

ESPINOSA

**MARCO DE REFERENCIA DE CIBERSEGURIDAD PARA
INFRAESTRUCTURA DE IOT USANDO LA TECNOLOGÍA DE IDS**

**CIP
UPAEP
2022**



Universidad Popular Autónoma del Estado de Puebla
Centro Interdisciplinario de Posgrados
Investigación y Consultoría
Departamento de Ingeniería
Doctorado en Planeación Estratégica y Dirección
de Tecnología

**Marco de referencia de ciberseguridad para
infraestructura de IoT usando la tecnología de IDS**

Tesis que para obtener el grado de
Doctor en Planeación Estratégica y Dirección de Tecnología

Presenta

Carmen Beatriz Espinosa Garrido

Puebla, México

Julio, 2022



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.



Universidad Popular Autónoma del Estado de Puebla
Vicerrectoría de Investigación y Posgrados
Decanato de Ingeniería y Negocios
Departamento de Ingeniería y Tecnologías de la Información
Doctorado en Planeación Estratégica y Dirección de Tecnología

MARCO DE REFERENCIA DE CIBERSEGURIDAD PARA INFRAESTRUCTURA DE IOT USANDO LA TECNOLOGÍA DE IDS

Tesis que para obtener el Grado de
Doctor en Planeación Estratégica y Dirección de Tecnología

Presenta:

MTRA. CARMEN BEATRIZ ESPINOSA GARRIDO

Director de Tesis:

Dr. Luis Rosales Roldán

Puebla, México

07 julio 2022



Universidad Popular Autónoma del Estado de Puebla
Decanato de Ingeniería
Doctorado en Planeación Estratégica
y Dirección de Tecnología

Se aprueba la Tesis:

**MARCO DE REFERENCIA DE CIBERSEGURIDAD PARA
INFRAESTRUCTURA DE IOT USANDO LA TECNOLOGÍA DE IDS**

Alumna
CARMEN BEATRIZ ESPINOSA GARRIDO

Comité Asesor

Dr. Luis Rosales Roldán
Director de Tesis

Dra. Alejandra Aldrette Malacara
Asesor 1

Dr. José María Enrique Bedolla Cordero
Asesor 2

Dra. Argelia Fabiola Miranda Pérez
Asesor 3

Dr. Juan Carlos Pérez García
Asesor 4

Puebla, México.

07 de julio de 2022.

Agradecimientos

Agradecimiento al Dr. Luis Rosales Roldán por su tiempo y apoyo para dirigir esta tesis. También agradezco a todos los Doctores docentes que me compartieron su conocimiento y sus experiencias durante el programa del doctorado de PE y DT y a la Universidad Popular Autónoma del Estado de Puebla por propiciar un entorno favorable que ha guiado mi aprendizaje y mi educación.

Agradezco especialmente a mi hija Diana por ser inspiración, a mi esposo Iván, a mi mamá Georgina, a mi papá Arturo y a mi hermano Arturo por su tiempo y comprensión durante todo este proceso.

DEDICATORIA

Dedicado a mi hija Diana, para que el conocimiento y el aprendizaje sean pilares en su vida.

Índice General

AGRADECIMIENTOS	I
DEDICATORIA	II
ÍNDICE GENERAL	III
ÍNDICE DE TABLAS	VIII
ÍNDICE DE FIGURAS	IX
LISTA DE ABREVIATURAS	XI
RESUMEN	I
INTRODUCCIÓN	1
1.1. JUSTIFICACIÓN	1
1.2. OBJETIVO GENERAL	1
1.3. OBJETIVOS ESPECÍFICO	2
1.4. PREGUNTA DE INVESTIGACIÓN	2
1.5. ALCANCES Y LIMITACIONES	2
1.6. VIABILIDAD DEL PROYECTO	3
1.7. CONTRIBUCIONES GENERALES ESPERADAS	3
1.8. IMPACTO SOCIAL ESPERADO	4
CAPÍTULO 2 PLANTEAMIENTO DEL PROBLEMA	5
CAPÍTULO 3 ESTADO DEL ARTE	9

