje universal en el área de seguridad informática, pero sí se reconoce que la participación de un diseñador gráfico es oportuna en estos proyectos. (Ver Tabla 5.3)

Se estima una reducción promedio del 25.7% del tiempo total dedicado al desarrollo de las aplicaciones si hubieran tenido disponible los patrones de interacción al inicio de los proyectos solicitados (Ver Tabla 5.5)

Las herramientas tradicionales de diseño son funcionales para crear aplicaciones de seguridad informática. Sin embargo, se estima que disponer de una colección de patrones de interacción facilitaría el trabajo a los desarrolladores de software al menos en un 20%. (Ver Tabla 5.6)

## 5.6 Discusión sobre la necesidad de patrones de interacción

En futuros estudios se podría incluir a egresados de estas carreras que estén inmersos en el campo laboral y estudiantes de Diseño Gráfico que tengan experiencia en participar en equipos de desarrollo de software.

El índice de satisfacción de los desarrolladores de aplicaciones de seguridad al usar herramientas tradicionales para el diseño de interfaces gráficas es muy bajo (Ver Tabla 5.2). Esto abre oportunidades para sugerir modelos que apoyen esta labor, pues las funciones de seguridad cada vez son más solicitadas para el software de usuario final, dado el aumento en número de usuarios de Internet.

Las herramientas generales de desarrollo de software permiten la construcción efectiva de aplicaciones (Ver Tabla 5.1), sin embargo, disponer de una colección de patrones de interacción facilita las tareas de diseño de una aplicación relativa a privacidad. Los patrones de interacción se presentan como una buena práctica en el ciclo de desarrollo de software (Ver Tabla 5.6) y se reduce el tiempo invertido en los proyectos (Ver Tabla 5.5).

Reconocer que no existe un lenguaje universal relativo a seguridad informática presenta áreas de oportunidad para proponer elementos que permitan enriquecer la colaboración entre expertos y equipos multidisciplinarios, el aprendizaje para quienes inician en esta área y el incremento de la cultura de este tema en los usuarios finales. (Ver Tabla 5.3)

La construcción de una colección de patrones de interacción que incluya estos resultados puede influir en temas de usabilidad y experiencia de usuario, al construir herramientas que apoyen en la administración de la privacidad. Muchas aplicaciones son desarrolladas sólo por expertos de seguridad, y esto hace que técnicamente cumplan los requerimientos funcionales, pero están alejadas de resolver problemas reales para los usuarios.

La interacción actual con los elementos de un aviso de privacidad no facilita el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición), haciendo que el usuario de Internet navegue en modo inseguro, quedando a expensas de los posibles malos usos que le puedan dar a tus datos personales. Desde el marco técnico y legal se cubre el objetivo de presentar al usuario las políticas acerca del tratamiento que se da a sus datos, pero el objetivo final, que consiste en proteger a las personas y facilitarles el ejercicio de los derechos ARCO, no se cumple. La experiencia de usuario registrada acerca de la interacción con un aviso de privacidad no es positiva.

Los elementos que facilitan el diseño y construcción de interfaces que involucren temas de privacidad para usuario final son escasos. Para implementar este tipo de aplicaciones se puede usar cualquier metodología y herramientas de desarrollo de software de acuerdo a los requerimientos solicitados y a los recursos disponibles, sin embargo, al contar con un conjunto de patrones de interacción específicos se reducen los recursos involucrados. Se sugiere como trabajos futuros proponer colecciones de patrones de interacción que incluyan ejemplos basados en la forma en que las personas aprenden e interactúan con interfaces humano-computadora para mejorar el índice de cultura de seguridad informática de los usuarios de Internet, disminuir riesgos y mitigar problemas asociados.

## 5.7 Resumen de patrones de interacción generados

Después de identificar las herramientas que se utilizan para construir aplicaciones relativas a seguridad, los factores críticos de privacidad de datos personales, los factores críticos para la administración de una y red y sus respectivas correlaciones más significativas con factores humanos, se propone un conjunto de patrones de interacción que aportan soluciones específicas en el campo de la seguridad informática y se demostró que es posible mejorar la experiencia de usuario.

Del capítulo 3, Administración de datos personales e interfaz de usuario, surgen dos patrones de interacción:

1. **Aviso de privacidad integral.** Se propone una alternativa de navegación modular para un documento que por ley se exige hacer disponible en un formato de solo texto en un lenguaje legal que resulta poco claro para sus usuarios. Con esta propuesta, las personas pueden identificar las partes que lo componen, la relación que existe entre dichos elementos así como el riesgo asociado a una mala administración de datos personales en el ámbito de la privacidad en Internet.
2. **Ejercicio de derechos ARCO (Acceso, Rectificación, Consulta, Oposición).** Esta propuesta presenta los elementos necesarios para que los usuarios de Internet puedan identificar y ejercer los derechos ARCO, así como reconocer las consecuencias asociadas a una mala administración de los datos personales.

Del capítulo 4, Administración de seguridad de red e interfaz de usuario, surgen dos patrones de interacción:

1. **Sistema de detección de intrusos.** A través de este patrón de interacción, un administrador puede identificar violaciones lógicas de seguridad dentro de una red. Se propone una interfaz que suple a la tradicional línea de comandos y ofrece una alternativa para quienes están poco familiarizados con ella o que la interacción de los usuarios con medios electrónicos ha sido en su mayoría de forma gráfica. Esta propuesta considera la experiencia previa de los usuarios con otras herramientas relativas a la gestión de una red.
2. **Descifrador de contraseñas.** Esta alternativa permite al administrador de una red aplicar conceptos básicos de gestión de seguridad para una tarea concreta como lo es descifrar las contraseñas de los usuarios en un grupo de trabajo. Esta actividad tiene su base en los principios de ética que sugieren auto atacar a una red para descubrir vulnerabilidades que puedan ser aprovechadas por terceros para actividad ilícita y proponer soluciones antes de que ocurran.

Se espera que al implementar soluciones basadas en estas propuestas se aprovechen los recursos invertidos y se mejore la experiencia de los usuarios que dispongan de estas herramientas para tareas relativas a seguridad.

## Capítulo 6. Conclusiones

---

*“Después de escalar una montaña muy alta, descubrimos que hay otras montañas por escalar”*

*Nelson Mandela*

En este capítulo se presentan las conclusiones generales de la investigación, la síntesis del trabajo desarrollado y el cumplimiento de los objetivos.

## 6. Conclusiones

Al iniciar el presente trabajo se postuló la idea de que sería posible definir una estrategia para mejorar la experiencia de usuario con factores críticos de seguridad informática. Esta situación se abordó considerando a la persona como actor central en la interacción con aplicaciones de software que involucran temas de seguridad. El estudio de este fenómeno se hizo desde tres perfiles distintos:

- Para usuarios no expertos: Se identificaron los factores críticos de la administración de privacidad de datos y su relación con los elementos de interfaz y factores humanos.
- Para usuarios expertos: Se identificaron los factores críticos de la administración de redes y su relación con los elementos de interfaz y factores humanos. Se compararon los resultados de medir la usabilidad de un conjunto de herramientas existentes y de un grupo de patrones de interacción propuestos en este trabajo.
- Para los desarrolladores de aplicaciones de seguridad: Se reconocieron las herramientas que se utilizan para el diseño y desarrollo de sistemas, se validó un conjunto de patrones de interacción y se midió su utilidad con respecto al uso de herramientas tradicionales.

A continuación se describen las conclusiones de los resultados obtenidos de las estrategias mediante una síntesis, después se enumera el cumplimiento de los objetivos propuestos para finalmente recomendar líneas de acción de trabajo a futuro.

### 6.1 Síntesis del trabajo desarrollado

#### Administración de datos personales e interfaz de usuario

Se logró identificar la experiencia de usuario con temas relativos a privacidad de información como un área de oportunidad para aportar nuevos modelos y soluciones, pues a pesar de que las aplicaciones y sitios de internet cumplen con los términos y contenidos exigidos por la ley, la realidad es que el usuario final se siente ignorado, desconcertado, decepcionado y confundido ante las opciones existentes para administrar y controlar sus datos personales. Esto implica áreas de oportunidad para quienes desarrollan software, pues es importante conjuntar términos legales, empatía con el usuario final y una adecuada interfaz que facilite la importante tarea de administrar los datos de las personas de forma pertinente y con impacto real.

Se encontraron las correlaciones (basadas en el Coeficiente de Correlación de Pearson) más importantes entre elementos de interfaz (personalización de navegador, lenguaje simple y diseño atractivo, entre los más relevantes) y factores de privacidad (elementos de un aviso de privacidad y tareas relativas al ejercicio de los derechos), para sugerir futuras implementaciones que mejoren la experiencia de usuario. Uno de los hallazgos más significativos consiste en el alto grado de satisfacción que tienen los usuarios sobre el manejo de su privacidad, sin embargo las acciones que toman para proteger sus datos son escasas o nulas. Esto implica que las personas no están conscientes de la trascendencia de este tema.

Se exploró la idea de incluir el estilo de aprendizaje (de acuerdo a la estructura propuesta por (CHAEA, 2002)) de las personas como un factor humano determinante en la generación de interfaces que mejoren la experiencia de usuario. En los estudios iniciales se identificó un comportamiento similar para todos los estilos de aprendizaje ante los temas de privacidad, encontrando con esto que las interfaces actuales no cumplen con su objetivo para ningún tipo de persona en particular.

### **Herramientas de administración de seguridad e interfaz de usuario**

Se aplicó un método de medición de usabilidad a un conjunto de herramientas de administración de seguridad en una red para usuarios expertos y se encontró que la percepción no es favorable. En general se reconoce que se debe dominar el uso de la línea de comandos pues durante muchos años la mayoría de las herramientas más poderosas se han desarrollado en este ambiente, sin embargo, cada vez son más las personas del área tecnologías de información que han crecido interactuando con ambientes gráficos y no resulta natural trabajar con espacios limitados sin opciones de personalización. Los resultados de este estudio sugieren que el desempeño del administrador podría mejorar si se implementan tópicos de usabilidad en interfaces de administración de seguridad y mejorar así la experiencia de usuario.

### **Patrones de interacción y diseño de interfaces**

Tradicionalmente los elementos que facilitan el diseño y construcción de interfaces que involucran temas de privacidad para usuario final son escasos. Para implementar este tipo de soluciones se usa cualquier metodología y herramientas de desarrollo de software de acuerdo a la experiencia del equipo de desarrollo, a los requerimientos solicitados y a los recursos disponibles. Mediante este trabajo, al contar con un conjunto de patrones de interacción específicos se reducen los recursos involucrados de acuerdo a las estimaciones calculadas en esta parte del proyecto. De acuerdo a la opinión de los desarrolladores, se identificó que las herramientas tradicionales son útiles en un 60% y los patrones de interacción diseñados como parte de este proyecto lo son en un 80%. Se estimó una reducción del tiempo invertido del 25% en el desarrollo de aplicaciones.

## **6.2 Cumplimiento de objetivos**

### **Acerca de identificar correlaciones significativas entre factores críticos de seguridad, elementos de interfaz y factores humanos:**

En la fase inicial de este trabajo, se identificaron cuáles son los factores críticos de seguridad que tienen impacto en las tareas más importantes relacionadas a privacidad de datos personales, para usuarios no expertos, y administración de una red, para usuarios expertos. Después se identificaron los elementos de interfaz que son importantes desde la perspectiva de los usuarios y que deben ser tomados en cuenta de forma estratégica en los diseños de este tipo de aplicaciones. Se consideró el estilo de aprendizaje como un factor humano que pudiera ser determinante en el diseño de interfaces de seguridad. Sin embargo, en las primeras indagaciones al respecto, se detectó que, la interacción actual

con temas de seguridad se mantenía constante sin importar el estilo de aprendizaje. Una vez identificados los factores críticos, se obtuvieron las correlaciones numéricas más significativas entre ellos de acuerdo a la importancia que le dan los usuarios a cada uno de ellos en relación a una tarea en particular, para considerarlas en implementaciones de interfaces. La aportación de este trabajo reside en proponer un modelo para construcción de interfaces donde las correlaciones se interpretaron al colocar los elementos con un grado de proximidad entre ellos de acuerdo al valor de la correlación, el tamaño del elemento de acuerdo al grado de importancia para el usuario y así sugerir una interacción con mayor sentido y familiaridad a las personas en las interfaces, impactando a la experiencia de usuario.

### **Acerca de documentar factores de la experiencia de usuario en torno a la interacción con tópicos emergentes de seguridad:**

Al inspeccionar la situación actual de cómo se relacionan los usuarios (expertos o no) con los factores críticos de seguridad, se identificaron que las interfaces no facilitaban esta tarea. Por un lado, quienes son responsables de hacer disponibles las aplicaciones cumplen con los requerimientos funcionales de las mismas y asumen que los usuarios serán los responsables de interpretarlas y usarlas correctamente. Los usuarios reconocen que son ellos quienes deben adaptarse a las interfaces, deseando que de alguna manera se les ofreciera la opción inversa (que las interfaces se adapten a los usuarios). Las tecnologías de información en este sentido no están cumpliendo con el objetivo de facilitar las tareas del ser humano, sino que se presentan como algo incuestionable, de élite, misterioso, donde es mejor dejar las opciones que vienen por default y pocos son quienes por necesidad o por ocio invierten tiempo en comprenderlas y sacar beneficio de ellas. Se identificaron frustración, enojo, sentimiento de no ser tomado en cuenta, limitados y que la interfaz hace sentir al usuario final como un ignorante. La aportación de este trabajo es sugerir que las interfaces gráficas sean personalizables tanto para expertos como no expertos, pues lo personalizable es ya más natural en las nuevas generaciones.

### **Acerca de valorar el uso de patrones de interacción en la construcción de interfaces efectivas de seguridad:**

Se distinguieron las principales herramientas y metodologías utilizadas tradicionalmente para diseñar y construir interfaces que involucran temas de seguridad. Éstas en su mayoría son instrumentos tradicionales y se seleccionan de acuerdo a la experiencia del equipo de desarrollo, a los requerimientos funcionales y a los recursos disponibles. No se identificó alguna colección significativa de herramientas en el área de seguridad que facilitara el trabajo de los desarrolladores y evitara construir un conjunto de proyectos solicitados con alguna ventaja o adelanto con respecto a otro tipo de aplicaciones, considerando solo las facilidades de los lenguajes de programación. La aportación fue presentar a los patrones de interacción como una alternativa de alto impacto para los desarrolladores en temas de seguridad y se midió que los recursos involucrados en el diseño y desarrollo fueron más eficientes y la productividad de los desarrolladores mayor.

**Acerca de producir un conjunto de patrones de interacción basado en factores humanos que facilite la percepción y manipulación de interfaces relativas a seguridad informática en un entorno universitario:**

La aportación de esta fase consistió en la definición, implementación y validación de ejemplos de interacción, resumidos en el capítulo 5.7

Los ejemplos de interacción para cada uno de los patrones fueron validados en diversos grupos de prueba con una mejora significativa en la usabilidad.

## Capítulo 7. Trabajo y líneas de investigación futuras

---

*“El hombre no puede descubrir nuevos océanos a menos que tenga el coraje de perder la vista de la costa”*

*Andre Gide*

En este capítulo se presentan el trabajo y líneas de investigación futuras.

## **7. Trabajo y líneas de investigación futuras**

Se presentan a continuación algunas propuestas de mejora al modelado de patrones de interacción desarrollado en esta tesis así como nuevas líneas de avance en la investigación.

### **Profundizar en los estilos de aprendizaje como factor crítico de mejora en la experiencia de usuario**

Dado que existen diversas taxonomías para describir los estilos de aprendizaje y cada una de ellas identifica diversos factores humanos como característicos, se sugiere analizarlas para investigar los efectos que pueden tener en su implementación de interfaces en el tema de seguridad. De esta manera, se podría disponer de una colección de patrones de interacción con mayores opciones para los responsables de implementar soluciones que aporten de forma efectiva en la experiencia de usuario.

### **Ampliar los perfiles de evaluación**

Todos los estudios dirigidos que se realizaron en este trabajo estuvieron limitados a un sector poblacional universitario. Es importante contar con la participación de otros sectores de la sociedad (edad, escolaridad, personas con capacidades diferentes, lenguas indígenas) para identificar necesidades propias de otros grupos para construir propuestas de interacción.

### **Evaluar patrones de interacción para tecnologías emergentes**

Las tecnologías móviles están incrementando su participación en el mercado de forma activa y se espera que esta tendencia continúe los próximos años. El paradigma de interacción con aplicaciones diseñadas para dispositivos móviles está en proceso de maduración con el creciente número de usuarios. Estas herramientas han desplazado a cierto sector de personas que tradicionalmente trabajaban desde una computadora de escritorio, con un monitor, teclado y mouse por separado. Es necesario analizar si los conceptos básicos de seguridad informática se verán modificados ante las nuevas formas de acceder a los sistemas y aplicaciones que los involucran.

### **Desarrollar métricas para evaluar usabilidad en el área de seguridad**

Existen hoy en día diversas metodologías para evaluar la usabilidad de un producto. La mayoría se enfocan a características generales y muestran resultados que son de gran utilidad en la toma de decisiones. Sin embargo, el área de seguridad informática se ha distinguido por mucho tiempo como un área exclusiva, donde se requiere un alto conocimiento técnico, y en ocasiones, pareciera que se desea mantener así, sin permear sus beneficios a los múltiples tipos de usuarios. Es importante generar herramientas que faciliten la construcción de interfaces efectivas para mejorar la interacción con factores de seguridad. Algunos años atrás, era extraño encontrar personas que hubieran tenido un acercamiento con algún tipo de dispositivo de cómputo desde temprana edad. Hoy en día, la mayoría de los niños desarrollan un paradigma de interacción natural con aplicaciones

gráficas. Esto debe ser considerado para proyectar el tipo de aplicaciones que se esperarían en un futuro cercano, y no sea ésta una razón para desanimar a los aspirantes de carreras relativas a tecnologías de información, tan escasos en estos tiempos.

### **Búsqueda de soluciones para mejorar la cultura de seguridad informática**

En este trabajo se detectó que el índice de cultura relativa a seguridad informática no es el deseable en una población universitaria. Esto es una problemática significativa que vale la pena ser analizada, pues para otros sectores de la sociedad, los cuales representan un grupo mayoritario, los resultados podrían ser alarmantes.

### **Validación del método de construcción de interfaces basado en correlaciones**

Se sugiere formalizar y evaluar el modelo sugerido en el apartado 3.2.7 para construir interfaces basados en valores de las correlaciones de los factores involucrados en un procedimiento a automatizar. Esto puede sugerir una alternativa para optimizar recursos al diseñar y construir interfaces usables no solo en el área de seguridad informática.

## 8. Referencias

- (HHS), D. C. (2004). *Usability.gov*. Obtenido de <http://www.usability.gov/what-and-why/user-experience.html>
- 25010:2011, I. (s.f.). *Systems and software Quality Requirements and Evaluation (SQuaRE)*. ISO.
- Acosta, A., & Zambrano, N. (2011). Importancia, Problemas y Soluciones en el Diseño de la interfaz de Usuario. *SABER*. ISSN: 2243-6468.
- Acosta, A., & Zambrano, N. (2011). *Importancia, Problemas y Soluciones en el Diseño de la interfaz de Usuario*. Obtenido de <http://www.ciens.ucv.ve:8080/genasig/sites/topicosihc/archivos/Modelo-AcostaZambrano-Saber.pdf>
- AMIPCI, A. M. (2012). *Estudio de Protección de Datos personales entre usuarios y empresas*. Obtenido de <http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=95&Type=1>
- AMIPCI, A. M. (2012). *Hábitos de los usuarios de Internet en México 2012*. Recuperado el 13 de abril de 2012, de <http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=115&Type=1>
- Arhippainen L., T. M. (2003). *Empirical Evaluation of user experience in two adaptative mobile application prototypes*. Norrköping, Sweden: Proceedings of the 2nd international conference on mobile and ubiquitous multimedia.
- AT&T. (1999). *Privacy bird*. Obtenido de [www.privacybird.org/](http://www.privacybird.org/)
- Bayle, E. (1998). Putting It All Together. Towards a Pattern Language for Interaction Design: ACHI 97 Workshop. SIGCHI Bulletin. *ACM SIGCHI*, 17-23.
- Berners-Lee, T. (1997). *The World Wide Web Consortium*. Recuperado el 2013, de <http://www.w3.org/>
- Bevan, N. (1999). Quality in use: meeting user needs for quality. *Journal of Systems and Software*, (págs. 89-96).
- Bevan, N., Kirakowsky, J., & Maissel, J. (1991). What is Usability. *Proceedings of 4th Intl. Conference on HCI*.
- Borchers, J. (2001). *A pattern approach to interaction design*. England: Wiley.
- Brook, J. (1998). *System Usability Scale*. Digital Equipment Co Ltd., Reading.

- Burns, B., & Killion, D. (2007). *Security power tools*. O'Reilly.
- Cartas, A. (2008). Políticas de privacidad en P3P y XACML. *ITAM. Laboratorio de redes avanzadas*.
- Caviglione, L. (2013). Using XACML for access control in Social Networks . En *Social Network Engineering for Secure Web Data and Services*. Information Science Reference.
- Cela, K., Fuentes, W., Alonso, C., & Sánchez, F. (2010). Evaluación de herramientas web 2.0, estilos de aprendizaje y su aplicación en el ámbito educativo. *Revista de Estilos de Aprendizaje*, no. 5.
- CHAEA. (2002). *Cuestionario Honey Alonso de Estilos de aprendizaje*. Obtenido de <http://www.estilosdeaprendizaje.es>
- Chiasson, S., Biddle, R., & Somayaji, A. (2007). Even Experts Deserve Usable Security: Design guidelines for security management systems. *Workshop on Usable IT Security Management. SOUPS 2007*.
- Claridge, N., & Kirakowski, J. (1984). *Website Analysis and MeasureMent Inventory*. Obtenido de <http://www.wammi.com/>
- Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Tech*, 186-196 .
- Constantine, L. (1999). *Software for Use: A Practical Guide to the Models and Methods of Usage-Centered Design*. Addison-Wesley.
- Conti, G., Ahamad, M., & Staskp, J. (2005). Attaking Information Visualization System Usability. Overloading and Deceiving the Human. *Symposium On Usable Privacy and Security (SOUPS)*.
- Cranor, L. F., & Garfinkel, S. (2005). *Security and Usability. Designing Secure Systems That People Can Use*. O'Reilly.
- Cranor, L., Langheinrich, M., & Marchiori, M. (2002). *W3C The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. Recuperado el 2013, de <http://www.w3.org/TR/P3P/>
- Cranor, L., Romanowsky, S., Hong, J., Acquisti, A., & Friedman, B. (2006). *Privacy Patterns for Online Interactions*. Obtenido de <http://repository.cmu.edu/hcii/72>
- Datos, I. F. (2012). *Guía práctica para generar el aviso de privacidad*. Obtenido de <http://inicio.ifai.org.mx/DocumentosdelInteres/privacidadguia.pdf>
- Desmet, D., Hekkert, P., & Hillen, M. (2003). *Values and emotions; an empirical investigation in the relationship between emotional responses to products and human values*. Barcelona, Spain: Proceedings of the fifth European academy of design conference.

- Dulaney, E. (2011). *Security +*. Sybex.
- El-Aziz, A. (2013). *Algorithms for mapping of XACML policies into temporal relations*. Lambert.
- Emerson, X., & Wladimir, M. (2013). Writing Access Policies to Protect Web Services of a Spatial Data. *Agile 2013 Proceedings*.
- Esponda, S. (2007). *Sistema de Autorización para Web Services*. Universidad de Belgrano.
- Esposito, D. (2011). *Browser Helper Objects: The Browser the Way*. Obtenido de MSDN Library: [http://msdn.microsoft.com/en-us/library/bb250436\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/bb250436(v=vs.85).aspx)
- Fácil, C. (2012). *Generador de avisos de privacidad*. Obtenido de <https://www.contratosfacil.com/document/51015f1c6df58/Generador-automtico-de-tu-Aviso-de-Privacidad-personalizado-en-minutos>
- Ferraiolo, D. (2007). *Role-Based Access Control*. Artech House.
- Foster, J., & Vincent, L. (2006). *Writing Security Tools and Exploits*. . Syngress Publishing.
- Gage Kelley, P., Cesca, L., & Faith, L. (s.f.). <http://repository.cmu.edu/cylab/1/>. *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*.
- Gage-Kelley, P., Brewer, R., Mayer, Y., Cranor, L., & Sadeh, N. (2011). An Investigation into Facebook Friend Grouping. *Human-Computer Interaction – INTERACT 2011*, 216-233.
- Gagne, A., & Beznosov, K. (2008). Human, Organizational, and Technological Factors of IT Security. *CHI '08 Extended Abstracts on Human Factors in Computing Systems*.
- Gamma, E., Helm, R., Ralph, J., & Vlissides, J. (1995). *Design Patterns*. Addison-Wesley.
- Garfinkel, S., & Faith, L. (2005). *Security and Usability. Designing Secure Systems That People Can Use*. O'Reilly .
- Gonzalez-Tablas, A. (2008). CERTILOC: Implementation of a Spatial-Temporal Certification Service Compatible with Several Localization Technologies. *Third International Conference on Availability, Reliability and Security, 2008. ARES 08. IEEE.*, 363-368.
- Hannaford, C. (2011). *Cómo aprende tu cerebro*. Pax.
- Harper, R. (2012). *Practical Foundations for Programming Languages*. Cambridge University Press.
- Hassan-Montero, Y. (2006). Factores del Diseño Web Orientado a la Satisfacción y No-Frustración de Uso. . *Revista Española de Documentación Científica*, 239-257.
- Hawkey, K., & Botta, D. (2008). Human, organizational, and technological factors of IT security. *CHI '08 Extended Abstracts on Human Factors in Computing System*.

- Hekkert, P. (2001). *The Experience of Design*. Aveiro, Portugal: 4EAD conference.
- Henninger, S. (2001). Supporting Design through Usability Guidelines and Patterns. *CHI2001 Workshop on Tools, Conceptual Frameworks, and Empirical Studies for Early Stages of Design*.
- Hernández Sampieri, R. (2010). *Metodología de la investigación*. Mc Graw Hill.
- Hernández-Hernández, M. E., Alvarez-Carrión, G., & Muñoz-Arteaga, J. (2012). *Patrones de Interacción para el Diseño de Interfaces WEB usables*. Obtenido de [www.willydev.net/descargas/PatronInter.pdf](http://www.willydev.net/descargas/PatronInter.pdf)
- Herrmann, J. (2010). Access Control Systems for Spatial Data Infrastructures and their Administration GeoXACML and the Layered Administration Model. *Proceedings of the 1st International Conference and Exhibition on Computing for Geospatial Research & Application*. ACM.
- Honey, A. (2011). CHAEA. *Cuestionario Honey Alonso de Estilos de aprendizaje*. Obtenido de <http://www.estilosdeaprendizaje.es>
- Iervolino, F. (2013). *Support XACML Policies within an advanced architecture for UserPrivac*. Lambert.
- Institute, S. E. (2000). *CERT Computer Emergency Response Team*. Obtenido de <http://cert.org>
- INTECO., I. N. (2011). *Gestión de la Seguridad*. Obtenido de [http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/demostrador/monografico\\_gestion\\_seguridad.pdf](http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/demostrador/monografico_gestion_seguridad.pdf)
- Irons, L. (2003). *Rapid Ethnography for User Experience Design*. . I.C. Technologies White Paper.
- Islam, S., & Dong, W. (2008). Human Factors in Software Security Risk Management. *1st International Workshop on Leadership and Management in Software Architecture (LMSA08)*.
- Jackson, G. (2012). *Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security*. John Wiley & Sons.
- Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools. *SIGCHI conference on Human Factors in Computing Systems*, 471-478.
- Joseph, Y., & Baraclow, J. (1997). *Architectural Patterns for Enabling Application Security*.
- Kandogan, E., & Haber, E. (2005). Security Administration Tools and Practices. En L. Cranor, *Security and Usability* (págs. 357-378). O'Reilly.

- Kandogan, E., & Haber, E. (2005). *Security Administration Tools and Practices*. Recuperado el 2014, de <http://www.plunk.org/eben/PublishedPapers/Security-ch18.pdf>
- Kankainen, A. (2002). *Thinking model and tools for understanding user experience related to information appliance product concept*. Espoo, Finland: Tesis doctoral, Hlesinky University of Technology.
- Karat, J., & Helander, M. (1997). User-centered software evaluation methodologies. En *Handbook of human-computer interaction*,.
- King, J., Lampine, A., & Smolen, A. (s.f.). *Privacy: Is there an app for that? Symposium On Usable Privacy and Security*. Recuperado el 2013, de <http://dl.acm.org/citation.cfm?id=2078843>
- King, J., Lampinen, A., & Alex, S. (2011). *Privacy: Is there an app for that?. Symposium on Usable Privacy and Security (SOUP'11)*. SOUP'11.
- Kirakowski, J. (1994). *Software Usability Measurement Inventory*. Obtenido de <http://www.ucc.ie/research/hfrg/questionnaires/sumi/index.html>
- Kirakowski, J. (2004). *Measuring the Usability of Multi-Media Systems*. Obtenido de <http://www.ucc.ie/research/hfrg/questionnaires/mumms/index.html>
- Komanduri, S., & Shay, R. (2011). Of Passwords and People: Measuring the Effect of Password-Composition Policies. *CHI 11. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.
- Kraemer, S. (2006). An adversarial viewpoint of human and organizational factors in computer and information security. *Doctoral Dissertation. University of Wisconsin*.
- Krug, S. (2006). No me hagas pensar. Una aproximación a la usabilidad en la web. Prentice Hall.
- Laugwitz, B. S. (2008). Construction and evaluation of a user experience questionnaire. . *USAB 2008, LNCS 5298*, 63-76.
- Lewis, J. R. (1995). *Computer System Usability Questionnaire*. Obtenido de <http://hcibib.org/perlman/question.cgi>
- Life, P. (2008). *HCI Patterns Collection - Version 2*. Recuperado el 2013, de [http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci\\_pattern\\_collection\\_v2-public.pdf](http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf)
- Lindskog, H. (2003). *Web Site Privacy with P3p*. Wiley.
- Lindskog, H. (2003). *Web Site Privacy with P3P*. Wiley.

- Lockhart, H. (2013). *eXtensible Access Control Markup Language (XACML) TC*. Obtenido de Organization for the Advancement of Structured Information Standards: <https://www.oasis-open.org>
- López, C.-S. (2011). El papel del color en los espacios inmateriales. *Libros Básicos en la Historia del Campo Iberoamericano de Estudios en Comunicación*.
- Loukides, M. (2002). *System performance tuning*. O'Reilly & Associates, Inc.
- Luse, A. (2009). *Exploring utilization of visualization for computer and network security*. Digital Repository @ Iowa State University.
- Luse, A. (2009). *Exploring utilization of visualization for computer and network security*. Obtenido de Digital Repository @ Iowa State University: <http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3030&context=etd>
- Madden, M., & Lenhart, A. (2013). Teens, Social Media, and Privacy. *Pew Research Center*.
- Malhortra, N. (2008). *Investigación de Mercados*. Pearson Prentice Hall. 5ª. Edición.
- Malone, E., Leacock, M., & Wheeler, C. (2005). *Implementing a Pattern Library in the Real World: A Yahoo! Case Study*. Obtenido de <http://boxesandarrows.com/implementing-a-pattern-library-in-the-real-world-a-yahoo-case-study/>
- Marti, R. (2009). *Applied Security Visualization*. Pearson.
- Maurer, M.-E. (2011). Using Data Type Based Security Alert Dialogs to Raise. *SOUPS 2011. Proceedings of the Seventh Symposium on Usable Privacy and Security*.
- Mayhew, D. (1999). *The Usability Engineering Lifecycle*. Elsevier Books, Oxford.
- Mcdonald, A., Robert, R., Gage-Kelley, P., & Cranor, L. (2010). A Comparative Study of Online Privacy Policies and Formats. *CHI '10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (págs. 1573-1582 ).
- Mendoza, R. (2009). Web Service-Security Specification based on Usability Criteria and Pattern Approach. *Journal of Computer*.
- México, S. d. (s.f.). *Manual de estilos de aprendizaje*. Obtenido de [http://www.dgb.sep.gob.mx/informacion\\_academica/actividadesparaescolares/multimedia/Manual.pdf](http://www.dgb.sep.gob.mx/informacion_academica/actividadesparaescolares/multimedia/Manual.pdf)
- Miller, D., & Harris, S. (2011). *Security Information and Event Management (SIEM) Implementation*. McGraw-Hill/Osborne.

- Miloslav, H. (2010). Usability versus security of authentication. *COMATIA'10 Proceedings of the 2010 international conference on Communication and management in technological innovation and academic globalization*.
- Montero, Y. H. (s.f.). *Introducción a la interacción persona-ordenador*. PID\_00176056.
- Moreno, A., & Sánchez-Segura, M. (2003). Patrones de Usabilidad: Mejora de la Usabilidad del Software. *VIII Jornadas de Ingeniería del Software y Bases de Datos (JISBD'03)*. Alicante.
- Morville, P. (2004). *Semantic Studios*. Recuperado el 2014, de <http://semanticstudios.com/publications/semantics/000029.php>
- Muñoz Arteaga, J., Medina Medina, A., Guerrero, J., & Muñoz Lopez, J. (2009). A methodology for designing information security feedback based on User Interface Patterns. *Advances in Engineering Software*, 1231-1241.
- Muñoz Arteaga, J., Medina Medina, A., Guerrero, J., & Muñoz Lopez, J. (2010). *Patrones de Interaccion para el Diseño de la Retoalimentación Visual de Sitios Web Seguros*. Obtenido de <http://www.aipo.es/articulos/2/50.pdf>
- Muñoz Arteaga, J., Medina Medina, A., Guerrero, J., & Muñoz Lopez, J. (2010). *Patrones de Interaccion para el Diseño de la Retoalimentación Visual de Sitios Web Seguros*. Obtenido de <http://www.aipo.es/articulos/2/50.pdf>
- Murillo, S. (2001). *ASIS: Diseño y Aplicación de un Sistema Integral de Seguridad Informática*. Obtenido de [http://catarina.udlap.mx/u\\_dl\\_a/tales/documentos/msp/murillo\\_c\\_sr/](http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/murillo_c_sr/)
- Murillo, S. R., & Sánchez, J. .. (2013). Patrones de interacción y su aplicación a la privacidad en Internet. *Segundo congreso internacional de ingeniería de sistemas INCOSE*. Puebla, México: ISBN: 978-607-8093-27-4.
- Murillo, S. R., & Sánchez, J. A. (2013). Studying the Relationships between the Management of Personal Data Privacy and User Interface. *Human Computer Interaction. Lecture Notes in Computer Science Volume 8278*, 79-89.
- Murillo, S. R., & Sánchez, J. A. (2014). Enhancing privacy awareness through interaction design. *XV International Conference on human computer interaction*.
- Nemeth, E., & Snyder, G. (2011). *Unix system administrator handbook*. Prentice Hall.
- Nielsen, J. (1993). *Usability Engineering*. Academic Press.
- Nielsen, J., & Normand, D. (1998). *Evidence-Based User Experience Research, Training, and Consulting*. Obtenido de <http://www.nngroup.com/>
- NNG. (2003). Recuperado el 2014, de Nielsen and Norman Group: <http://www.nngroup.com/about/userexperience.htm>