CAPÍTULO 4 MARCO TEÓRICO	17
4.1 INTERNET DE LAS COSAS	17
4.2 CIBERSEGURIDAD EN IoT	19
4.3 ESTÁNDARES DE SEGURIDAD DE IT	20
4.3.1 MODELO DE MADUREZ DE CAPACIDAD DE CIBERSEGURIDAD	21
4.3.2 MARCO DE REFERENCIA NIST	21
4.3.3 ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN	23
4.3.3.1 <i>ISO/IEC 27002</i>	23
4.3.3.2 <i>ISO/IEC 27001/2013</i>	24
4.3.3.3 <i>ISO/IEC 27035</i>	24
4.3.4 MATRIZ MITRE ATT&CK	25
4.3.5 MODELO CORE COBIT 2019	25
4.3.6 ESTÁNDAR DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	26
4.3.7 OCTAVE	26
4.3.8 MARCO DE SEGURIDAD LUBUA	27
4.4 PROTOCOLOS DE APLICACIÓN	27
4.4.1 PROTOCOLO TLS	27
4.4.2 PROTOCOLO MQTT	28
4.4.2.1 <i>SEGURIDAD DE MQTT</i>	28
4.4.2.2 <i>VULNERABILIDADES DE MQTT</i>	29
4.5 ARQUITECTURA DE RED DE IoT	30
4.6 SISTEMA DE DETECCIÓN DE INTRUSOS	31
4.6.1 ANÁLISIS COMPARATIVO DE IDS	32
4.6.2 CIBERATAQUES CONTRA IDS	33

4.6.2.1 ATAQUES ADVERSARIOS DE APRENDIZAJE DE MÁQUINA DE IDS	33
---	-----------

5 METODOLOGÍA	37
----------------------	-----------

5.1 ANÁLISIS COMPARATIVO DE MODELOS DE SEGURIDAD	38
---	-----------

6 MARCO DE REFERENCIA DE SEGURIDAD PARA DISPOSITIVOS IOT, MARCIOT	42
--	-----------

6.1 Estructura de MaRCIoT	43
---------------------------	----

6.1.1 ESTABLECER DIRECCIÓN	43
----------------------------	----

6.1.2 ADMINISTRACIÓN DE ACTIVOS DE LA INFORMACIÓN	43
---	----

6.1.2.1 <i>Desarrollo de perfil de activos de la información</i>	43
--	----

6.1.2.2 <i>Identificar los contenedores de los activos de la información</i>	43
--	----

6.1.3 POLÍTICAS Y PROCEDIMIENTOS	44
----------------------------------	----

6.1.3.1 <i>Términos y definiciones</i>	44
--	----

6.1.3.2 <i>Organización de la seguridad de la información</i>	44
---	----

6.1.3.3 <i>Procedimientos y procesos de protección de información</i>	44
---	----

6.1.4 PROTEGER OPERACIÓN	44
--------------------------	----

6.1.4.1 <i>Operación de activos</i>	44
-------------------------------------	----

6.1.4.2 <i>Operación de recursos humanos</i>	45
--	----

6.1.5 IDENTIFICAR AMENAZAS	45
----------------------------	----

6.1.5.1 <i>Detectar áreas de preocupación</i>	45
---	----

6.1.5.2 <i>Definir los escenarios de amenaza</i>	45
--	----

6.1.5.3 <i>Investigación de escritorio sobre guías de seguridad</i>	46
---	----

6.1.5.4 <i>Cuestionario de ciberseguridad de IoT</i>	47
--	----

6.1.5.5 <i>Taller con los especialistas y desarrolladores de IoT</i>	47
--	----

6.1.5.6 <i>Pruebas de seguridad</i>	47
-------------------------------------	----