- Norman, K., Shneiderman, B., & Harper, B. (1995). *Questionnaire for User Interaction Satisfaction*.  
Obtenido de <http://www.cs.umd.edu/hcil/quis/>
- Openwall. (2001). *John the Ripper password cracker*. Obtenido de  
<http://www.openwall.com/john/>
- Paluch, K. (2006). *What is User Experience Design*. . Obtenido de  
<http://www.montparnas.com/articles/what-is-user-experience-design/>
- Parlamentarios, C. d. (2010). *Ley federal de protección de datos personales en posesión de los particulares*. México.
- Peter, K. (2012). *Information Flow Based Security Control Beyond RBAC*. Springer Vieweg.
- Preece, J. (1994). *Human-Computer Interaction: Concepts And Design*. Addison Wesley.
- Programme., E. C. (2010). *PRIMELIFE . HCI Pattern Collection – Version 2*. Obtenido de  
[http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci\\_pattern\\_collection\\_v2-public.pdf](http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf)
- Quesenbery, W. (2001). *“What Does Usability Mean: Looking Beyond 'Ease of Use'.* Obtenido de  
<http://www.wqusability.com/articles/>
- Rajbhandari, L. (2013). Consideration of Opportunity and Human Factor: Required Paradigm Shift for Information Security Risk Management. *EISIC '13 Proceedings of the 2013 European Intelligence and Security Informatics Conference*.
- Ramachandran, V., & Blakeslee, S. (1999). *Phantoms in the Brain: Probing the Mysteries of the Human Mind*. William Morrow.
- Ramírez-Barrera, W. (2012). La experiencia de usuario y la usabilidad. *Schema*, 67-86.
- Rauschenberger, M., & Medien-Systempartne, M. (2012). Measurement of user experience: A Spanish language version of the user experience questionnaire (UEQ). *Information Systems and Technologies (CISTI). 7th Iberian Conference on*, 1-6.
- Rebollo, L. (s.f.). *Vida privada y protección de datos. Un acercamiento a la regulación internacional europea y española*. Recuperado el 2014, de Biblioteca virtual del instituto de investigaciones jurídicas de la UNAM:  
<http://biblio.juridicas.unam.mx/libros/6/2758/10.pdf>
- Redish, J. (1995). Are we really entering a post-usability era? *ACM SIGDOC Asterisk Journal of Computer*, (págs. 18-24).
- Reed, C. (1994). *Open Geospatial Consortium*. Obtenido de <http://www.opengeospatial.org/>
- Research, S. (2001). *Secure Internet Management and SNMP*. Obtenido de <http://www.snmp.com/>

- Roam, D. (2013). *The Back of the Napkin: Solving Problems and Selling Ideas with Pictures*. Portfolio Trade.
- Ross, S. (2010). *Unix system security tools*. McGraw-Hill.
- Rosson, M., & Carroll, J. (2002). *Usability engineering*. Morgan Kaufmann.
- Rubio-Valdehita, S., Díaz-Ramiro, E., & López-Higes, R. (2012). Effects of task load and cognitive abilities on performance. *Anales de psicología*, 28(3), 986-995.
- Rusu, C. (2014). Usability versus User Experience:Theory and Practice. *XV International Conference on Human Computer Interaction* (pág. 20). Puerto de la Cruz, Tenerife. Spain: AIPO.
- Saffer, D. (2008). *The disciplines of user experience*. Obtenido de <http://www.kickerstudio.com/2008/12/the-disciplines-of-user-experience/>
- SANS, I. (2013). *Securing Linux/Unix*. Obtenido de <https://www.sans.org/course/securing-linux-unix>
- Schaub, F., & Walch, M. (2013). Exploring the Design Space of Graphical Passwords on Smartphones. *Symposium on Usable Privacy and Security (SOUPS) 2013*.
- Schlegel, R. (2011). Eyeing your Exposure: Quantifying and Controlling. *SOUPS '11 Proceedings of the Seventh Symposium on Usable Privacy and Security*.
- Shneiderman, B., Plaisant, C., Cohen, M., & Jacobs, S. (2009). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Addison-Wesley.
- Sourcefire. (2000). *Open source network intrusion prevention and detection system (IDS/IPS)*. Obtenido de <http://www.snort.org>
- Spool, J. (2003). *Design Patterns: An Evolutionary Step to Managing Complex Sites*. Obtenido de [http://www.uie.com/articles/design\\_patterns/](http://www.uie.com/articles/design_patterns/)
- Stobert, E., & Biddle, R. (2013). Memory Retrieval and Graphical Passwords. *Symposium on Usable Privacy and Security (SOUPS) 2013*.
- Suárez-Torrente, C. (2011). SIRIUS: Sistema de Evaluación de la Usabilidad Web Orientado al Usuario. Oviedo, España.
- Systems, C. (2001). *Network Security Policy: Best Practices*. Obtenido de [http://www.cisco.com/en/US/tech/tk869/tk769/technologies\\_white\\_paper09186a008014f945.shtml](http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f945.shtml)
- Tanenbaum, A. (2010). *Computer Networks*. Prentice Hall.

- Technology, N. I. (2000). *An Introduction to Computer Security: The NIST Handbook*. Obtenido de <http://csrc.nist.gov/publications/nistpubs/800-12/>
- Tipton, H. F., & Micki, K. (2007). *Information Security Management Handbook*. Auerbach Publications.
- Todd, E., Kemp, E., & Phillips, C. (2004). What makes a good user interface pattern language? *Proceedings of the fifth conference on Australasian user interface*.
- Unión, C. d. (2010). *Ley federal de protección de datos personales en posesión de los particulares*. Recuperado el 2013, de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- Van den Berg, S. (2000). *Welcome to procmail.org*. Obtenido de <http://www.procmail.org/>
- Van-Welie, M. (2001). *Patrones de Diseño de Interacción*. Universidad de Amsterdam Facultad de informática. Obtenido de <http://www.welie.com>
- Varela Tabuyo, R. (2005). *Patrones de Diseño Web e Interacción*. Obtenido de <http://galinus.com/>
- Velasco-Santos, P., Laureano-Cruces, A., Mora-Torres, M., & Herrera-Bautista, M. (2011). Diseño de agentes pedagógicos a partir de los estilos de aprendizaje; una perspectiva a través del color. *IV congreso mundial de estilos de aprendizaje ISBN 978-607-7533-66-5*.
- Velasco-Santos, P., Sánchez-Guerrero, L., & Laureano-Cruces, A. (2009). Un diseño de interfaz: tomando en cuenta los estilos de aprendizaje. *Memorias XXII Congreso Nacional y VIII Congreso Internacional de Informática y Computación de la ANIEI*.
- Vélez, O., Solano, D., Zúñiga, L., Argüello, M., Aguado, J., Aldana, J., y otros. (2005). Los estilos cognitivos y el aprendizaje maquinal den el diseño de interfaces inteligentes adaptativas. Universidad del Sinú. Centro de Investigaciones y Desarrollo. *Informática. Universidad de Manizales*.
- Welie, M., Veer, G., & Eliëns, A. (2000). Patterns as Tools for User Interface Design. *International Workshop on Tools for Working with Guidelines*.
- Wiedenbeck, S., & Birget, J.-C. (2005). Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice . *Symposium On Usable Privacy and Security. SOUPS 2005*.
- Winkler, D. (2012). *PAESSLER. The network monitoring company*. Obtenido de <http://www.paessler.com/blog/2012/08/23/news/ease-of-use>
- Woodward, B. (1998). Evaluation methods in usability Testing. *IEEE software*, 94-95.
- Yoshioka, N., Washizaki, H., & Maruyama, K. (2008). A survey on security patterns. *Progress in Informatics*, 35-47.

## **Apéndices**

Se anexan las publicaciones resultantes de este  
trabajo de investigación.

## **Appendix A. Doctoral Consortium**

**Patrones de interacción y su aplicación a la administración de la privacidad en Internet.**

Memorias IV Congreso Mexicano de Interacción Humano Computadora. Vol. II. México D.F. 2012. México City, México. Pp 45,46,47. ISBN: 978-607-477-875-5.

### **Objetivo:**

Presentar la propuesta doctoral ante un comité formado por expertos en el área de Interacción Humano-Computadora para recibir retroalimentación, delimitar alcances y analizar tópicos que no habían sido considerados para mejorar la argumentación del proceso de investigación para comprobar la hipótesis planteada.

En este documento se presenta el objetivo, la situación actual del proyecto y los resultados esperados.

# Patrones de interacción y su aplicación a la administración de la privacidad en Internet

Murillo, Sandra R.,

Universidad Popular Autónoma del Estado  
de Puebla  
Facultad de Tecnologías de Información  
sandrarocio.murillo@upaep.mx

Sánchez, J. Alfredo

Universidad de las Américas Puebla  
j.alfredo.sanchez@gmail.com

## ABSTRACT

A pesar de los esfuerzos tecnológicos que se han implementado para que los usuarios de Internet puedan navegar manteniendo el control de la privacidad de su información, los resultados no son los esperados. La poca cultura de seguridad informática y la inconsistencia de interfaces preventivas o correctivas entre las aplicaciones más comunes crean confusión en las personas y genera incertidumbre sobre el uso de su información por terceros. Algunos investigadores han sugerido la aplicación de estilos de aprendizaje para generar interfaces que faciliten la ergonomía cognitiva de los usuarios. Este proyecto explora la viabilidad de facilitar la administración de la privacidad de la información de usuarios en Internet basándose en un conjunto de patrones de interacción para la construcción de interfaces sustentados en perfiles de aprendizaje.

## TÉRMINOS GENERALES

Factores Humanos, Seguridad.

## INTRODUCCION

El concepto del control individual de la información personal constituye uno de los tópicos centrales de la privacidad [7]. En ocasiones los usuarios involucran información sensible sin tener conciencia de ello al navegar en Internet. Ante los diversos problemas que han surgido como el robo de identidad, fraudes y extorsiones, entre otros, organismos de reconocimiento internacional han propuesto mecanismos para que los desarrolladores de software incluyan opciones que fortalezcan la privacidad de la información del usuario. El software desarrollado bajo estrictas metodologías para cubrir con los requerimientos de seguridad de la información del usuario va en aumento. En la parte técnica ha sido posible detectar las áreas de

oportunidad y ofrecer soluciones [3]. Sin embargo, el bajo índice de cultura de seguridad informática [1], así como diseños poco adecuados, hacen que el usuario promedio no aproveche las soluciones ofrecidas en interfaces con las que interactúa [4].

Muchos de estos sistemas ofrecen opciones de manejo de privacidad en un lenguaje técnico o legal poco claro para un usuario. Algunas personas, por curiosidad o necesidad, invierten tiempo en comprender los conceptos para fortalecer sus medidas de prevención o solución de un problema de este tipo. Sin embargo, cada software maneja los términos y simbología de forma distinta, lo que causa frustración y rechazo ante estos temas. En un trabajo publicado en 2011 [6] se sugiere que hacer explícitos los riesgos de privacidad en una aplicación Web puede ayudar a los usuarios a tomar mejores decisiones con respecto a este tema. Esto, sin embargo, para cierto tipo de usuarios podría desalentar el uso de dichas aplicaciones pues tienen un diseño estático

A la luz de la neurofisiología y psicología, se han propuesto modelos de rasgos cognitivos, afectivos y fisiológicos que sirven como indicadores de cómo las personas perciben interacciones y responden a sus ambientes de aprendizaje [2,10]. Se les denomina estilos de aprendizaje y han contribuido al proceso educativo en los últimos años [7]. Algunos proyectos de investigación han sugerido su aplicación para generar interfaces que faciliten la ergonomía cognitiva de los usuarios [9,11]. Hasta el momento no existe evidencia de la aplicación de estilos de aprendizaje para la construcción de interfaces que faciliten el manejo de la privacidad de la información de los usuarios de Internet.

## EL PROBLEMA

El número de usuarios de internet a nivel nacional va en aumento y se espera que esta tendencia continúe. En un estudio reciente con usuarios de Internet mayores de edad, se observa que a nivel nacional el 13% de los internautas mayores de edad consideran que es responsabilidad de los titulares de la información el debido tratamiento de los datos personales. El 31% no pudieron definir lo que es un dato personal. Sólo el 11% de los evaluados no saben que el Derecho a la privacidad es un Derecho Constitucional. El 19% leen siempre el aviso de privacidad de un sitio, y de esta población al 62% les toma más de 4 minutos leerlas. El 61% de los internautas no saben qué tratamiento le darán a sus datos personales en las redes sociales en las que se encuentran inscritos [1]

Estos datos revelan lo siguiente:

4. El creciente número de usuarios en internet carece de cultura de seguridad informática en el ámbito de la privacidad de datos.
5. Los usuarios disponen de interfaces que facilitan su interacción con Internet, pero no incluyen mecanismos intrínsecos de alertas sobre riesgos relativos a la privacidad de datos.
6. Los internautas mayores de edad desconocen o no aplican medidas de seguridad en el tema

## OBJETIVO GENERAL

El objetivo de este trabajo consiste en generar un conjunto de patrones de interacción sustentado en estilos de aprendizaje para la construcción de interfaces humano-computadora que mejoren la administración de la privacidad de los usuarios en Internet.

## OBJETIVOS ESPECIFICOS

4. Establecer una relación entre la administración de la privacidad de los usuarios de Internet y estilos de aprendizaje de los usuarios
5. Crear un conjunto de patrones para el diseño de interfaces específico a cada estilo de aprendizaje
6. Definir los tópicos emergentes de privacidad de información en la Web para una población determinada.
7. Aplicar el conjunto de patrones a interfaces de usuario para navegación en la Web en un grupo de prueba.

8. Hacer disponibles públicamente los patrones de interacción junto con recomendaciones para su uso y aplicación a la administración de la privacidad.

## SITUACIÓN ACTUAL DEL PROYECTO

Se está realizando un estudio estadístico con usuarios cotidianos de Internet seleccionados al azar para identificar la relación actual de factores (técnicos y humanos) involucrados en el uso de Internet y la privacidad de su información (ver Tabla 1 y Tabla 2)

| Que el usuario pueda definir:                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Dato personal</li> <li>• Niveles de Seguridad</li> <li>• Sellos de confianza</li> <li>• Consecuencias de compartir datos personales</li> <li>• Tipos de navegador</li> <li>• Dispositivos de acceso</li> </ul> |

**Tabla 1. Factores técnicos involucrados en el uso de Internet y la privacidad de información**

| Preferencias de los usuarios respecto a:                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Idioma</li> <li>• Imágenes</li> <li>• Textos</li> <li>• Audios</li> <li>• Opinión de amigos/familiares</li> <li>• Estilo de aprendizaje</li> <li>• Personalización de interfaces</li> <li>• Capacitación</li> <li>• Responsabilidad de los actores</li> </ul> |

**Tabla 2. Factores humanos involucrados en el uso de Internet y la privacidad de información**

Se está aplicando una encuesta de siete puntos en Escala Likert donde los usuarios pueden expresar su experiencia actual sobre su interacción con Internet y la privacidad de su información. Se espera validar este instrumento mediante un Alpha de Cronbach [8] para su análisis estadístico.

## RESULTADOS ESPERADOS

Este proyecto se presenta como proyecto de tesis de Sandra Rocío Murillo Cano para obtener el grado en el Doctorado en Tecnologías de Información y Análisis de Decisiones en la Universidad Popular Autónoma del Estado de Puebla, siendo el asesor del proyecto el Dr. Alfredo Sánchez Huitrón.

A la fecha dos alumnos de la Facultad de Tecnologías de Información de la carrera de Ingeniería en Computación y Sistemas (UPAEP) están realizando sus respectivas tesis en la implementación de soluciones de privacidad de información. Se espera culminen para Agosto 2013.

Al finalizar este proyecto se espera contar con un conjunto de patrones para el diseño de interfaces basado en perfiles de aprendizaje.

Se pretende construir y probar un prototipo para medir la interacción de los usuarios de Internet con interfaces creadas de acuerdo a su perfil de aprendizaje y reportar los resultados obtenidos en el manejo de la privacidad de información.

## REFERENCIAS

- [1] Asociación Mexicana de Internet AMIPCI. Estudio de Protección de Datos personales entre usuarios y empresas.  
<http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=95&Type=1>
- [2] CHAEA. Cuestionario Honey Alonso de Estilos de aprendizaje.  
<http://www.estilosdeaprendizaje.es>
- [3] Lorrie Cranor, M. L.-M. (*The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*).  
<http://www.w3.org/TR/P3P/>
- [4] Garfinkel, L. F. (*Security and Usability. Designing Secure Systems That People Can Use*. O'Reilly (2005)
- [5] Hannaford, C. *Cómo aprende tu cerebro*. PAX. (2011)
- [6] Jennifer King, A. L. Privacy: Is there an app for that? *Symposium On Usable Privacy and Security. SOUP 2011*. (2011).
- [7] Lindskog, H. *Web Site Privacy with P3P*. Wiley (2003)
- [8] Malhortra, Naresh K. *Investigación de Mercados*. Pearson Prentice Hall. 5ª. Edición. (2008)
- [9] Perla Velasco-Santos, A. L.-C.-T. *Diseño de agentes pedagógicos a partir de los estilos de aprendizaje; una perspectiva a través del color*. Memorias del IV congreso mundial de estilos de aprendizaje. ISBN 978-607-7533-66-5. (2010)
- [10] Secretaría de Educación Pública. *Manual de estilos de aprendizaje*. [http://www.dgb.sep.gob.mx/informacion\\_academica/actividadesparaescolares/multimedia/Manual.pdf](http://www.dgb.sep.gob.mx/informacion_academica/actividadesparaescolares/multimedia/Manual.pdf)
- [11] Velez Oswaldo, Solano Darling, Zúñiga Lina, Argüello Mery, Aguado Jorge, Aldana José, Pabel López, Alarcón Edgar . *Los estilos cognitivos y el aprendizaje maquinal den el diseño de interfaces inteligentes adaptativas*. Universidad del Sinú. Centro de Investigaciones y Desarrollo. (2005)

## **Appendix B. Patrones de interacción y su aplicación a la privacidad en Internet**

Segundo Congreso Internacional de Ingeniería de Sistemas INCOSE – México 2013.

ISBN: 978-607-8093-27-4

### **Objetivo:**

Determinar la utilidad de una colección de patrones de interacción para facilitar la percepción y manipulación de interfaces relativas a la privacidad de datos personales.

En este documento se define el concepto de patrón de interacción, el metapatrón sugerido para esta investigación y se presentan los resultados de evaluación de una colección de patrones por parte de 10 participantes (5 del área de ingeniería en computación y 5 del área de diseño gráfico)

# Patrones de interacción y su aplicación a la privacidad en Internet

Sandra. R. Murillo<sup>1</sup>, J. Alfredo Sánchez<sup>2</sup>

<sup>1</sup>Universidad Popular Autónoma del Estado de Puebla,  
Puebla, Puebla 72410, México

<sup>2</sup>Universidad de las Américas Puebla,  
Cholula, Puebla 72810, México

sandrarocio.murillo@upaep.mx  
j.alfredo.sanchez@gmail.com

**Resumen.** La inconsistencia de interfaces preventivas o correctivas entre las aplicaciones más comunes crea confusión en las personas y genera incertidumbre sobre el uso de su información por terceros. En las últimas décadas se han creado patrones de seguridad para facilitar la construcción de interfaces que involucran temas de privacidad de información pues el acceso a Internet se incrementa día con día y las necesidades de los usuarios superan las normas establecidas en un momento dado. Los usuarios aceptan o rechazan aplicaciones basados en la percepción que tengan de ella, sin embargo, la seguridad de un sistema se trata como un requerimiento no funcional de una aplicación y eso genera horas extras de codificación y frustración en el usuario. Este trabajo presenta una colección de patrones de interacción para facilitar la construcción de aplicaciones que involucren temas de privacidad de datos personales. A través de un estudio multidisciplinario se valida la pertinencia de dicha colección.