6.1.5.7	<i>Generar reporte</i>	47
6.1.6	MITIGACIÓN DE AMENAZAS	48
6.1.6.1	<i>Identificar riesgos</i>	48
6.1.6.2	<i>Análisis de riesgos</i>	48
6.1.6.3	<i>Seleccionar la mitigación</i>	48
6.1.6.3.1	<i>Detección de Intrusos</i>	48
6.1.7	CUMPLIMIENTO	50
6.1.7.1	<i>Evaluación</i>	50
6.2	OPERACIÓN DEL MARCIoT	50
6.3	POLÍTICAS Y PROCEDIMIENTOS DEL MARCIoT	52
6.3.1	PROCEDIMIENTOS Y PROCESOS DE PROTECCIÓN DE INFORMACIÓN DE MARCIoT	52
6.4	PROTEGER OPERACIÓN DE MARCIoT	53
6.4.1	DIAGRAMA DE RED DE MARCIoT	57
6.4.2	FLUJO DE OPERACIONAL DE MARCIoT	59
6.4.3	ANÁLISIS DEL TRÁFICO NORMAL A TRAVÉS DE WIRESHARK	60
6.4.4	INSPECCIÓN DEL TRÁFICO UTILIZANDO IDS EN LA PLATAFORMA SURICATA	62
6.5	IDENTIFICAR AMENAZAS	64
6.5.1	SIMULACIÓN DE ATAQUES DE CIBERSEGURIDAD	65
6.7.3	ANÁLISIS DEL TRÁFICO A TRAVÉS DE WIRESHARK	67
6.7.4	ANÁLISIS DEL TRÁFICO A TRAVÉS DE IDS SURICATA	70
6.7.5	REVISIÓN DE VULNERABILIDADES DE CVE	70
6.7.6	REVISIÓN DE VULNERABILIDADES MATRIZ MITRE ATT&CK ICS	72
7	RESULTADOS	74

7.1	VALIDACIÓN DEL MARCO DE SEGURIDAD DE INFRAESTRUCTURA DE IOT	74
7.2	ANÁLISIS DE DATOS	77
8	CONCLUSIONES / TRABAJOS FUTUROS	80
	REFERENCIAS	83
8	ANEXO A	90
9	ANEXO B	97
10	ANEXO C	102

Índice de Tablas

TABLA 4.1 DEFINICIÓN DEL TÉRMINO DE “INTERNET DE LAS COSAS”	18
TABLA 4.2 DEFINICIÓN DE “SEGURIDAD EN IoT”	20
TABLA 4.3 MARCO DE REFERENCIA NIST CSF	22
TABLA 5.1 ANÁLISIS COMPARATIVO DE LOS MARCOS DE CIBERSEGURIDAD	38
TABLA 5.2 PROCESO DE CODIFICACIÓN DE LOS MARCOS DE SEGURIDAD	40
TABLA 5.3 ANÁLISIS COMPARATIVO ENTRE LOS MARCOS DE REFERENCIA	41
TABLA 6.1 BASE DE DATOS DE MITRE ATT&CK ICS	46
TABLA 6.2 DIRECCIONES IP ASIGNADAS EN MODELO DE CIBERSEGURIDAD DE IoT PARA LAS PRUEBAS	58
TABLA 6.3 COMUNICACIÓN DESTINO PARA PLATAFORMA DE IoT DE ARDUINO OPLÀ	61
TABLA 6.4 REGLAS PREDETERMINADAS DE MQTT EN SURICATA	65
TABLA 6.5 CANTIDAD DE VULNERABILIDADES CVE® MQTT EN HERRAMIENTAS IoT	71
TABLA 6.6 VULNERABILIDADES DE CVE RELACIONADAS A MQTT (CVE - SEARCH RESULTS, 2022)	71
TABLA 6.7 CANTIDAD DE VULNERABILIDADES CVE® MQTT QUE AFECTA LA CONFIDENCIALIDAD DE DATOS EN IoT	72
TABLA 6.8 CANTIDAD DE VULNERABILIDADES CVE® MQTT QUE AFECTA LA DISPONIBILIDAD DE DATOS EN IoT) ..	72
TABLA 6.9 MATRIZ MITRE ATT&CK ICS (MATRIX MITRE ATT&CK®, 2022)	73
TABLA 7.1 CUESTIONARIO DE VALIDEZ DE MARCO DE REFERENCIA DE SEGURIDAD DE INFRAESTRUCTURA DE IoT USANDO LA TECNOLOGÍA IDS. PREGUNTAS GENERALES.	75
TABLA 7.2 CUESTIONARIO DE VALIDEZ DE MARCO DE REFERENCIA DE SEGURIDAD DE INFRAESTRUCTURA DE IoT USANDO LA TECNOLOGÍA IDS. PREGUNTAS ACERCA DEL MARCO DE REFERENCIA DE SEGURIDAD	76
TABLA 7.3 MATRIZ DE CORRELACIÓN DEL COEFICIENTE ALFA DE CRONBACH	77
TABLA 7.4 ESTADÍSTICA DE LAS CATEGORÍAS DEL MARCO DE REFERENCIA DE CIBERSEGURIDAD	77
TABLA A.1 FORMATO PARA ALCANCE DE LA ESTRATEGIA. IMPACTO DE LOS CIBERATAQUES EN LA ESTRATEGIA DE LA ORGANIZACIÓN.	90
TABLA A.2 PERFIL DE ACTIVOS	91
TABLA A.3 FORMATO DE RIESGOS DE ACTIVOS DE INFORMACIÓN.	91
TABLA A.4 CUESTIONARIO DE AFECTACIÓN DE LA TRIADA DE SEGURIDAD EN UN ACTIVO DE INFORMACIÓN.	92
TABLA A.5 CUESTIONARIO DE EVALUACIÓN DE CIBERSEGURIDAD	92
TABLA C.1 VULNERABILIDADES DE CVE ® (CVE - SEARCH RESULTS, 2022)	102

Índice de Figuras

FIGURA 4.1 MARCO DE REFERENCIA ISO/IEC 27001:2013	25
FIGURA 4.2 <i>ARQUITECTURA DE RED</i>	30
FIGURA 4.3 <i>EVALUACIÓN NIDS</i>	31
FIGURA 5.1 METODOLOGÍA DE LA INVESTIGACIÓN	37
FIGURA 6.1 MARCO DE REFERENCIA DE SEGURIDAD PARA IoT UTILIZANDO IDS. ELABORACIÓN PROPIA.....	42
FIGURA 6.2 MODO DE OPERACIÓN DE MARCIoT (ELABORACIÓN PROPIA).....	52
FIGURA 6.3 ARQUITECTURA DE MARCIoT PARA LAS PRUEBAS	53
FIGURA 6.4 PLATAFORMA DE LA NUBE DE IoT PARA RECOLECCIÓN DE DATOS DEL SENSOR	53
FIGURA 6.5 FIREWALL QUE PERTENECE A LA CAPA DE RED	54
FIGURA 6.6 MÁQUINA VIRTUAL PARA IDS.....	55
FIGURA 6.7 IDS EN PLATAFORMA SURICATA	55
FIGURA 6.8 PUNTO DE ACCESO PARA RED INALÁMBRICA.....	56
FIGURA 6.9 SWITCH CON PUERTO EN MODO “ESPEJO”	56
FIGURA 6.10 ROUTER PARA CONEXIÓN HACIA INTERNET	56
FIGURA 6.11 <i>DISPOSITIVO SENSOR DE ARDINO OPLA</i>	57
FIGURA 6.12 DIAGRAMA DE RED DEL MODELO DE CIBERSEGURIDAD DE IoT.....	58
FIGURA 6.13 DIAGRAMA OPERACIÓN DE LAS PRUEBAS DEL MODELO DE CIBERSEGURIDAD DE IoT, MARCIoT	59
FIGURA 6.14 COMUNICACIÓN ENTRE EL SENSOR Y PLATAFORMA IoT	60
FIGURA 6.15 PROTOCOLO DE APLICACIÓN DE DATOS.....	61
FIGURA 6.16 CANTIDAD DE TRÁFICO, PROTOCOLO TLS	61
FIGURA 6.17 <i>ESTRUCTURA DE SURICATA 6.0.5</i>	62
FIGURA 6.18 ANÁLISIS DE TRÁFICO CON SURICATA.....	63
FIGURA 6.19 REGISTRO DE LA INSPECCIÓN DE SURICATA	63
FIGURA 6.20 ALERTAS DE TRÁFICO.....	64
FIGURA 6.21 BÚSQUEDA DE CONTRASEÑA CON HERRAMIENTA HYDRA.	65
FIGURA 6.22 ESCANEADO DE PUERTOS EN LOS SENSORES DE ARDUINO.	66
FIGURA 6.23 ESCANEADO DE PUERTOS EN LOS SENSORES DE ARDUINO.	66
FIGURA 6.24 ATAQUE DoS A LOS SENSORES DE ARDUINO POR EL PUERTO 80	67
FIGURA 6.25 ATAQUE DoS A LOS SENSORES DE ARDUINO POR EL PUERTO 8443	67
FIGURA 6.26 ESCANEADO DE PUERTOS DE RED A LOS SENSORES ARDUINO. PAQUETES/SEGUNDO.....	68
FIGURA 6.27 ESCANEADO DE PUERTOS DE RED A LOS SENSORES ARDUINO. BYTES/SEGUNDO.....	68
FIGURA 6.28 ATAQUE DoS A LOS SENSORES ARDUINO. PAQUETES/SEGUNDO.	68
FIGURA 6.29 ATAQUE DoS A LOS SENSORES ARDUINO. BYTES/SEGUNDOS.....	69
FIGURA 6.30 ATAQUE DoS A LOS SENSORES ARDUINO. DETALLE PAQUETE.	69