**Términos Generales:** Factores Humanos, Usabilidad, Seguridad.

## 1 Introducción

Una apropiada arquitectura de seguridad es parte esencial para implementar una aplicación robusta y confiable. Disponer de un conjunto de soluciones a un problema recurrente en contextos similares con algunas variantes en su implementación puede facilitar el proceso de desarrollo de software y mejorar la experiencia de usuario en una aplicación. El campo de investigación relativo a patrones de seguridad y técnicas para su uso en las distintas fases de desarrollo de software ofrece diversas áreas de oportunidad debido a la constante evolución de las aplicaciones informáticas. Existen conjuntos de buenas prácticas para profesionales de la seguridad, sin embargo, aún existe una brecha entre los expertos de esta área y los diseñadores de interfaces. Se reconocen destacadas colecciones de patrones de interacción que abordan distintos temas, algunas de ellas incluyen temas relativos a seguridad informática. Existen leyes internacionales aplicadas en algunos países que exigen mostrar en lenguaje legal los términos y condiciones del uso de la información almacenada por un tercero, sin embargo, no existe un formato universal para presentar estos datos ni los riesgos asociados para los titulares de la información. Este trabajo está organizado de la siguiente manera: La Sección 2 presenta temas principales en el ámbito de patrones de interacción. El problema principal es definido en la Sección 3, mientras que en la Sección 4 se describe la metodología seguida para este estudio. Los resultados iniciales son presentados en la Sección 5 y discutidos en la Sección 6. Finalmente, la Sección 7 presenta las conclusiones derivadas del estudio.

## 2 Patrones de Interacción

Un patrón es un medio de comunicación que expresa una solución de interfaz en una forma textual y gráfica a un problema recurrente dentro de un contexto específico. Su especificación permite comunicar la experiencia y el conocimiento en un área específica [1,2]. Un patrón de interacción describe una solución exitosa a un problema recurrente relativo a la interfaz de usuario en un contexto dado [3]. Sirve para describir relaciones visuales, estéticas y de satisfacción al mismo tiempo que define un problema, su contexto y

solución. Esto facilita la comunicación entre miembros de distintas disciplinas permitiendo registrar el conocimiento y la experiencia para construir prototipos de interfaz de usuario [4,5,6].

Los lenguajes de patrones son representaciones que han sido usadas en diseño urbano y arquitectura desde los 70's para representar de una forma generalizada la interacción entre formas físicas y la conducta social [7]. Un lenguaje de patrones de interacción genera un diseño de interacción espacio/tiempo que representa un modelo mental de las tareas de usuario con el objetivo de construir una interfaz humano-computadora (IHC) lo más transparente posible. La definición intencionalmente no se expresa para describir lo que es un solo patrón de interacción, pues la vinculación entre los patrones se considera tan importante como los propios patrones individuales.

El objetivo de un lenguaje de patrones de interacción consiste en compartir soluciones de diseño IHC exitoso entre los profesionales de IHC y para proporcionar un lenguaje común para el diseño de IHC para cualquier persona involucrada en el diseño, desarrollo, evaluación, o el uso de sistemas interactivos. J. Borchers [2] propone una estructura de patrón haciendo uso de un metapatrón, esto es, un patrón que permite describir patrones. En este metapatrón se definen los componentes requeridos en cualquier dominio de conocimiento. No es necesario describir cada uno de los componentes para todos los patrones, salvo aquellos que son obligatorios: nombre, problema, solución y contexto. Esta estructura se presenta en la Tabla 1.

**Tabla 1** Estructura de los patrones de interacción

| Componente            | Descripción                                                                                                                                                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre                | Comunica la idea central del patrón.                                                                                                                         |
| Autor                 | Indica el nombre del creador del patrón.                                                                                                                     |
| Clasificación         | Indica el tipo de patrón.                                                                                                                                    |
| Rango                 | Indica la calificación del patrón.                                                                                                                           |
| Problema              | Describe la interacción desde el punto de vista del usuario                                                                                                  |
| Solución              | Describe la solución del problema en forma descriptiva y gráfica                                                                                             |
| Contexto              | Presenta las condiciones bajo las cuales se usa este patrón                                                                                                  |
| Fuerzas               | Señala los conflictos que pueden restringir la solución                                                                                                      |
| Usabilidad            | Describe el impacto del uso del patrón para el usuario.                                                                                                      |
| Consecuencias         | Describe el resultado de aplicar el patrón.                                                                                                                  |
| Ejemplos              | Muestra ejemplos de la solución propuesta.                                                                                                                   |
| Patrones relacionados | Enumera otros patrones relacionados con este patrón (cuando un patrón referencia a otro significa que requiere de su descripción para completar la solución) |

Asimismo, J. Borchers propone una taxonomía que distingue tres dimensiones principales en las que se pueden clasificar los patrones de interacción:

1. Nivel de abstracción (objeto, estilo, tarea)
2. Función
  - a. Percepción (interfaz de salida)
  - b. Manipulación (interfaz de entrada)
  - c. Navegación
3. Dimensión física (espacio, secuencia, tiempo)

Yoder y Baraclow [8] introdujeron en 1997 el concepto de patrones a la comunidad de seguridad informática. Desde entonces, diversos trabajos han sido presentados en el área de patrones de seguridad que han solucionado distintos problemas [9,10,11]. Sin embargo, día con día las necesidades son diversas y se requieren de nuevas propuestas. Por su parte, Schümmer [12] introduce un conjunto de patrones que pueden ser agrupados en dos categorías: patrones que bloquean información personal para ser transferida a otra entidad y patrones que filtran información enviada al usuario por un tercero.

### 3 El problema

Desde el 2008, el proyecto de investigación PrimeLife [13] ha sido desarrollado para crear una colección de patrones de IHC con el objetivo de proporcionar directrices sobre cómo diseñar interfaces de usuario usables para la mejora de la privacidad en los sistemas y aplicaciones. Estas propuestas se estructuran en patrones relacionados con la privacidad, políticas de gestión, visualización de privacidad de información y flujos de trabajo, paradigmas de interacción, así como descripciones de maquetas interactivas de PET (Privacy Enhancing Technologies). En el nombre de cada patrón se incluye una calificación de 0 a 5 estrellas ( 0: No hay ninguna prueba de usuario final, 5: Ha sido probado de manera exhaustiva y se considera una versión final ) para reflejar la cantidad de experiencia que se tiene de cada patrón. Sin embargo, estos patrones están desarrollados bajo un contexto de términos legales europeos y no existe evidencia de su implementación y uso en entornos latinoamericanos. Es relevante la propuesta de los patrones *Privacy Policy Display* y *Dynamic Privacy Policy Display*, cuyos modelos sugieren la representación mínima de un Aviso de Privacidad. Sin embargo ninguno de los dos propone un esquema para representarlo de forma extendida [13]. Disponer de una colección de patrones de interacción para el diseño de la retroalimentación visual podría contribuir a que el usuario tenga un mayor control sobre su de seguridad [14]. Hoy en día no existe una colección de patrones que apoye la construcción de interfaces relativas a la privacidad de usuario.

#### 3.1 Objetivo

El objetivo de este estudio consiste en mostrar y determinar la utilidad de una colección de patrones de interacción para facilitar la percepción y manipulación de interfaces relativas a la privacidad de datos de usuario.

#### 3.2 Objetivos específicos

1. Identificar si el metapatrón representa un modelo de solución para un grupo multidisciplinario de desarrollo de aplicaciones.
2. Medir la colección ante dos perfiles multidisciplinarios involucrados en el diseño de interfaces y presentar los resultados.

### 4 Método

Se cuenta con diez voluntarios para participar en este proyecto:

- Cinco de ellos son del área de Ingeniería en Computación. (2 profesores, 1 exalumno, 2 alumnos)
- Cinco alumnos de Diseño Gráfico.

De manera individual, sin tener contacto con los otros participantes durante el experimento, se pide que asuman el rol de pertenecer a un equipo de desarrollo de software. Tienen a su disposición la colección de patrones COPPEMA y se les pide que evalúen la utilidad de cada patrón conforme a una escala definida.

#### 4.1 COPPEMA

COPPEMA es una **CO**lección de **PA**trones de interacción para facilitar la **PE**rcepción (interface input) y **MA**nipulación (interface output) de interfaces relativas a la privacidad de datos de usuario. Esta colección se sustenta en la revisión del Estado del Arte sobre privacidad de información e interfaces de usuario, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) [14] y las relaciones entre la privacidad de datos personales e interfaz de usuario [15]. El metapatrón utilizado para esta colección se describe en la Tabla 2.

COPPEMA está compuesta por dos grupos principales de patrones: Tareas y Elementos complementarios. (Ver Fig. 1). Las Tareas son patrones de interacción definidos para representar tareas que involucran la privacidad del usuario en un sitio web. Estas tareas se relacionan con los elementos requeridos en un Aviso de

Privacidad extendido [14]. Los elementos complementarios son patrones de interacción definidos para representar elementos auxiliares en tareas que involucran la privacidad del usuario en un sitio web. Cada grupo se divide a su vez en Patrones informativos y Patrones interactivos. Los patrones informativos tienen una naturaleza de comunicar una idea y no tienen asociada una retroalimentación adicional. Los patrones interactivos tienen asociada una tarea adicional y se espera una respuesta del usuario.

## 4.2 Condiciones del estudio

Se presenta a los participantes el metapatrón de la colección para identificar sus elementos y se les pide que lo califiquen en una escala del 1 al 10 si consideran que tiene los elementos necesarios para representar el modelo mental del objeto a representar. Posteriormente se les pide que tomen el tiempo necesario para leer y comprender cada elemento de la colección. A cada persona se le pide que se considere parte de un equipo de desarrollo responsable de diseñar e implementar hipotéticamente cuatro aplicaciones con base a su perfil de desarrollo (computación o diseño gráfico). Desde su perspectiva debe calificar del 1 al 10 la utilidad de cada patrón de interacción.

Las cuatro aplicaciones hipotéticas son:

- Interface de captura de datos personales.
- Interface de despliegue de datos personales.
- Construcción de un Aviso de Privacidad.
- Administración de “Settings” en una cuenta de usuario.

**Tabla 2.** Metapatrón utilizado en COPPEMA

| Componente                   | Descripción                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Nombre</b>                | Comunica la idea central del patrón                                                           |
| <b>Problema</b>              | Describe la interacción desde el punto de vista del usuario                                   |
| <b>Solución</b>              | Describe la solución del problema en forma descriptiva y gráfica                              |
| <b>Contexto</b>              | Presenta las condiciones bajo las cuales se usa este patrón                                   |
| <b>Usabilidad</b>            | Describe el impacto del uso del patrón para el usuario                                        |
| <b>Consecuencias</b>         | Describe el resultado de aplicar el patrón                                                    |
| <b>Patrones relacionados</b> | Enumera otros patrones relacionados con este patrón                                           |
| <b>Ejemplo(s)</b>            | Muestra en forma simple los campos de datos requeridos para la representación del componente. |

| Tareas                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1) Patrones Informativos <ul style="list-style-type: none"> <li>a) Cambios y/o actualización del Aviso de Privacidad</li> <li>b) Uso de tecnologías para recolección de información</li> <li>c) Previsiones especiales grupos vulnerables</li> </ul>                                                                                                  |
| 2) Patrones Interactivos <ul style="list-style-type: none"> <li>a) Finalidad del tratamiento de los datos personales</li> <li>b) Limitar uso y/o divulgación de datos personales</li> <li>c) Ejercer derechos ARCO</li> <li>d) Transferencias de datos personales</li> <li>e) Revocar consentimiento al tratamiento de datos personales</li> </ul>    |
| Elementos complementarios                                                                                                                                                                                                                                                                                                                             |
| 1) Patrones Informativos <ul style="list-style-type: none"> <li>a) Datos personales</li> <li>b) Datos personales sensibles</li> <li>c) Responsable de albergar datos personales</li> <li>d) Información sobre organismo regulador</li> <li>e) Consecuencias del uso de datos personales</li> <li>f) Prevención del uso de datos personales</li> </ul> |
| 2) Patrones Dinámicos <ul style="list-style-type: none"> <li>a) Consentimiento expreso</li> <li>b) Localización del aviso de privacidad integral</li> </ul>                                                                                                                                                                                           |

**Fig. 1** Colección COPPEMA

Se aplicó una encuesta para que los participantes calificaran la utilidad de cada patrón para la construcción hipotética de las cuatro aplicaciones. Cada patrón se califica en una escala de 1 a 10, (donde 1 significa “nada” útil y 10 significa “extremadamente útil”). Se validó la confiabilidad del instrumento al obtener un valor de 0.875 en la variable Alfa de Cronbach [16] (Ver Fig. 2).

#### 4.3 Pregunta del estudio

¿Qué relevancia tiene para los miembros de un equipo multidisciplinario de desarrollo de software contar con una colección de patrones de interacción para diseñar interfaces que involucren tópicos de privacidad de usuario final?

| Resumen del procesamiento de los casos |                        |    |       | Estadísticos de fiabilidad |                |
|----------------------------------------|------------------------|----|-------|----------------------------|----------------|
|                                        |                        | N  | %     | Alfa de Cronbach           | N de elementos |
| Casos                                  | Válidos                | 10 | 100.0 | .875                       | 16             |
|                                        | Excluidos <sup>a</sup> | 0  | .0    |                            |                |
|                                        | Total                  | 10 | 100.0 |                            |                |

a. Eliminación por lista basada en todas las variables del procedimiento.

**Fig. 2** Confiabilidad del instrumento

#### 4.4 Variables de estudio

Los valores involucrados se obtienen mediante la media, máximos y mínimos en las calificaciones asignadas por los participantes obtenidos por el programa SPSS [16].

- Utilidad del metapatrón para representar un patrón de interacción en un contexto dado.
- Utilidad de cada patrón de la colección para el diseñar y construir interfaces que involucren la privacidad del usuario.
- Utilidad general de COPEMMA para el diseño y construcción de interfaces que involucren la privacidad del usuario.

### 5 Resultados

Las calificaciones asignadas al metapatrón son las siguientes:

- El metapatrón obtiene una media de 8.4 (Ver tabla 3)
- El metapatrón obtiene una media de 8.8 considerando solo la opinión de los Ingenieros en Computación (Ver tabla 3)
- El metapatrón obtiene una media de 8.0 considerando solo la opinión de los Diseñadores Gráficos (Ver tabla 3)

Las calificaciones asignadas a COPPEMA se muestran a continuación:

- COPEMMA obtiene una media de 8.3 (Ver tabla 4)
- COPEMMA obtiene una media de 8.0 considerando solo la opinión de los Diseñadores Gráficos (Ver tabla 4)
- COPEMMA obtiene una media de 8.6 considerando solo la opinión de los Ingenieros en Computación (Ver tabla 4)
- El 50% de toda la población asigna una calificación general de 8.0 (Ver tabla 5)
- El 40% de toda la población asigna una calificación general de 9.0 (Ver tabla 5)

- El 10% de toda la población asigna una calificación general de 7.0 (Ver tabla 5)
- La calificación general mínima asignada por los Diseñadores Gráficos es de 7.0 y la máxima es de 9.0 (Ver tabla 4)
- La calificación general mínima asignada por los Ingenieros en Computación es de 8.0 y la máxima es de 9.0 (Ver tabla 4)
- La calificación promedio más baja asignada a un patrón es de 8.3250 (Ver tabla 6)
- La calificación promedio más alta asignada a un patrón Es de 9.4250 (Ver tabla 6)
- Solo un patrón fue asignado con una calificación mínima de 6.0 (Ver tabla 6)

Observaciones generales por parte de los participantes de Ingeniería en Computación:

- Muestran interés inherente para diseñar y codificar estructuras de datos para cada patrón.
- Muestran interés inherente para diseñar y codificar bases de datos que representen el lenguaje de patrones.

Observaciones generales por parte de los participantes de Diseño Gráfico:

- Muestran interés inherente por aplicar teorías de diseño para representar los ejemplos mostrados en cada patrón.
- Muestran interés inherente por representar los ejemplos mostrados en cada patrón en una interface web.

**Tabla 3** Calificaciones Generales del metapatrón

| Diseñadores Gráficos |         |        | Ingenieros en Computación |         |        | Toda la población |         |        |
|----------------------|---------|--------|---------------------------|---------|--------|-------------------|---------|--------|
| N                    | Valid   | 5      | N                         | Valid   | 5      | N                 | Valid   | 10     |
|                      | Missing | 0      |                           | Missing | 0      |                   | Missing | 0      |
| Mean                 |         | 8.0000 | Mean                      |         | 8.8000 | Mean              |         | 8.4000 |
| Minimum              |         | 7.00   | Minimum                   |         | 8.00   | Minimum           |         | 7.00   |
| Maximum              |         | 9.00   | Maximum                   |         | 10.00  | Maximum           |         | 10.00  |

**Tabla 4** Estadística descriptiva calificaciones generales

| Calificación                 | N  | Minimum | Maximum | Mean  | Std. Deviation |
|------------------------------|----|---------|---------|-------|----------------|
| Diseñadores Gráficos         | 5  | 7.00    | 9.00    | 8.000 | 0.70711        |
| Ing. en Computación          | 5  | 8.00    | 9.00    | 8.600 | 0.54772        |
| Calificación General COPPEMA | 10 | 7.00    | 9.00    | 8.300 | 0.67495        |

**Tabla 5** Calificación General COPPEMA

|       |       | Frequency | Percent |
|-------|-------|-----------|---------|
| Valid | 7.00  | 1         | 10.0    |
|       | 8.00  | 5         | 50.0    |
|       | 9.00  | 4         | 40.0    |
|       | Total | 10        | 100.0   |

## 6 Discusión

Este estudio fue dirigido a estudiantes y maestros de las áreas de Ingeniería en Computación y Diseño gráfico. Estas características suponen experiencia en la construcción de aplicaciones de software a nivel general desde cada disciplina. Para el caso de los alumnos de Diseño gráfico, como requisito debían tener experiencia básica en el diseño de interfaces. En futuros estudios se podría incluir a egresados de estas

carreras que estén inmersos en el campo laboral. La colección de patrones fue manipulada en papel, sin embargo se podría contar con versiones digitales para futuros casos.