FIGURA 6.31 ATAQUE DoS A LOS SENSORES ARDUINO. PAQUETES MASIVOS ENVIADOS EN ESTADO SYN.	69
FIGURA 6.32 ALERTA DE POSIBLE ATAQUE DoS EN IDS SURICATA	70
FIGURA B.1. <i>AUTORIDAD RESPONSABLE</i>	97
FIGURA B.2 ESTRATEGIA APEGADA AL NEGOCIO	97
FIGURA B.3 GESTIÓN DE ACTIVOS DE INFORMACIÓN	97
FIGURA B.4 <i>GLOSARIO DE TÉRMINOS Y DEFINICIONES</i>	97
FIGURA B.5 FORMALIZAR POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE DATOS	98
FIGURA B.6 COMUNICAR POLÍTICAS DE SEGURIDAD	98
FIGURA B.7 GUÍA ORAL, APARTE DE LA POLÍTICA PRINCIPAL	98
FIGURA B.8 PROCEDIMIENTOS EN CASOS EMERGENTES	98
FIGURA B.9 IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD	99
FIGURA B.10 INVESTIGACIÓN DE ESCRITORIO	99
FIGURA B.11 CUESTIONARIO DE ESPECIALISTAS.....	99
FIGURA B.12 COLABORACIÓN ABIERTA CON LOS USUARIOS FINALES	99
FIGURA B.13 IMPORTANCIA DE RIESGOS DE SEGURIDAD DE INFORMACIÓN	100
FIGURA B.14 MITIGAR O ACEPTAR RIESGOS	100
FIGURA B.15 SISTEMAS DE DETECCIÓN DE INTRUSOS EN IoT	100
FIGURA B.16 GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE INFORMACIÓN	100
FIGURA B.17 FORMALIZAR Y COMUNICAR PLAN DE COMUNICACIÓN.....	101

Lista de Abreviaturas

Inglés

3G	Third generation wireless
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AP	Access Point
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
COBIT	Control Objectives for Information and Related Technologies
CTD	Cyber Threat Dictionary
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of service
DSL	Digital subscriber line
DTLS	Datagram Transport Layer Security
ETSI	European Telecommunications Standards Institute
FGSM	Fast Gradient Sign Method
FL	Federated Learning
FTP	File Transfer Protocol

FNN	Feed-forward Neural Network
GAN	Generative Adversarial Networks
HIP	Host Identity Protocol
HTTP	Hypertext Transfer Protocol
IA	Inteligencia Artificial
ICMP	Internet Control Message Protocol
IDMEF	Intrusion Detection Message Exchange Format
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISA	International Society of Automation
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
JSMA	Jacobian Based Saliency Map Attack
LTE	Long-Term Evolution
Mbs	Megabit per second
MDSEA	Model-Driven Service Engineering Architecture
MQTT	Message Queue Telemetry Transport
NCSA	Next Generation Cyber Security Architecture

NFS	Network File System
NFV	Network Function Virtualization
NIDS	Network Intrusion Detection System
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NMAP	Network Mapper
NTP	Network Time Protocol
OASIS	Open Artwork System Interchange Standard
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security
PGD	Project Gradient Descent
SDN	Software Defined Networking
SIP	Session Initiation Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNN	Self-normalizing Neural Network
SSH	Secure Shell Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WiMAX	Worldwide Interoperability for Microwave