**Tabla 6** Estadística descriptiva calificaciones individuales

| Patrones                                                   | N  | Minimum | Maximum | Mean  | Std. Deviation |
|------------------------------------------------------------|----|---------|---------|-------|----------------|
| Datos personales                                           | 10 | 7.00    | 9.75    | 8.700 | .85635         |
| Datos personales sensibles                                 | 10 | 8.00    | 10.00   | 9.225 | .68160         |
| Responsable de albergar datos personales                   | 10 | 7.00    | 9.25    | 8.650 | .69921         |
| Consentimiento Expreso                                     | 10 | 7.75    | 10.00   | 8.875 | .77504         |
| Información para localizar el aviso de privacidad integral | 10 | 8.00    | 9.25    | 8.850 | .50277         |
| Información sobre el Organismo Regulador                   | 10 | 7.25    | 9.50    | 8.950 | .66458         |
| Consecuencias del uso de datos personales                  | 10 | 6.00    | 9.75    | 8.600 | 1.23153        |
| Prevención del uso de datos personales                     | 10 | 7.25    | 10.00   | 9.125 | .75691         |
| Finalidad del tratamiento                                  | 10 | 8.00    | 10.00   | 9.425 | .65670         |
| Limitar uso/divulgación datos personales                   | 10 | 7.00    | 9.00    | 8.325 | .62417         |
| Ejercer derechos ARCO                                      | 10 | 7.50    | 9.50    | 8.850 | .66875         |
| Transferencias de datos personales                         | 10 | 7.25    | 9.50    | 8.725 | .72121         |
| Cambios y/o actualización en el aviso de privacidad        | 10 | 8.00    | 9.75    | 8.875 | .64818         |
| Revocar consentimiento al tratamiento de datos personales  | 10 | 7.00    | 10.00   | 9.050 | 1.01926        |
| Uso de tecnologías para recolección de información         | 10 | 8.00    | 10.00   | 9.075 | .67752         |
| Previsión especial grupos vulnerables                      | 10 | 8.00    | 10.00   | 9.175 | .69771         |

La estructura propuesta para el Metapatrón fue acogida en un sentido positivo por los dos perfiles de participantes. Esto demuestra que es una estructura objetiva para representar una solución a un problema recurrente relativo a la interfaz. (Ver Tabla 3)

Los promedios generales obtenidos (Ver Tabla 4 y Tabla 5) y las calificaciones asignadas de manera individual a cada patrón (Ver Tabla 6) indican un grado de aceptación positivo entre los miembros de un equipo multidisciplinario de desarrollo de interfaces con temas de privacidad de datos.

Los patrones actuales podrían incluir ejemplos propuestos por el área de diseño gráfico y evaluar su impacto en aplicaciones utilizadas por distintos grupos de usuarios.

## 7 Conclusiones

El presente trabajo demuestra que los patrones de interacción representan una alternativa significativa para diseño de interfaces relativas a la de seguridad informática. Sería deseable contar con colecciones de patrones que relacionen los factores críticos de privacidad con tópicos de diseño gráfico de interfaz para diferentes tipos de usuarios. Aplicar los rasgos distintivos de interacción humano-computadora podría beneficiar a los usuarios para mejorar su privacidad y a los desarrolladores para contar con un marco de referencia que mejore la experiencia de usuario y la usabilidad de un sistema. Estos trabajos podrían contribuir a la creación de modelos de aplicación de un lenguaje de patrones de interacción para la construcción de interfaces relativas a la privacidad del usuario.

## Referencias

- 1 Gamma, E., Helm, R., Ralph, J., & Vlissides, J. (1995). *Design Patterns*. Addison-Wesley.
- 2 Borchers, J. (2001). *A pattern approach to interaction design*. England: Wiley.
- 3 Hernandez-Hernandez, M. E., Alvarez-Carrion, G., & Muñoz-Arteaga, J. (s.f.). *Patrones de Interacción para el Diseño de Interfaces WEB usables*. Obtenido de <http://www.willydev.net/descargas/PatronInter.pdf>
- 4 Bayle, E. (1998). *Putting It All Together. Towards a Pattern Language for Interaction Design: ACHI 97 Workshop*. Obtenido de SIGCHI Bulletin: <http://dl.acm.org/citation.cfm?id=280580>

- 5 Van-Welie, M. (2001). *Patrones de Diseño de Interacción*. Universidad de Amsterdam Facultad de informática. Obtenido de <http://www.welie.com>
- 6 Acosta, A., & Zambrano, N. (2006). *Importancia, Problemas y Soluciones en el Diseño de la interfaz de Usuario*. Obtenido de <http://www.ciens.ucv.ve:8080/genasig/sites/topicosihc/archivos/Modelo-AcostaZambrano-Saber.pdf>
- 7 Bayle, E. (1998). *Putting It All Together. Towards a Pattern Language for Interaction Design: ACHI 97 Workshop*. Obtenido de SIGCHI <http://dl.acm.org/citation.cfm?id=280580>
- 8 Joseph, Y., & Baraclow, J. (1997). *Architectural Patterns for Enabling Application Security*.
- 9 Cranor, L., Romanowsky, S., Hong, J., Acquisti, A., & Friedman, B. (2006). *Privacy Patterns for Online Interactions*. Obtenido de <http://repository.cmu.edu/hcii/72>
- 10 Yoshioka, N., Washizaki, H., & Maruyama, K. (2008). A survey on security patterns. *Progress in Informatics*, 35-47.
- 11 Muñoz Arteaga, J., Medina Medina, A., Guerrero, J., & Muñoz Lopez, J. (s.f.). *Patrones de Interacción para el Diseño de la Retoalimentación Visual de Sitios Web Seguros*. Obtenido de <http://www.aipo.es/articulos/2/50.pdf>
- 12 Shümmer, T. (s.f.). *The Public Privacy - Patterns for Filtering Personal Information in Collaborative Systems*. CHI2004.
- 13 Programme, E. C. (2010). *PRIMELIFE . HCI Pattern Collection – Version 2*. Obtenido de [http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci\\_pattern\\_collection\\_v2-public.pdf](http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf)
- 14 Parlamentarios, C. d. (2010). *Ley federal de protección de datos personales en posesión de los particulares*. México.
- 15 Murillo, S., Sánchez, Alfredo. (2013). *Studying the relationships between the management of personal data privacy and the user interface*.
- 16 Malhortra, N. K. (2008). *Investigación de Mercados*. . Pearson Prentice Hall. 5ª. Edición.

## **Appendix C. Studying the relationships between the management of personal data privacy and user interface.**

6th Latin American Conference, CLIHC 2013, Carrillo, Costa Rica, December 2-6, 2013, Proceedings. Lecture Notes in Computer Science Series. Volume 8278. Series ISSN 0302-9743 Pages pp 79-89

### **Objetivo:**

Identificar los factores críticos de manejo de privacidad de datos personales y su relación con la interface de usuario y estilos de aprendizaje para su sugerir estrategias de diseño que mejoren la administración de la seguridad por parte de los usuarios.

Se realizó un análisis cuantitativo basado en un estudio de frecuencias y correlación de variables (Coeficiente de correlación de Pearson). Se sugiere que las correlaciones con valores muy altos son factores muy importantes a considerar en el diseño de una interface relativa a privacidad de datos. Se consideró una población de una universidad de 8157 estudiantes, haciendo una muestra de 275 personas, presentando un nivel de confianza del 95%.

# Studying the relationships between the management of personal data privacy and user interface

Sandra R. Murillo<sup>1</sup>, J.Alfredo Sánchez<sup>2</sup>

<sup>1</sup> Universidad Popular Autónoma del Estado de Puebla,  
Puebla, Puebla 72410, México

<sup>2</sup> Universidad de las Américas Puebla,  
Cholula, Puebla 72810, México

[sandrarocio.murillo@upaep.mx](mailto:sandrarocio.murillo@upaep.mx)

[j.alfredo.sanchez@gmail.com](mailto:j.alfredo.sanchez@gmail.com)

**Abstract.** Despite technological efforts that have been implemented so that users can navigate on the Internet with increased control of the privacy of their information, results are not always as expected. The lack of information security culture and the inconsistency of preventive or corrective interfaces among common applications create confusion in people and insecurity about the use of their information by third parties. Some researchers have suggested that the application of learning styles to build interfaces can facilitate users' cognitive ergonomics. This paper presents the current relationship between the management of personal data privacy, user interface and learning styles through an ethnographic study. These relationships suggest a model to navigate among these components and improve user experience.

**Keywords:** Human factors, usability, security.

## 1 Introduction

There are important factors to be considered by users to manage their privacy on the Internet. Most users usually move quickly through default settings when they install or use software without reading the details. Internet sites maintain records that indicate whether privacy notices were read and the terms and conditions of use of personal data were accepted. However, users in general are not aware of the consequences of the accepted terms. When any software has been used for a while, the risks associated with the information provided at the beginning or during usage are not evident. Users interact with applications on a daily basis without being certain of what can happen if a third party misuses the data they capture. Today, there is no universal format for presenting the elements of a website privacy notice and the associated risks for the owner of the information. There are international laws applied in some countries that require legal language to show how stored information can be handled by a third party. The interface is critical at all times to support user decisions on this issue. Some research papers have suggested the application of learning styles for building interfaces; however there is no evidence of their application in the management of the information privacy of Internet users. This paper reports initial findings on how learning styles and user interfaces are related with the way the privacy of personal information is managed. The paper is organized as follows: Section 2 discusses the main issues in the realm of information privacy on the Internet. The main problem is defined in Section 3, whereas Section 4 describes the methodology followed in our study. Our initial results are presented in Section 5 and discussed further in Section 6. Finally, Section 7 presents the conclusions derived from our study.

## 2 Internet privacy

The increasing use of diverse technologies has made it possible for personal user information to be used for purposes other than those originally intended. Sometimes personal data may be transferred to other entities without the owner's explicit consent. From the perspective of personal data protection, the owner of the data has the right and the freedom to decide what to communicate, when and to whom, maintaining control over their personal information at all times [1]. Due to problems that have arisen (identity theft, fraud, etc.), international organizations have proposed mechanisms for software developers to include options that strengthen user privacy. On the technical side it has been possible to detect and provide solutions [2]. However, the low level of information security culture and unsuitable interface designs cause the average user to remain unaware of the solutions available [3].

Some systems offer privacy options in legal language that is unclear to the average user. Some people, by curiosity or necessity, take time to understand the concepts to strengthen measures to prevent or solve privacy problems. However, each type of software handles terms and symbols differently, thus causing frustration and rejection. A paper published in 2011 [4] suggested that making the risks that can affect the privacy of users of a Web application explicit, can help them make better decisions regarding this issue. However, for some users, static design discourages the use of these applications. Considering human factors in safety mechanisms has increased the efficiency of the proposed solutions.

During the last years, researchers have found some relationship between security topics and human factors as shown in Table 1.

**Tab. 1** Relationship between security topics and human factors.

| Research                                                                                                                                                                                                                                                                                                                                                                | Security factors        | Human factors                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------------------------------------------------------------|
| An online study [5] showed that policy formats do have significant impact on users' ability to both quickly and accurately find information and on users' attitudes regarding the experience of using privacy policies. In another study, [6] participants did not continue reading the full policy when the information they sought was not available at short notice. | Policy formats          | Unclear language, finding information, recognizing personal data. |
| However, users interviewed in Switzerland and India feel responsible for protecting their sensitive documents themselves, instead of relying on cloud storage providers. It shows that end-users have a strong belief, fueled by media stories and hacker stereotypes, that the Internet is intrinsically insecure [7].                                                 | Cloud storage           | Unreliable                                                        |
| Another job studied both the relationship between demographics and phishing susceptibility. Gender and age are two key demographics that predict phishing susceptibility [8].                                                                                                                                                                                           | Phishing susceptibility | Demographics                                                      |
| Another study revealed that people really get angry about apps in social networks because they take and redistribute                                                                                                                                                                                                                                                    | Third-party access and  | Concern, anger,                                                   |

|                                                                                                                                       |                     |             |
|---------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------|
| their personal information without consulting them first , in spite of the fact that it is specified somewhere in the social network. | redistributing data | frustration |
|---------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------|

From the perspective of neurophysiology and psychology, some articles have proposed cognitive, affective and physiological models with features that indicate how people perceive their interactions and respond to learning environments [9]. These are referred to as learning styles and have contributed to the educational process in recent years [10]. Some research projects have suggested their application to generate interfaces that facilitate users' cognitive ergonomics [11-13].

### 3 The problem

The number of Internet users is increasing globally and this trend is expected to continue. In a national study with adults, it is observed that 13% said that information owners are responsible for the proper treatment of personal data. However, 31% could not define what personal data may be and only 19% always read the privacy notice of a web site, whereas 62% of those surveyed take over 4 minutes to read it. 61% do not know how their information will be handled in the social networks they are involved in [14].

These data reveal the following:

1. The growing number of Internet users lack information security culture in the area of data privacy.
2. Users have interfaces at their disposal to manage their privacy but do not use them.
3. Adult Internet users do not know how to apply security measures.

The legal terms in extensive privacy policies generate feelings of insecurity, uncertainty or indifference in users as to the processing of personal data. People do not know the real effect of what they share on line. Sometimes, they delegate responsibility for information management to the default options presented by the interface. So far, learning styles have not been considered to define the elements of privacy notices and their relationship with users. This also limits developers to creating interfaces that meet the goal of helping surfers in their decision making.

Multidisciplinary teams work to create interfaces and follow the legal requirements in each country. Software components and graphic elements have been associated with the concept of security. However, it cannot be ignored that there are different user profiles and static designs cannot cover all of them. Learning styles and design theories have been applied to create virtual environments to improve cognitive ergonomics. Color has been used as a quantifiable variable of human-computer interaction. So far, no other variables have been proposed to associate privacy with personality features.

#### 3.1 Objective

The goal of this research is to identify the current relationship among the factors of the privacy management of personal data, user interface and learning styles.

#### 3.2 Specific objectives

1. To identify the current relationship between technical and human factors in Internet use and information privacy
2. To establish a relationship between privacy management and learning styles of web users.

3. To recognize the factors considered by users to be critical in managing their privacy.

## 4 Methodology

A quantitative analysis of data was performed. It was based on a parametric analysis using frequencies and correlation coefficients [13]. Frequency analysis and the Pearson correlation method were applied using the SPSS software to identify relationships between the study variables. A survey was applied to 280 students in a University in the city of Puebla, México, with a total population of 8157 students. Their participation was voluntary and compensation was not offered to participants. For a significant sample, the number of respondents was proportional to the total number of students for each major discipline as seen in Table 2. Only 275 surveys were used for the study. This presents a confidence level of 95% with an error of 5.81%.

### 4.1 Demographics

Demographic factors considered are: Major, semester, sex and age, as seen in Tables 2, 3, 4 and 5. The study inquired about the predominant learning style of the participants [15]. It recognized the significant presence of the four styles in the entire sample as shown in Table 6.

### 4.2 Study questions

The study was designed to include three blocks in a third version of the survey:

- 1) Demographics.
- 2) Learning style: People selected their significant learning style based on:

**Active:** Improviser, discoverer, adventurous and spontaneous. I prefer to do and experiment.

**Pragmatic:** Impatient, experimenter, practical, effective and realistic. I prefer to try things out to see their functionality.

**Reflective:** Prudent, cautious, researcher, collector, analytical and thorough. I prefer to observe and reflect.

**Theoretical:** Methodical, logical, objective, critical and structured. I prefer to understand the concepts, ideas and relationships between them.

- 3) We presented a seven-point Likert (0: Nada importante, 6: extremely important). We asked eight questions to understand their knowledge of privacy and we asked four questions to better understand some interface factors:

Rate the importance in degree of the following activities when you browse any website:

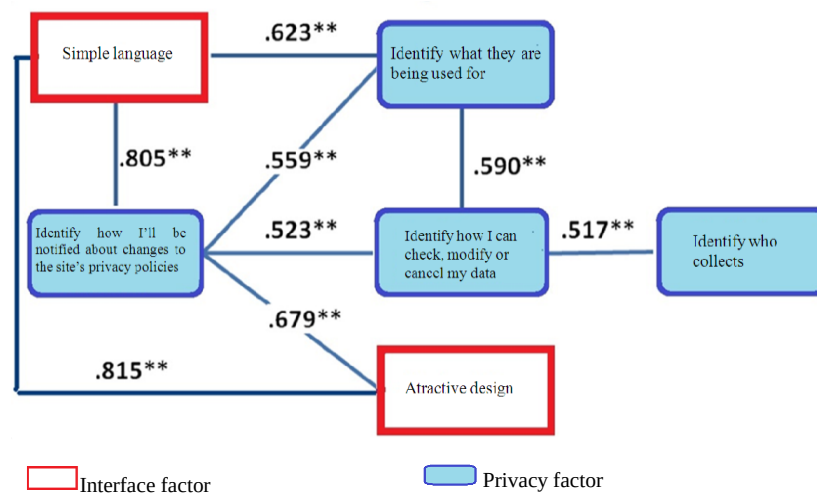
- 4 Identifying who collects your personal data.
- 5 Knowing what they are being used for.
- 6 Applying basic privacy measures.
- 7 Reading the privacy notice.
- 8 Recognizing the main elements in a privacy notice.
- 9 Knowing the federal law about protecting personal data in your country.
- 10 Identifying how you will be notified if there are changes in the privacy notice in a site.
- 11 Identifying options for checking, modifying or canceling your data.

- 12 Simple language.
- 13 Attractive interface design.
- 14 Customizing the browser.
- 15 Suggestions about interface customization according to your tastes.

The relationship among these variables was analyzed using SPSS [16]. The reliability of the instrument was validated based on Cronbach's Alpha of 0.863 as shown in Table 7 and Table 8.

### 4.3 Correlation between study variables

Based on the results obtained by the Pearson Correlation Coefficient, the most significant relationships of the factors that users consider important to manage personal data privacy when browsing any website can be summarized as shown in Fig. 1.



**Fig. 1** Significant relationships based on Pearson Correlation Coefficient

At the end of the survey, participants were asked about the overall rate of satisfaction about the decisions made regarding privacy of data (0 is no satisfaction and 10 is complete satisfaction). The results are presented in Table 9.

## 5 Results

### 5.1 General results

These are the main results from this study:

- A majority of users, regardless of their learning style, present a similar handling of their privacy.
- 85.8% identify their personal information.
- 56.7% know what a Privacy Notice is.
- 87.6% were not aware of the existence of federal laws about the protection of personal data.
- 18.9% apply online measures to maintain the privacy of their personal data.
- A majority of users recognize that it is important to know what third parties do with their personal data; however, no security measures are applied (Fig. 2)
- 18.2% of participants read the online privacy notices of the pages they visit and take from one to four minutes. (Fig. 3)

**Table 2. Major**

| Major                                 | Frequency | Percentage |
|---------------------------------------|-----------|------------|
| Accounting and Senior Management      | 6         | 2.3        |
| Agronomic Engineering                 | 3         | 1.1        |
| Architecture                          | 10        | 3.6        |
| Automotive Design Engineering         | 10        | 3.6        |
| Bionic Engineering                    | 5         | 1.8        |
| Biotechnology Engineering             | 2         | 0.7        |
| Business Administration               | 5         | 1.8        |
| Chemical Engineering                  | 2         | 0.7        |
| Cinema and Audiovisual Production     | 7         | 2.5        |
| Civil Engineering                     | 5         | 1.8        |
| Communications                        | 6         | 2.2        |
| Computer Systems Engineering          | 6         | 2.2        |
| Design and Advertising Production     | 13        | 4.7        |
| Economics                             | 1         | 0.4        |
| Electronic Engineering                | 4         | 1.5        |
| Environmental Engineering             | 11        | 4          |
| Financial and Stock Market Management | 1         | 0.4        |
| Gastronomy                            | 9         | 3.3        |
| Humanities                            | 2         | 0.7        |
| Industrial Engineering                | 11        | 4          |
| Intelligence Business                 | 4         | 1.5        |
| International Relations               | 3         | 1.1        |
| International Trade                   | 10        | 3.7        |
| Journalism                            | 1         | 0.4        |
| Law                                   | 6         | 2.2        |
| Marketing                             | 5         | 1.8        |
| Mechatronics Engineering              | 9         | 3.3        |
| Medicine                              | 71        | 25.8       |
| Institutional Management              | 5         | 1.9        |
| Nursing                               | 7         | 2.5        |
| Nutrition                             | 4         | 1.5        |
| Odontology                            | 9         | 2.9        |
| Pedagogy                              | 2         | 0.7        |
| Philosophy                            | 3         | 1.2        |
| Physiotherapy                         | 5         | 1.8        |
| Political Sciences                    | 1         | 0.4        |
| Psychology                            | 5         | 1.8        |
| Psychopedagogy                        | 2         | 0.7        |
| Veterinary Medicine and Zootechnics   | 4         | 1.5        |

**Table 3. Semester**

| Semester   | Frequency | Percentage |
|------------|-----------|------------|
| 1          | 46        | 16.7       |
| 2          | 8         | 2.9        |
| 3          | 47        | 17.1       |
| 4          | 15        | 5.5        |
| 5          | 57        | 20.7       |
| 6          | 17        | 6.2        |
| 7          | 48        | 17.5       |
| 8          | 12        | 4.4        |
| 9          | 18        | 6.5        |
| 10         | 5         | 1.8        |
| 11 or more | 2         | 0.8        |
| Total      | 275       | 100        |

**Table 4. Sex**

| Sex    | Frequency | Percentage |
|--------|-----------|------------|
| Male   | 136       | 49.5       |
| Female | 138       | 50.5       |
| Total  | 275       | 100        |

**Table 5. Age**

| Age   | Frequency | Percentage |
|-------|-----------|------------|
| 17    | 4         | 1.5        |
| 18    | 26        | 9.5        |
| 19    | 50        | 18.2       |
| 20    | 63        | 22.9       |
| 21    | 56        | 20.4       |
| 22    | 35        | 12.7       |
| 23    | 29        | 10.5       |
| 24    | 7         | 2.5        |
| 25    | 5         | 1.8        |
| Total | 275       | 100        |

**Table 6. Learning style**

| Learning style | Frequency | Percentage |
|----------------|-----------|------------|
| Active         | 78        | 28.4       |
| Reflexive      | 73        | 26.5       |
| Theoretical    | 56        | 20.4       |
| Pragmatic      | 68        | 24.7       |
| Total          | 275       | 100        |

**Table 7.** Summary of case processing

|       |                    | N   | %   |
|-------|--------------------|-----|-----|
| Cases | Excluded           | 275 | 100 |
|       | Valid <sup>a</sup> | 0   | 0   |
|       | Total              | 275 | 100 |

a. Deletion based on all variables in the procedure.

**Table 8.** Statistical reliability

| Cronbach's Alpha | N elements |
|------------------|------------|
| 0.863            | 12         |

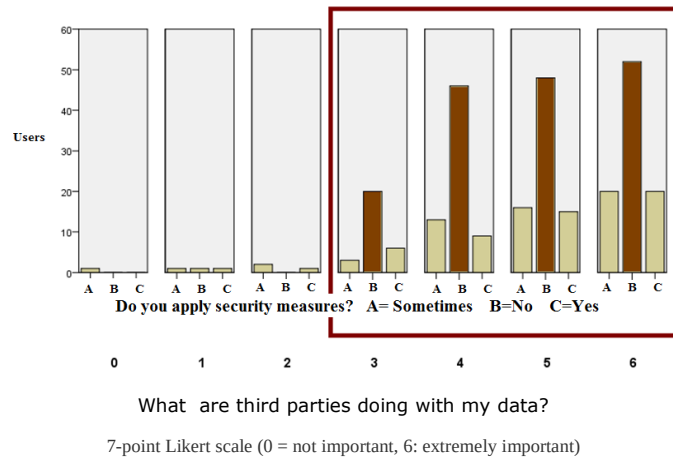
- 48% customize their browser (Fig. 4 and Fig. 5)
- Most respondents have a high level of satisfaction about their privacy decisions. (Fig. 6)
- To manage their privacy, 81.5% would like their tastes for interface customization to be taken into consideration.
- 81.5% expect a simple format and attractive design in a privacy notice.

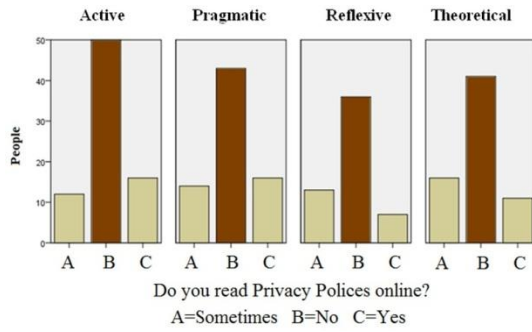
The four most significant correlations based on the Pearson correlation coefficient are:

1. Interfaces must have attractive and simple language (.815 \*\*)
2. Changes to the privacy policies should be displayed in plain language (.805 \*\*)
3. Changes to the privacy policies should be displayed in an attractive design (.679 \*\*)
4. The use of personal data should be displayed in plain language (.623 \*\*)

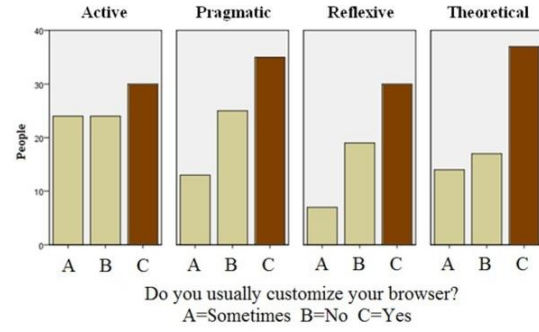
**Table 9.** Overall rate of satisfaction

| Valids | Frequency | Percentage |
|--------|-----------|------------|
| 1      | 4         | 1.5        |
| 2      | 31        | 11.3       |
| 3      | 21        | 7.6        |
| 4      | 25        | 9.1        |
| 5      | 41        | 14.9       |
| 6      | 34        | 12.4       |
| 7      | 45        | 16.4       |
| 8      | 51        | 18.5       |
| 9      | 22        | 8.0        |
| 10     | 1         | 0.4        |
| Total  | 275       | 100.0      |

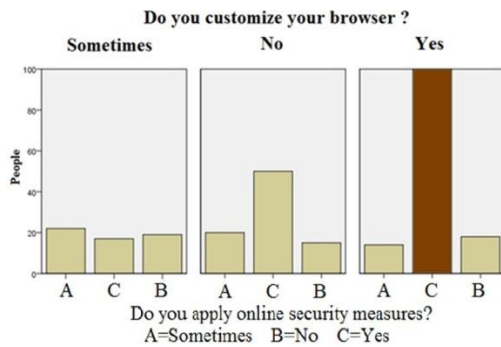
**Fig. 2** Use of personal data and security measures



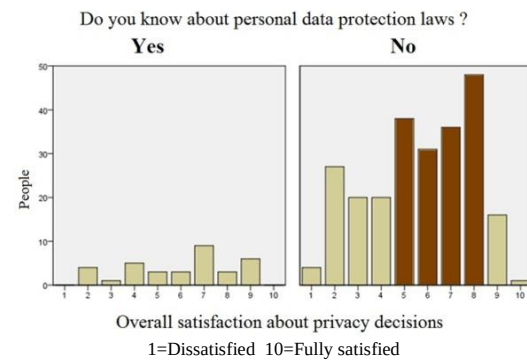
**Fig. 3** Learning style and reading privacy notices



**Fig. 4** Learning style and browser customization



**Fig. 5** Browser customization and security measures



**Fig. 6** Overall satisfaction about privacy decisions

## 6 Discussion

The study was conducted with students from different undergraduate semesters of all the existing majors in a university. These characteristics assume a particular approach and management of information technology and also assume a certain socioeconomic level for a geographic area. Future studies could include people who are outside the set explicitly considered in this ethnographic study and compare the results. The previous experience of the participants was taken into account and a usability study with any particular type of software was not applied. This study considered a particular learning styles theory because there are already tools that allow for their identification; however, it is recognized that there are other theories to consider.

In the context of information privacy, interface design is crucial for managing the security of Internet users (see Fig. 1). Current interfaces do not support the process of understanding the basics of this topic, as some authors have suggested, but the results are not as expected. The absolute values of Pearson's correlation coefficients may suggest a hierarchical navigation between these components. Most respondents customize their interface when surfing on the Internet; however, no security measures are applied (see Fig. 5). This presents areas of opportunity for the proposal of alternate mechanisms to present this information and encourage its application.

This study distinguishes similar behavior in how people manage issues about personal data regardless of their learning style (see Fig. 3). Users want customization preferences to be taken into

account (see Fig. 5). What effect would be generated by considering these preferences in the management of personal data? Would different behavior be observed, in accordance with their learning styles?

This study recognizes the importance of privacy for users and the high degree of satisfaction they claim to have with their decisions regarding privacy (see Fig. 6). However, no security measures are applied by users (see Fig. 5), so this is an obvious problem. But users want their configuration tastes to be taken into account (see Fig. 5) and recognize the importance of protecting their data (see Fig. 2). This means that there are a number of opportunities to propose alternative mechanisms to provide information and promote the implementation of security measures.

## 7 Conclusions

This study shows that the factors related to user interface should be considered from the perspective of security. It would be desirable to provide implementation guidelines that relate the critical factors of information privacy and interface design topics. All learning styles show similar behavior in regards to the interfaces of current privacy management. There is an obvious problem in that users are satisfied with their decisions about the handling of their information without safety measures. Understanding how people perceive and respond to these interactions could bring benefits in terms of increasing their security and in allowing developers to have a framework to improve user experience and system usability.

## References

- 1 Lindskog, H. Web Site Privacy with P3P. Wiley (2003)
- 2 Cranor, L., Langheinrich, M., Marchiori, M. (The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. <http://www.w3.org/TR/P3P/>
- 3 Garfinkel, S., Faith, L. (Security and Usability. Designing Secure Systems That People Can Use. O'Reilly (2005)
- 4 King, J., Lampine, A, Smolen, A.: Privacy: Is there an app for that? Symposium On Usable Privacy and Security. <http://dl.acm.org/citation.cfm?id=2078843>
- 5 Gage, P., Cesca, L., Bresee, J. Faith, L.: Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach [http://www.cylab.cmu.edu/files/pdfs/tech\\_reports/CMUCyLab09014.pdf](http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf)
- 6 McDonald, A., Reeder, R., Gage, P., Lorrie Faith L. : A Comparative Study of Online Privacy Policies and Formats. <http://www.springer.de/comp/lncs/index.html>
- 7 Ion, I., Sachdeva, N., Kumaraguru, P., C'apkun, S.: Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage. [http://cups.cs.cmu.edu/soups/2011/proceedings/a13\\_Sachdeva.pdf](http://cups.cs.cmu.edu/soups/2011/proceedings/a13_Sachdeva.pdf)
- 8 Sheng, S., Holbrook, M., Kumaraguru, P., Faith, L. Downs,: Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions <http://dl.acm.org/citation.cfm?id=1753383>
- 9 Hannaford, C: Cómo aprende tu cerebro. PAX. 20-25 (2011)
- 10 Secretaría de Educación Pública. Manual de estilos de aprendizaje. [http://www.dgb.sep.gob.mx/informacion\\_academica/actividadesparaescolares/multimedia/M anual.pdf](http://www.dgb.sep.gob.mx/informacion_academica/actividadesparaescolares/multimedia/M anual.pdf)
- 11 Muñoz-Arteaga Jaime, Rodriguez-Gomez Gustavo. Patrones de Interacción. Una solución

- para el Diseño de Retroalimentación Visual de Sistemas Interactivos.  
<http://ccc.inaoep.mx/~grodrig/Descargas/InteraPatternToCIC.pdf>
- 12 Perla Velasco-Santos, A. L.-C.-T. Diseño de agentes pedagógicos a partir de los estilos de aprendizaje; una perspectiva a través del color. Memorias del IV congreso mundial de estilos de aprendizaje. ISBN 978-607-7533-66-5. (2010)
  - 13 Velez, O., Solano, D., Zúñiga, L., Argüello, M., Aguado, J., Aldana, J., López, P., Alarcón, A., : Los estilos cognitivos y el aprendizaje maquinal en el diseño de interfaces inteligentes adaptativas. Universidad del Sinú. Centro de Investigaciones y Desarrollo. 3-6 (2005)
  - 14 Asociación Mexicana de Internet AMIPCI. Estudio de Protección de Datos personales entre usuarios y empresas.  
<http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=95&Type=1>
  - 15 CHAEA. Cuestionario Honey Alonso de Estilos de aprendizaje.  
<http://www.estilosdeaprendizaje.es>
  - 16 Malhortra, N.: Investigación de Mercados. Pearson Prentice Hall. 5ª. Edición. (2008)

## **Appendix D. Enhancing privacy awareness through interaction design.**

XV International Conference on Human Computer Interaction. Interacción 2014. September 10-12, 2014. Puerto de la Cruz. Tenerife. Spain. pp 287-290

### **Objetivo:**

Definir un conjunto de patrones de interacción para facilitar la construcción, percepción y manipulación de un aviso de privacidad utilizando para el diseño los resultados sugeridos en los trabajos presentados en:

*II. Patrones de Interacción y su aplicación a la privacidad en Internet y*

*III. Studying the relationships between the management of personal data privacy and user interface.*

La primera parte de este trabajo presenta la percepción que se tiene por parte de una población universitaria respecto a los avisos de privacidad de las páginas de internet. La segunda parte registra las herramientas que usan los desarrolladores para construir estas aplicaciones. Finalmente se analiza si un conjunto de patrones de interacción mejora la interacción con éste por parte de los usuarios finales y si facilita el trabajo de los desarrolladores de estas aplicaciones.

# Enhancing Privacy Awareness through Interaction Design

Sandra R. Murillo

Universidad Popular Autónoma del Estado de Puebla  
Puebla, Puebla 72410, México  
sandrarocio.murillo@upaep.mx

J. Alfredo Sánchez

Interactive and Cooperative Technologies Lab  
Universidad de las Américas Puebla  
alfredo.sanchez@udlap.mx

## ABSTRACT

A wide range of tools can be used for endowing applications with functionality related to user privacy according to customer's requirements and developer's experience. This implies a high investment of resources because it requires team skills in legal areas, computer security, graphic design and cognitive ergonomics. Despite this situation, there are no specific software tools that allow developers to build effective privacy management applications that consider three critical requirements: compliance with legal terms, adherence to budget limitations, and usability for the target audience. This paper proposes applying interaction patterns to reduce current gaps in the interaction between users and privacy notices.

### Categories and Subject Descriptors

K.4.1 [Computers and Society]: Public Policy Issues, Privacy

### General Terms

Human Factors, Design, Security

### Keywords

Human factors, Usability, Security.

## 1. INTRODUCTION

The increasing popularity of diverse technologies has made it possible for personal information to be used for purposes other than those originally intended. Sometimes, personal data may be transferred to other entities without the owner's explicit consent. From the perspective of personal data protection, owners of data have the right and freedom to decide what to communicate, when and to whom, maintaining control over their personal information at all times. Due to problems that have arisen (identity theft, fraud, etc.), international organizations have proposed mechanisms for software developers that include options that strengthen user privacy. On the technical side, it has been possible to detect and provide solutions. This paper investigates what tools developers use to build privacy software, and proposes a pattern based on interaction with the elements of a privacy notice as means to reduce existing communication gaps. The paper is organized as follows: Section 2 discusses the

main information privacy issues. Current situation of privacy policies is defined in Section 3. Legacy tools versus interaction

patterns are presented in Section 4. Finally, Section 5 presents future work.

## 2. INFORMATION PRIVACY

More and more countries have passed laws that claim to protect people and not just data (Rebollo). Early efforts date from 1967, with Resolution 509 of the European Council about "human rights and new scientific and technical achievements." In the late 1970s, Germany, France, Denmark, Austria and Luxembourg approved similar national laws. During the 1980s, the European Council legislated on protection of privacy against potential aggressiveness of technologies, through the promulgation of Convention 108 to protect people against the automated processing of data. The purpose was to ensure that citizen's respect of their rights and freedoms, notably the right to privacy. These provisions granted users the right to access their information and modify it if deemed inaccurate, the right to eliminate data when it is no longer relevant or has become obsolete, and the right to oppose their use by a third party.