Español

CICIC Complejidad, Informática y Cibernética

IoC Internet de las Cosas

TI Tecnologías de la Información

PyME Pequeña y Mediana Empresa

RESUMEN

El Internet de las Cosas es una tecnología que está en apogeo porque permite recolectar datos personales y organizaciones para tomar decisiones y para mejorar procesos de automatización, entre otros. Sin embargo, tiene una ciberseguridad endeble que es causada por cuestiones técnicas o porque aún no se tiene marcos de referencia o herramientas de red enfocadas al Internet de las Cosas. En la presente tesis se describe la situación actual del Internet de las Cosas, la ciberseguridad y los Sistemas de Detección de Intrusos. Se identifica la problemática de la ciberseguridad del Internet de las Cosas, ciberseguridad y Sistemas de Detección de Intrusos. Basados en la revisión literaria se seleccionan los marcos de referencia, NIST CSF, ISO/IEC 27002, OCTAVE Allegro, ISA/IEC 62443 y marco de referencia de Lubua para generar un marco de referencia de ciberseguridad a través de un análisis comparativo. A lo que se genera un marco de referencia de ciberseguridad de IoT, llamada MaRCIoT, que está compuesta por las categorías Establecer el alcance, Administración de activos de información, Políticas y procedimientos, Proteger operación, Identificar amenazas, Mitigar amenazas y Cumplimiento. El MaRCIoT es validado a través de encuestas realizados a especialistas de IT. Después se generan pruebas de las categorías Políticas y procedimientos, Proteger operación, Identificar amenazas, donde se simulan ciberataques a una infraestructura controlada de IoT que utiliza un Sistema de Detección de Intrusos. A través del MaRCIoT se pueden detectar los ciberataques, siendo que es un marco de referencia de ciberseguridad de IoT y que considera la misión y visión de la organización, la gestión de activos de información, políticas y procedimientos, medidas de protección de operación, el cómo identificar y mitigar las ciber amenazas, para finalmente hacer evaluaciones de manera recurrente.

Introducción

1.1. Justificación

Las tendencias de mercado anticipan un crecimiento de billones de dispositivos IoT conectados en las siguientes décadas; que están respondiendo y comunicándose con personas, con el ambiente y entre ellos; los reportes de Machina Research estiman un crecimiento aproximado de 7.2 billones de dispositivos electrónicos conectados globalmente en 2023 (Castillo & Thierer, 2015). No obstante, al ser una tecnología emergente se manifiestan hallazgos de seguridad tanto en las políticas, estándares y en el ámbito tecnológico (Bauer et al., 2017) . Siendo parte indispensable proteger los dispositivos de IoT para que cumplan con disponibilidad, integridad y confidencialidad de los datos que procesan y transfieren, de no hacerlo una organización puede ser objeto de robo de información y de actos perjudiciales en sus servicios críticos (de Bruijn & Janssen, 2017) .

Por lo que es relevante proteger la infraestructura de IoT, considerando la confidencialidad, integridad y disponibilidad de la información en las capas de la arquitectura, para lo que se propone la revisión de los marcos de referencia existentes de ciberseguridad para IoT, con el fin de generar un marco de referencia con mejoras que evite la substracción de información sensible del negocio e impida algún impacto económico o de reputación del negocio.

1.2. Objetivo General

Proponer un marco de referencia validado para ciberseguridad de IoT usando la tecnología de IDS para proteger contra los ciberataques que atacan la integridad, confidencialidad y disponibilidad.

1.3. Objetivos Específico

- Revisar literatura de los marcos de referencia de ciberseguridad ya existentes para infraestructura de IoT.
- Analizar comparativamente de los marcos de referencia de seguridad de IoT, su enfoque, estructura y funciones.
- Desarrollar el marco de referencia propuesto para ciberseguridad de IoT utilizando IDS.
- Validar el marco de referencia a través de encuesta a los especialistas de seguridad.

1.4. Pregunta de Investigación

¿Las categorías de un marco de referencia de seguridad propiciarán una mayor protección contra ciberataques para una infraestructura de IoT?

La hipótesis de investigación establecerá una relación de causalidad bi-variada. Siendo la variable independiente las categorías del marco de referencia de seguridad y la variable dependiente la protección contra ciberataques en una infraestructura de IoT

Hi: Las categorías de un marco de referencia de seguridad para infraestructura de IoT, asegurarán una mayor protección contra ciberataques en una infraestructura de IoT

1.5. Alcances y limitaciones

La investigación es cuantitativa con un alcance descriptivo, tomando como fenómeno de estudio la seguridad para infraestructura de IoT, considerando los componentes de seguridad y evaluando un marco de referencia de ciberseguridad. El marco de ciberseguridad de IoT propuesto estará contrarrestando faltas de los estándares y marcos de referencia existentes. La evaluación del marco de referencia se hará a través de una simulación con herramientas de código abierto por

cuestión de presupuesto. Para la defensa de la infraestructura de IoT se utilizará un IDS Suricata por su procesamiento de multi-hilo y por su mayor tasa de detección en comparación con Snort (Park & Ahn, 2017). Para representar los ciberataques se manipulará la herramienta Kali Linux.