Several other projects have been implemented (Cranor, Langheinrich, & Marchiori, W3C The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, 2002) (Garfinkel & Faith, 2005); however, only few experiences in Latin America have been reported. The Federal Law on Protection of Personal Data Held by Private Parties (Unión, 2010) was adopted in Mexico in 2010. According to Article 16 of this law, protecting personal data is a fundamental right. Any business or entity requesting personal information should develop and publish a Privacy Notice, a document that discloses some or all of the ways a party gathers, uses, reveals and manages customer's data. There are several guidelines, interaction patterns (Life, 2008), tools (Datos, Guía práctica para generar el aviso de privacidad, 2012) and research projects (Gage Kelley, Cesca, & Faith) that have proposed and evaluated (Jensen & Potts, 2004) mechanisms to generate a privacy notice. However, the information generated does not produce a useful document for end users, thus delegating responsibility to the default options suggested by the interface (Murillo & Sánchez, Studying the Relationships between the Management of Personal Data Privacy and User Interface, 2013).

## 3. CURRENT SITUATION OF PRIVACY POLICIES

In order to examine the current situation of online privacy notices in México, a quantitative study has been conducted. The average time that users need to identify privacy notice elements, as well as other human factors, have been documented. A statistical study based on frequency analysis (Malhortra N. K., 2008) was performed based on the previous experience of participants, using a paper-based questionnaire to document human factors related to reading a privacy notice. We investigate whether privacy notices include the elements required by law, and whether users perceive a user-friendly format. We measure the time invested in identifying various elements and document user satisfaction with regard to interaction. Online privacy notices and paper-based questionnaires are used to collect data. Subsequently, the performance of a group of developers who use legacy tools to build interactive privacy policy applications is documented and compared to determine whether they had any interaction patterns set in place from the beginning of the project.

### 3.1 Results

1. The average time to read a privacy notice was 10.3 minutes, assuming a college level of reading and understanding.
2. None of the privacy notices showed all the elements required by law.
3. Required items such as Identity and Address of the person in charge, Purpose of data processing and Options to exercise ARCO rights were found in 86.7% of the sample.
4. Mandatory element "Method and options by which changes are reported in the Privacy Notice" was found in 80% of the total sample.
5. Options for limiting the use and disclosure of data was found in only 46.7%.
6. No participant agrees with respect to the similarity among notice formats across all the web pages they visit.
7. 66.7% of our subjects consider it is very difficult to identify the elements of a privacy notice and it is unpleasant to read the notices.
8. 33.3% of the sample think the websites do not help to manage privacy.
9. 66.7% of the sample think Internet users in general cannot understand the contents of a privacy notice.

### 3.2 Discussion

This study was conducted with volunteer eighth- and ninth-semester Information Technology students who were not offered any compensation for their time. An advanced reading level was assumed. In order to protect users, the presence of a privacy notice is required; however, these notices do not have a homogeneous structure, nor do they include patterns, icons or universal formats to help users understand their basic elements. Participants believe that most people do not understand the contents of a privacy notice. If this happens to people in higher

education, it is essential to investigate what happens in other sectors of the population.

It takes too long to read the average notice, considering that this step is mandatory in order to access a web page that collects personal data. For most users it is not an enjoyable activity and they perceived that there were no mechanisms to help them manage their privacy. From this, two things are suggested. First, to study the relationship between the user interface and privacy factors to propose schemes that improve the browsing experience. Additionally, it is key to analyze whether developers of privacy-related applications have appropriate tools at their disposal to facilitate this task.

## 4. LEGACY TOOLS VS INTERACTION PATTERNS

We have compared the performance of developers when building end-user privacy applications by using legacy tools versus using interaction patterns. Legacy tools refer to traditional programming languages or frameworks (Harper, 2012) whereas an interaction pattern describes a successful solution to a recurring problem related on the user interface than can be replicated in a given context (Borchers, 2001). During the Fall 2012 a group of eleven students in a course of the seventh semester of Computer Engineering and Software Engineering was organized in order to identify the software elements used to build applications about privacy. They were allowed to freely choose the tools they considered appropriate for their design and implementation.

After completing the course and evaluating the functionality of their applications, students were provided with a set of interaction patterns (COPEMMA (Murillo & Sánchez, Patronos de interacción y su aplicación a la privacidad en Internet, 2013)) and the Privacy Notice (which will be described in Section 4.1). Each team was asked to estimate the impact on the finished work, if they had received such patterns at the beginning of the course. Students participated under the premise that only the fulfillment of the requested functional requirements is assessed. Development teams did not have the support of legal experts or graphics (or similar) designers. Functional requirements were presented to each team without mentioning the purpose of this study. Each team selected its methodology for software development, programming language, icons, images and organization of information on the screen. They were invited to present their conclusions and participated voluntarily in a survey without any compensation.

There were five projects involved in this study. The projects were titled as follows: (1) Navigation prototype for a privacy notice on an Android-based mobile device; (2) Web graphics display elements of a privacy notice for college students; (3) View of a simplified Android privacy notice based on learning styles; (4) Augmented reality applied to display elements of privacy; and (5) Display privacy policies based on P3P

(Platform for Privacy Preferences) for the Chrome browser. In the three partial evaluation sessions of functional requirements of each application, developers were asked openly on all tools, guidelines and standards used as the basis for building each project. A summary of these tools is presented in Table 1.

**Table 1. Programming tools, guides and standards**

| Tools              | Methodology                              | Information security standards                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eclipse, PHP, Java | Modeling Scrum, Object-oriented modeling | Protection of personal data Law, collections of icons, data encryption function, password entry fields, APIs development, Privacy-Bird-P3P*, XACML**<br>* <a href="http://www.w3.org/P3P/">http://www.w3.org/P3P/</a><br>** <a href="http://sunxacml.sourceforge.net/">http://sunxacml.sourceforge.net/</a> |

## 4.1 Interaction Pattern: Privacy Policy

The following interaction pattern was designed based on the observations made in 4.1.2 and previously published work: (Murillo & Sánchez, Patrones de interacción y su aplicación a la privacidad en Internet, 2013) (Murillo & Sánchez, Studying the Relationships between the Management of Personal Data Privacy and User Interface, 2013)

**Name:** Full privacy notice

**Problem:** The Privacy Notice is a document generated by the individual or entity responsible for the proper compiling and processing of personal data and should be made available to the owner of the data. This document does not have a defined structure and each party decides on the format. The document is written in legal language, unclear to the end user, and it is difficult to identify its parts. It is commonly ignored by users because of its length.

**Solution:** A hierarchy of data distribution and navigation information based on usability rules is proposed. The user is shown the procedure to identify the elements of a privacy notice and the function of each one.

**Context:** According to Article 16 of the FPDPPP (Federal Law on Protection of Personal Data Held by Private Parties) in Mexico, a comprehensive format is required to explicitly include the following:

- Handling of data collected
- Individuals responsible for storing data
- How to exercise ARCO rights
- How changes in the Privacy Notice will be announced
- How to limit the use of data, consent for the transfer of data
- Revoking consent for processing captured data
- Revoking consent for the transfer of data to third parties
- Explicit information about vulnerable groups
- Use of cookies and additional data collection

technologies

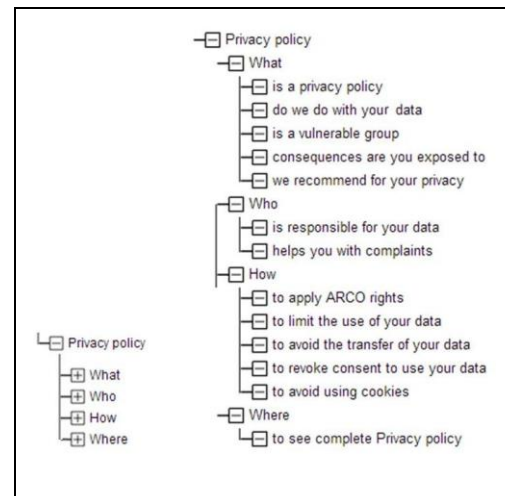
- Display of consequences of possible misuse of data
- Tips to prevent misconduct

**Usability:** Helps users to identify the elements of a privacy notice.

**Consequences:** Users can identify the parts of a Privacy Notice, recognize its importance and exercise their ARCO rights in a timely manner.

**Related patterns:** Personal information, Sensitive personal data, Exercise ARCO rights.

**Example:**



During the last review session participants were asked to evaluate the tools used. During the Summer term of 2013, students who developed the five projects studied the concept of interaction patterns, unknown to the students at that time. They were asked to estimate how their Fall 2012 projects would have been influenced had they been given to them at the beginning of their projects. Finally, they were asked to estimate the average hours they would have saved had they been given the interaction patterns at the beginning of their projects.

## 4.2 Results

Neither team used tools to build prototypes, nor there was any comprehensive collection of specialized items identified as having helped them in their design and development. Supporting elements (Java classes, extensions for particular types of browsers) were found to support any type of application (See Table 1). The tools used are considered useful in designing a privacy application 60% of the time, compared to 80% for interaction patterns. The existence of a universal language in the area of security information is not recognized. The participation of a graphic designer is considered pertinent in these projects.

An average reduction of 25.7% of the total development time for applications is expected if interaction patterns are made available at the beginning of the project. Traditional design tools are useful for creating IT security applications. However, having a collection of interaction patterns makes it easier for software developers.

### 4.3 Discussion

Future studies will include graduates majoring in areas involved in the software industry and graphic design students who have experience in software development teams. The satisfaction of the developers regarding the use of traditional security tools for the graphical interfaces design is very low. This fact promotes opportunities to suggest models that support these projects. Due to the increasing number of Internet users, it is necessary to build security software applications. Legacy development tools support building effective applications, however, having a collection of interaction patterns facilitates the tasks related with the design of privacy-aware applications. These patterns are presented as good practices in the software development cycle and may reduce the implementation time. The fact that there is not a universal language about security information presents opportunities to propose elements to enhance collaboration between experts and multidisciplinary teams.

The construction of a collection of interaction patterns that includes these results can influence issues of usability and user experience when building tools to support the administration of privacy. Many applications are developed solely by security experts, which may fulfill functional requirements, but this typically is far from solving real problems for users. Current interaction with the elements of a privacy policy does not facilitate the exercise of ARCO rights, thus forcing Internet users to navigate in insecure mode, being at the expense of any possible misuse that may be given to personal information.

Presenting users with policies regarding how their data will be treated has been approached from the technical and legal framework perspectives, but the ultimate goal, which is to protect people and facilitate the exercise of the ARCO rights has not been satisfied. The observed user experience with privacy notices has not been positive. Resources that facilitate the design and construction of interfaces involving privacy issues for end users are scarce. In order to implement this kind of applications developers can apply any methodology and software development tools according to the needs and available resources; however, addressing user needs can be facilitated by relying on a set of specific interaction patterns.

## 5. ONGOING AND FUTURE WORK

Ongoing work includes the development of collections of interaction patterns based on how people learn and interact with human-computer interfaces in order to improve information security culture of Internet users, reduce risks and

mitigate associated problems. We plan to include other profiles for potential users in a formal study and involve a larger sample.

## 6. REFERENCES

- [1] L. Rebollo, "Vida privada y protección de datos. Un acercamiento a la regulación internacional europea y española," [Online]. Available: <http://biblio.juridicas.unam.mx/libros/6/2758/10.pdf>.
- [2] L. Cranor, M. Langheinrich and M. Marchiori, "W3C The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," 2002. [Online]. Available: <http://www.w3.org/TR/P3P/>.
- [3] S. Garfinkel and L. Faith, Security and Usability. Designing Secure Systems That People Can Use., O'Reilly , 2005.
- [4] C. d. d. H. C. d. l. Unión, "Ley federal de protección de datos personales en posesión de los particulares," 2010. [Online]. Available: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.
- [5] P. Life, "HCI Patterns Collection - Version 2," [Online]. Available: [http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci\\_pattern\\_collection\\_v2-public.pdf](http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf).
- [6] I. F. d. A. a. l. I. y. P. d. Datos, "Guía práctica para generar el aviso de privacidad," [Online]. Available: <http://inicio.ifai.org.mx/DocumentosdeInteres/privacidadguia.pdf>.
- [7] P. Gage Kelley, L. Cesca and L. Faith, "http://repository.cmu.edu/cylab/1/", "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach.
- [8] C. Jensen and C. Potts, "Privacy policies as decision-making tools," SIGCHI conference on Human Factors in Computing Systems, pp. 471-478, 2004.
- [9] S. R. Murillo and J. A. Sánchez, "Studying the Relationships between the Management of Personal Data Privacy and User Interface," Human Computer Interaction. Lecture Notes in Computer Science Volume 8278, pp. 79-89, 2013.
- [10] N. K. Malhortra, Investigación de Mercados., Pearson Prentice Hall. 5ª. Edición., 2008.
- [11] R. Harper, Practical Foundations for Programming Languages, Cambridge University Press, 2012.
- [12] J. Borchers, A pattern approach to interaction design, England: Wiley, 2001.
- [13] S. R. Murillo and J. A. Sánchez, "Patrones de interacción y su aplicación a la privacidad en Internet," in INCOSE, Puebla, 2013.

## **Appendix E. Empowering Interfaces for Network Security Administrators. Keeping the Command Line in Mind when Designing GUIs.**

XV International Conference on Human Computer Interaction. Interacción 2014. September 10-12, 2014. Puerto de la Cruz. Tenerife. Spain. pp 308-311

Objetivo:

Definir un conjunto de patrones de interacción para facilitar la percepción y manipulación de herramientas de administración de una red con base a los factores críticos de seguridad informática y la interface de usuario.

En la primera parte de este trabajo se identifican los factores técnicos y humanos considerados como críticos para administrar de una red y se presentan los resultados de una evaluación de usabilidad para herramientas basadas en líneas de comandos. Con base en las observaciones de la fase anterior, se construye y evalúa la usabilidad de un prototipo GUI para identificar si existe una mejora en el desempeño de los administradores de red.

# Empowering Interfaces for System Administrators: Keeping the Command Line in Mind when Designing GUIs

Sandra R. Murillo  
Universidad Popular Autónoma del Estado de Puebla  
Puebla, Puebla 72410, México  
sandrarcio.murillo@upaep.mx

J. Alfredo Sánchez  
Interactive and Cooperative Technologies Lab  
Universidad de las Américas Puebla  
alfredo.sanchez@udlap.mx

## ABSTRACT

In terms of usability, network management software based on command line interfaces (CLI) is efficient but error prone. With GUIs, a new generation of security tools emerged and were adopted by young system administrators. Though usability has improved, it has been argued that CLI-based software tends to support better user performance. Incorporating CLI advantages into graphical versions (or vice versa) remains a challenge. This paper presents a quantitative study regarding system administrators' practices and preferences regarding GUIs and CLIs and reports on initial results of a usability evaluation performed on proposed interfaces that are informed by our study. Personalization features are particularly appreciated by network administrators, which suggests possible strategies for graphical interface designs that improve user experience while maintaining the positive aspects of CLI-based software.

### Categories and Subject Descriptors

H.1.2 [User/Machine Systems]: Human factors

### General Terms

Human Factors, Design, Security

### Keywords

Human factors, Usability, Security, GUIs, command line interfaces.

## 1. INTRODUCTION

The administration of computing and telecommunications infrastructure supporting services is a continuous challenge. Nowadays, there are several tools that can be implemented to manage the basic principles a safe system should have in place: integrity, confidentiality, availability, authentication and non-repudiation. Though most software in this area complies with its technical objective, it does not typically adhere to guidelines for interface design, and may not be the best for the technology consumers in terms of critical factors of user experience. In some cases, this causes frustration, waste of time and prevents the transference of the acquired experience on to the utilization of other tools in a natural manner, forcing users to adapt to each tool, and not the other way around.

At present, each user has to be not only an expert in information security, but also in interface usage. With such a poor integration, users are responsible for correlating and making sense of the results obtained through multiple distributed systems using different techniques, including some manual procedures.. Tools based on the command line interface (CLI) are still considered very powerful, as they allow a detailed handling of data and parameters, including those provided by graphical interfaces. In order to take advantage of CLI-based tools, users should have syntactic knowledge of sentences to be executed, and are constantly at risk of making typing errors. This paper presents a quantitative study about system administration practices and preferences regarding GUIs and CLIs. The paper is organized as follows: Section 2 discusses the main issues in the usability and security management tools. The main problem is defined in Section 3, whereas Section 4 describes the methodology followed in our study. Our initial results are presented in Section 5. A prototype measurement is presented in Section 6. Finally, Section 7 presents the future work derived from our study.

## 2. SECURITY AND USABILITY

Due to the constant growth of Internet usage, working in security software is a challenge for all of those involved [1]. According to [2], over 70% of the security breaches against company networks come from the "application level" and not from the "network level" in terms of the OSI model [3]. This indicates that having a deep knowledge of programming, routing protocols or operating systems is not even necessary to cause severe damage through easy to use applications. Having the tools to predict and mitigate undesirable acts and to opportunely detect "false positives" within a network is indispensable (Jackson, 2012) (Miller & Harris, 2011).

According to (Kandogan & Haber, Security Administration Tools and Practices, 2005), a security support tool would have a high level of usability if it had standard formats that permit inter-tool integration, data mining applications, events flow automatic processing, collaboration and information interchange, as well as effective, scalable work spaces that allow personalization with programmable visualizations. Moreover, in [9] it is said that reporting capabilities, historical analysis and real time monitoring are data analysis strategies that must be present in security related tools. As stated by (Rubio-Valdehita, Díaz-Ramiro, & López-

Higes, 2012), when designing graphical interfaces for tools based on command lines, it is necessary to identify user experience elements that are important and are strongly correlated, making sure the design avoids blindness due to lack of attention.

A good interface design should offer the possibility of finding the interaction elements that pinpoint what/who the interface addresses, where the elements are located, and how it performs its tasks. Various authors (Nielsen J. , 1993) (Constantine, 1999) agree that the principles of interface design should focus on ensuring consistency between the functionality of the applications and the environment where they will be utilized, so they can offer a comprehensible space for interaction. There is a considerable amount of security tools based on command line (SANS, 2013) (Ross, Unix system security tools, 2010). A command line interface (CLI) is a type of human-computer interface that relies solely on a set of specific commands and their corresponding parameters, all of this in pure text (for entering commands) and textual display of results. That is, the entire display screen, or the currently active portion of it, shows only characters, and input is usually performed entirely with a keyboard (Loukides, 2002). Some advantages according to (Preece, 1994), first, the user faces less distraction as there is no need to interact with GUI; second, commands in CLI can be used to create complex shell scripts to solve complex tasks. In the other hand, a disadvantage of CLI is the user's high cognitive workload because they have to remember the commands and parameters.

### 3. THE PROBLEM

There are several specific tools based on CLI for each security administration task in a given network. It is very hard to transfer the experience acquired while using one of these tools to the use of another that is based on a different interface paradigm, as the representations of the basic factors that are common to such tasks have not yet been standardized. For every system, the user must know beforehand the command syntax and parameters for the task to be executed. Security administrators consider an application usable as long as it fulfils the specific technical objective for which it was originally developed (Nemeth & Snyder, 2011). For years, applications have maintained the same format and it is well known that experts in this area should be able to totally adapt to them, with no certainty of whether or not both GUI and CLI versions would be available. We thus formulated the following working hypothesis:

*The performance of network administrators will improve by relying on usable graphical interfaces of the corresponding command line tools.*

### 4. METHODOLOGY

In order to investigate the validity of our hypothesis, we conducted a quantitative study, based on a parametric analysis using frequencies and correlation coefficients (Malhortra N. , 2008). Frequency analysis and the Pearson correlation method were

applied using the SPSS software to identify relationships between the study variables. A prototype was designed and a usability study (Brook, System Usability Scale, 1998) and a survey were applied. Fifteen experienced network administrators were asked to mention the 20 basic tools they utilize to perform their duties as network security administrators, regardless of whether they like to use them or not. The following was observed: 53% use a CLI version, 31% a GUI version, and 16% both versions. According to these results, only the four most voted tools based on Command line version were selected: an intrusion detection system (Snort (Sourcefire, 2000)), a password cracking program (John the Ripper (Openwall, 2001)), an email policy administrator (Procmail (Van den Berg, 2000)), and a remote device administrator (SNMP (Research, 2001)).

#### 4.1 Technical elements and interface elements

By means of a survey, the participants were asked to indicate the technical elements and the interface elements that they consider should have a common and consistent representation throughout the four tools selected for this study. The technical elements, in no particular order, that participants would expect to find in a consistent manner throughout network security tools are the following:

- |                                               |                                            |
|-----------------------------------------------|--------------------------------------------|
| • Internet Protocol (IP) address range        | • Progress bar                             |
| • Ports menu                                  | • Execution time (Hours, minutes, seconds) |
| • Protocols menu                              | • Execution mode (Online, offline)         |
| • Network card menu                           | • Real time log                            |
| • Workgroup                                   | • Expected results                         |
| • Application status (Active / inactive)      | • Advanced functions                       |
| • Scheduling tasks                            | • Save/send log                            |
| • Basic functions (Start, stop, pause, reset) | • Save/send partial results                |
| • Administrative menu                         | • Save/send final results                  |
| • Network map                                 | • Save/send Log                            |
| • Percentage of completion                    |                                            |

The interface elements, in no particular order, that participants would expect to find in a consistent manner throughout network security tools are the following: Customizing colors, customizing typography, representative icons, relocating elements, graphical version and command line version. The participants answered four paper-based questionnaires (one per tool) containing five-point Likert scale items in order to determine the importance of each one of the elements present in the tools. The relationship between variables was analyzed using SPSS (Malhortra N. , 2008).

### 5. INITIAL RESULTS

These are the main results of this study:

- The values obtained through the SUS evaluation for the four tools under study range between 20.5 and 28.3. This data shows that there is a perceived low usability level for CLIs.
- None of the participants feel satisfied with the idea that CLI tools facilitate network security tasks.
- For the four tools, there are strong correlations between each tool's basic functions and interface related elements (Table 1 to 4).

## 6. IMPLEMENTATION AND MEASUREMENT

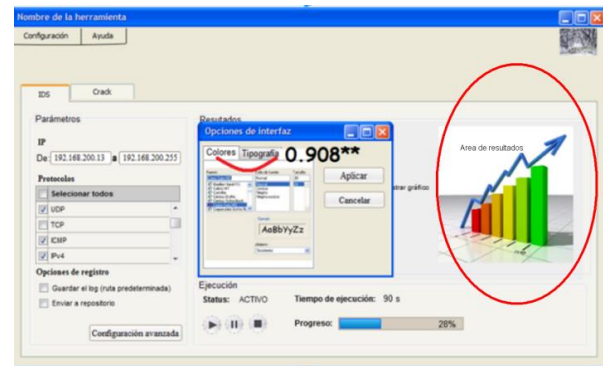
A prototype based on the results presented in Section 5 was designed as follows. See an example in Figure 1.

1. Interactive elements were placed near or far from each other according to the values of the correlations presented in Section 5 of this paper. If the correlation was very high, proximity was immediate. For example, in Snort GUI prototype, proximity of the Colors and Typography is on the highest identified correlation value (Figure 1).
2. The proportion of the interaction elements on the screen was considered based on the importance of the corresponding task. For example, the area of Expected Results (highlighted by an oval) is Muy importante for potential users of the graphical version of Snort (Figure 1).

Participants were asked to assess the original CLI tools, according to their previous experience and to assess a second version of this prototype, as well as the usability of such tools by means of the questionnaire recommended by the SUS methodology (Brook, System Usability Scale, 1998). The average scores given by the 15 participants are shown in Table 5.

**Table 1 . Snort result**

| Correlations                                                                                                                                                                                                                                                                                                                                                                                                                                            | Interpretation                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• <i>Changing colors</i> is correlated to <i>basic functions</i> (0.891**), to <i>expected results</i> (0.721), to <i>change typography</i> (0.908**) and to <i>progress bar</i> (0.881**).</li> <li>• <i>Representative icons</i> is correlated to <i>basic functions</i> (0.928**), to <i>expected results</i> (0.784*), to <i>change typography</i> (0.874*) and to <i>progress bar</i> (0.906**).</li> </ul> | It is necessary to include <i>representative icons</i> and to apply <i>changing colors</i> option to <i>basic functions</i> , <i>expected results</i> , <i>change typography</i> and <i>progress bar</i> . |
| <i>Change typography</i> is correlated to <i>graphical version</i> (0.700).                                                                                                                                                                                                                                                                                                                                                                             | It is Muy importante to include <i>change typography</i> option in a GUI version.                                                                                                                          |



**Figure 1. Prototype**

**Table 2. John the Ripper results**

| Correlations                                                                                                                                                                                                                          | Interpretation                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Change colors</i> is correlated to <i>administrative menu</i> (0.725), to <i>Command line version</i> (0.960**), to <i>basic functions</i> (0.725), to <i>relocate elements</i> (0.735) and to <i>change typography</i> (0.960**). | It is necessary to include <i>change colors</i> option to <i>administrative menu</i> , <i>CLI</i> , <i>basic functions</i> , <i>relocate elements</i> and <i>change typography</i> . |
| <i>Relocate elements</i> is correlated to <i>basic functions</i> (0.730) and to <i>real time log</i> (0.730).                                                                                                                         | It is necessary to include <i>relocate elements</i> option to <i>basic functions</i> and to <i>real time log</i> .                                                                   |
| <i>Representative icons</i> and <i>basic functions</i> (0.923**) are strongly correlated.                                                                                                                                             | It is indispensable to include <i>representative icons</i> in <i>basic functions</i> .                                                                                               |

**Table 3. SNMP results**

| Correlations                                                                                                                                                                                 | Interpretation                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Change colors</i> is correlated to <i>command line version</i> (0.725), to <i>scheduling tasks</i> (0.702), to <i>relocate elements</i> (0.710) and to <i>change typography</i> (0.764*). | It is necessary to include <i>change colors</i> option to <i>scheduling tasks</i> , <i>relocate elements</i> and <i>change typography</i> tasks. |
| <i>Expected results</i> is correlated to <i>change colors</i> (0.711), to <i>representative icons</i> (0.753) and to <i>relocate elements</i> (0.826*).                                      | <i>Expected results</i> needs <i>change colors</i> , <i>representative icons</i> and <i>relocate elements</i> options.                           |

**Table 4. Procmail results**

| <b>Correlations</b>                                                                                                                                                                                                                                                          | <b>Interpretation</b>                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Basic functions</i> is correlated to <i>representative icons</i> (0.795*), to <i>application status</i> (0.859*), to <i>advanced functions</i> (0.723), to <i>change colors</i> (0.881), to <i>graphical version</i> (0.786) and to <i>command line version</i> (0.779*). | <i>Basic functions</i> need <i>representative icons</i> and <i>change colors</i> options, also need to be close to <i>application status</i> , <i>advanced functions</i> , <i>GUI</i> and <i>CLI</i> . |
| <i>Change colors</i> is correlated to <i>change typography</i> (0.842*).                                                                                                                                                                                                     | <i>Change colors</i> option needs to be close to <i>change typography</i> .                                                                                                                            |
| <i>Command line version</i> is correlated to <i>representative icons</i> (0.921**).                                                                                                                                                                                          | <i>CLI version</i> needs <i>representative icons</i> .                                                                                                                                                 |

## 7. PRELIMINARY CONCLUSIONS

This study was conducted with the help of senior undergraduate students majoring in Information Security, and lecturers with more than fifteen years of experience in information security education and consulting. Future studies will include security experts coming from different geographical and cultural regions in order to assess the impact of these variables. There is a strong correlation between changing colors and changing typography, which means that the users consider them as *Muy importante* elements and they should be placed one next to the other within the interface. For all security tools, including representative icons is an indispensable feature. Users expect to find the available options represented in a graphical language, consistent throughout all the evaluated tools. This element shows a high correlation with the tool's basic functions for all the four cases studied. When it comes to performing tasks as a security administrator, the presence of these icons is considered even more important than the presence of technical options. Establishing a universal set of security icons to be applied on the interface could increase the tools' usability and improve users' performance. Changing the position of the elements within the interface and having a graphical version, additional to the command line version are options the users of these tools consider of high priority. This suggests that personalization of the workspaces could increase the tools' usability and improve users' performance. It is possible that the best option for some users is command line version; however, people with other profiles could make better use of their different skills using a graphical version.

**Table 5. SUS Results Part 1**

| <b>Tool</b>     | <b>SUS Results CLI</b> | <b>SUS Results Prototype</b> |
|-----------------|------------------------|------------------------------|
| Snort           | 22                     | 70.6                         |
| John the Ripper | 28.3                   | 71.3                         |
| Procmail        | 20.5                   | 69                           |
| SNMP            | 23.3                   | 68.6                         |

The initial values obtained through the SUS evaluation (Table 5) show that the level of usability for the tools under study is low and it doesn't satisfy the users who utilize them on a daily basis. There is an improved usability of GUI management security tools, which typically are used as CLI (Table 5). Further studies may investigate whether specific personality characteristics of administrators may suggest customization models to improve their performance. It is necessary to conduct a study with users in which they are asked to perform a set of typical network administration tasks using different versions of the considered tools and make comparisons to determine whether the usability of one tool is objectively better than the other. At this point in the study, we do not have final results regarding usability metrics such as the number of completed tasks, runtime, number of requests for help, errors and level of satisfaction according to age, gender and experience. After that, it will be possible to document the observations and determine the outcome of the hypothesis proposed at the beginning of this work.

## 8. REFERENCES

- [1] G. Jackson, *Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security*, John Wiley & Sons, 2012.
- [2] D. Miller and S. Harris, *Security Information and Event Management (SIEM) Implementation*, McGraw-Hill/Osborne, 2011.
- [3] E. Kandogan and E. Haber, "Security Administration Tools and Practices," 2005. [Online]. Available: <http://www.plunk.org/eben/PublishedPapers/Security-ch18.pdf>. [Accessed 2014].
- [4] S. Rubio-Valdehita, E. Díaz-Ramiro and R. López-Higes, "Effects of task load and cognitive abilities on performance," *Anales de psicología*, vol. 28, no. 3, pp. 986-995, 2012.
- [5] J. Nielsen, *Usability Engineering*, Morgan Kaufmann, 1993.
- [6] L. Constantine, *Software for Use: A Practical Guide to the Models and Methods of Usage-Centered Design*, Addison-Wesley, 1999.
- [7] I. SANS, "Securing Linux/Unix," 2013. [Online]. Available: <https://www.sans.org/course/securing-linux-unix>.
- [8] S. Ross, *Unix system security tools*, McGraw-Hill, 2010.
- [9] M. Loukides, *System performance tuning*, O'Reilly & Associates, Inc., 2002.
- [10] J. Preece, *Human-Computer Interaction: Concepts And Design*, Addison Wesley, 1994.
- [11] E. Nemeth and G. Snyder, *Unix system administrator handbook*, Prentice Hall, 2011.
- [12] N. Malhorta, *Investigación de Mercados*, Pearson Prentice Hall. 5ª. Edición, 2008.
- [13] J. Brook, "System Usability Scale," [Online]. Available: <http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>.
- [14] Sourcefire, "Open source network intrusion prevention and detection system (IDS/IPS)," [Online]. Available: <http://www.snort.org>.
- [15] Openwall, "John the Ripper password cracker," [Online]. Available: <http://www.openwall.com/john/>.
- [16] S. Van den Berg, "Welcome to procmail.org," [Online]. Available: <http://www.procmail.org/>.
- [17] S. Research, "Secure Internet Management and SNMP," [Online]. Available: <http://www.snmp.com/>.

## **Appendix F. Cuestionario sobre Factores críticos de privacidad**

A continuación de se presenta el cuestionario utilizado en el apartado:

### **3.2.4 Factores críticos de privacidad e interfaz**

## Privacidad de la información en Internet

En la Facultad de Tecnologías de Información se está realizando un proyecto de investigación sobre la cultura actual de los alumnos de nivel licenciatura de la UPAEP en el tema de la privacidad de la información de los usuarios de Internet. Esta encuesta será de utilidad para dicho proyecto. Los datos que se obtengan serán usados únicamente para fines estadísticos sobre esta investigación. Agradecemos su tiempo y le pedimos que conteste todas y cada una de las preguntas con veracidad de acuerdo a su criterio.

Semestre:

|   |   |   |   |   |   |   |   |   |    |          |
|---|---|---|---|---|---|---|---|---|----|----------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 o más |
|---|---|---|---|---|---|---|---|---|----|----------|

Carrera: \_\_\_\_\_

Edad:

|       |    |    |    |    |    |    |    |    |    |     |
|-------|----|----|----|----|----|----|----|----|----|-----|
| Menos | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | Más |
|-------|----|----|----|----|----|----|----|----|----|-----|

Género:

|        |       |
|--------|-------|
| Hombre | Mujer |
|--------|-------|

1. Para navegar en internet utilizo mayormente: (seleccione las que aplique)

|                                  |        |                  |       |
|----------------------------------|--------|------------------|-------|
| <b>Laptop</b>                    | propia | prestada         | Ambas |
| <b>Computadora de escritorio</b> | propia | prestada/escuela | Ambas |
| <b>Dispositivo móvil</b>         | propio | prestado         | Ambos |

2. ¿Conoces el aviso de privacidad de la página de UPAEP? Si No Más o menos

3. ¿Sabes identificar cuáles son tus datos personales? Si No Más o menos

4. De los siguientes, ¿cuáles consideras son datos personales sensibles? (marque solo una opción)

- a) Nombre, dirección, teléfono
- b) Salario, número de tarjeta de crédito
- c) Religión, afiliaciones políticas, preferencias sexuales

5. Indica el punto que se acerca más a tu personalidad (solo uno):

- ☐ Animador, improvisador, descubridor, arriesgado y espontáneo. Prefiero hacer y experimentar.
- ☐ Prudente, precavido, investigador, recopilador, analítico y exhaustivo. Prefiero observar y reflexionar.
- ☐ Soy Metódico, lógico, objetivo, crítico y estructurado. Prefiero entender los conceptos, ideas y relaciones entre éstas.
- ☐ Impaciente, experimentador, práctico, eficaz y realista. Prefiero probar las cosas para ver su funcionalidad.

6. Con lo que sabes acerca de los Avisos de Privacidad, ¿qué tan satisfecho te sientes al respecto? (0 es sin satisfacción y 10 es satisfacción completa):

|   |   |   |   |   |   |   |   |   |   |    |
|---|---|---|---|---|---|---|---|---|---|----|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|----|

**Para mantener la privacidad de mis datos personales cuando navego en cualquier PÁGINA DE INTERNET es importante:**

|                                                                                                                                            | Nada importante | Muy Poco importante | Poco Importante | Indiferente | Importante | Muy importante | Extremadamente importante |
|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---------------------|-----------------|-------------|------------|----------------|---------------------------|
| Identificar la identidad y domicilio del responsable que los recaba                                                                        |                 |                     |                 |             |            |                |                           |
| Saber para qué los van a usar                                                                                                              |                 |                     |                 |             |            |                |                           |
| Identificar las opciones que me ofrece el responsable de almacenarlos para que yo limite su uso o divulgación a otras personas             |                 |                     |                 |             |            |                |                           |
| Reconocer los medios que me ofrecen para que pueda acceder, rectificar, cancelar u oponerme a otro uso de mis datos                        |                 |                     |                 |             |            |                |                           |
| Saber si harán transferencias de mis datos a otras personas                                                                                |                 |                     |                 |             |            |                |                           |
| Identificar la forma en que el responsable de almacenar mis datos me comunicará si hay cambios sobre las políticas de privacidad del sitio |                 |                     |                 |             |            |                |                           |
| Saber lo que es un Aviso de privacidad                                                                                                     |                 |                     |                 |             |            |                |                           |
| Leer completamente el Aviso de privacidad                                                                                                  |                 |                     |                 |             |            |                |                           |
| Que el Aviso de privacidad sea breve para motivarme a leerlo                                                                               |                 |                     |                 |             |            |                |                           |
| Que el Aviso de privacidad sea tan extenso como sea necesario para que no queden dudas                                                     |                 |                     |                 |             |            |                |                           |
| Que el aviso de privacidad se presente en un formato ameno                                                                                 |                 |                     |                 |             |            |                |                           |
| Que el aviso de privacidad se presente en un lenguaje coloquial                                                                            |                 |                     |                 |             |            |                |                           |
| Cuando capturo mis datos personales me alerten sobre posibles riesgos                                                                      |                 |                     |                 |             |            |                |                           |
| Que el aviso de privacidad se presente en un lenguaje estrictamente legal                                                                  |                 |                     |                 |             |            |                |                           |
| Que los medios masivos de comunicación divulguen temas relacionados                                                                        |                 |                     |                 |             |            |                |                           |
| Tener capacitación y cursos sobre este tema                                                                                                |                 |                     |                 |             |            |                |                           |