1.6. Viabilidad del proyecto

El tiempo planeado para la presente investigación es de aproximadamente dos años, contemplando la generación de la introducción, la revisión de la literatura para el marco teórico y el estado del arte, seguimiento de la metodología, colaboración con especialistas de TI, análisis de datos, validación del marco de referencia propuesto, simulación de ciberataques a la infraestructura controlada de IoT, exploración de resultados y generación de conclusiones. Esta investigación se llevará a cabo teniendo como fuente de información la revisión de la literatura y datos de colaboradores de TI. Para la revisión de literatura se tiene acceso a bases de datos como EBSCO, Elsevier y Biblioteca UPAEP. La validación del marco de referencia se hará a través de encuestas a especialistas de TI y simulando ciber ataques de seguridad en una infraestructura de prueba de servicios de IoT. Se cuenta con presupuesto para los recursos de hardware, como son computadoras con capacidad de procesamiento y memoria y dispositivos IoT.

1.7. Contribuciones generales esperadas

Las contribuciones originales esperadas de esta investigación es contar con un marco de referencia que pueda ser utilizado en cualquier empresa de servicios de IoT, de manera que cuente con los lineamientos basados en la revisión literaria y la validación de los especialistas de TI. El contenido de esta investigación ha sido presentado durante el Décima Segunda Conferencia Iberoamericana de Complejidad, Informática y Cibernética (CICIC 2022) y el artículo está publicado en las memorias de este.

1.8. Impacto social esperado

Los dispositivos de IoT tienen un incremento en su prevalencia y recolectan una gran cantidad de información, sin embargo, tienen riesgos asociados a la seguridad, como son que personal no autorizado acceda a sistemas productivos, obtenga y use información confidencial, o que incluso comprometa la seguridad física. De tener accesos no autorizados, los atacantes podrían conocer la geolocalización, número de cuentas financieras, información de valor comercial, entre otros (Smith, 2014). Con el marco de referencia de seguridad propuesto se cubrirían deficiencias de marcos de referencia existentes, aumentando la tasa de detección de eventos y por lo tanto disminuyendo la probabilidad de que datos sensibles del negocio acaben en propiedad de personal no autorizado y que tengan un uso inapropiado o ilegal. De este modo, las empresas con infraestructura de IoT tendrían confianza de que su información crítica está siendo protegida e incrementarían el valor económico de sus servicios (Radanliev et al., 2018).

Capítulo 2 Planteamiento del problema

El Internet de las Cosas (en inglés, Internet of Things) es un nuevo paradigma, que conecta equipos heterogéneos en una infraestructura no centralizada, con un tráfico y almacenamiento masivo; se estima que en el 2020 habría 20.4 billones de estos dispositivos a nivel global, incluyendo en las categorías más comunes a sensores para la industria de salud, de automóviles, del deporte, dispositivos de casa, entre otros (Smith, 2014). Su arquitectura básica se conforma por tres capas: percepción, red y aplicación; siendo la primera la que procesa energía y almacena datos, la segunda la que transmite la información y la última la que da el servicio e interactúa con el usuario (El-hajj et al., 2019). En la construcción del IoT debe integrarse una administración confiable y principios de seguridad (Čolaković & Hadžialić, 2018). Refiriéndose estos últimos a la confidencialidad, integridad y disponibilidad de los sistemas; para asegurar que la información sea accedida solo por personal autorizado, que no sea modificada por ninguna entidad no autorizada y que esté a disposición del negocio en cualquier momento (Srinivas et al., 2019).

A pesar de las estandarizaciones, alianzas e investigaciones para el IoT, se continúa con una seguridad endeble, lo que lo limita a alcanzar su potencial máximo; se detectan debilidades en la privacidad, en cuanto a autenticación y autorización de los dispositivos, al igual que en la encriptación del transporte e interfaz para web/software/firmware; para lo que se recomiendan políticas de seguridad e implementación de protocolos seguros (Čolaković & Hadžialić, 2018). De modo similar, (Safkhani & Shariat, 2018) revelan debilidades de autenticación en los protocolos de IoT en diferentes aplicaciones, recomendando el cómo mejorarlos.

(Bauer et al., 2017) indican que la industria en general tiene preocupación de mantener la seguridad de inicio a fin en la red IoT, sin embargo, los administradores no tienen detectados

riesgos de ciberseguridad relacionados con la automatización, no tienen un plan de respuesta o medidas necesarias contra los ataques externos de seguridad. Seguidamente, (Pan & Yang, 2018) mencionan que los desafíos de ciberseguridad para IoT son el número masivo de dispositivos con capacidades limitadas y que son vulnerables a amenazas, la integración con tecnologías emergentes como Virtualización de Funciones de Red (en inglés, Network Function Virtualization) y Redes Definidas de Software (en inglés, Software Defined Networking), la cantidad y velocidad del almacenamiento de datos, la colaboración y la conexión unidireccional de los equipos; por lo que sugieren de manera teórica hacer transacciones de datos con la tecnología de cadena de bloques, usar la inteligencia artificial, emplear métodos y algoritmos ligeros, implementar técnicas de protección activas e implementar llaves encriptadas entre los dispositivos.

(Chatfield & Reddick, 2019) resaltan que en IoT se tiene falta de visibilidad y consciencia pública para protegerse de amenazas por sus diferencias con otras tecnologías, además que indican que se prioriza la disponibilidad, luego la integridad y finalmente la confidencialidad; para lo que desarrollan un marco de referencia teórico con políticas de ciberseguridad y de tecnología de IoT para identificar oportunidades de negocio, crear valor en una empresa e influir en un gobierno estratégico. De manera similar (Matheu-García et al., 2019) indican que la metodología de certificación de seguridad de IoT tiene un reto de seguridad por la heterogeneidad de dispositivos y que se debe identificar los ataques, a lo que proponen un marco de referencia basado en estándares del Instituto Europeo de Estándares de Telecomunicaciones (en inglés, European Telecommunications Standards Institute) y en los de la Organización Internacional de Estándares (en inglés, International Organization for Standardization), sin embargo no resuelve el problema de privacidad y de riesgos.

La seguridad en IoT tiene un impacto económico porque se trata de conexiones de dispositivos en sistemas de manufactura, de transporte, de banca electrónica; para lo que (Radanliev et al., 2018) crean un modelo de evaluación de impacto de riesgos de IoT en la industria 4.0 para entender el efecto económico. Sin embargo, por no poseer datos específicos para riesgos de IoT no pueden realizar una valuación confiable de los riesgos cibernéticos asociados.

Los hallazgos de seguridad detectados en trabajos previos le dan la posibilidad a personal no autorizado de monitorear, identificar, acceder y controlar los dispositivos de IoT, obteniendo información sensible del negocio (Smith, 2014). Para estos eventos de seguridad (Lu & Xu, 2019) sugieren una taxonomía, donde clasifican las amenazas para equipos, ubicación, nivel de acceso, información, estrategias, protocolos, capas, coacción a anfitrión y ofensas mayores; si a través de estos ataques existe fuga de información puede haber un impacto negativo en las empresas y en las personas, porque se trata de datos como los de la bolsa de valores, registros financieros, médicos, personales, entre otros.

En cuanto a los modelos de seguridad y de maduración de ciberseguridad (Yigit Ozkan & Spruit, 2019) indican que son complejos y que no son sencillos de implementar para una autoevaluación, no son adecuados para desarrollar planes personalizados y no consideran características organizacionales. (Frayssinet Delgado et al., 2021) comenta que en general no se cuenta con una metodología para detección de incidentes en instituciones de gobierno y los ciudadanos quedan expuestos. Cuando los estándares y metodologías para proteger la tecnología no son respetadas o mal manejadas, se pueden ocasionar brechas de seguridad que comprometen los pilares de la ciberseguridad.

A pesar de las investigaciones de seguridad de IoT se identifican debilidades en la privacidad de datos, en la autenticación y autorización de los dispositivos, en la encriptación del transporte de datos (Čolaković & Hadžialić, 2018) , en la autenticación en los protocolos de IoT (Safkhani & Shariat, 2018), en aplicaciones automatizadas de IoT (Bauer et al., 2017) y en dispositivos con capacidades limitadas (Pan & Yang, 2018). No hay un plan de respuesta contra los ataques externos de seguridad y se carece de visibilidad para protegerse de amenazas (Chatfield & Reddick, 2019), no se tiene un marco de referencia que integre todos los estándares y tecnologías en la infraestructura de IoT. (Prokofiev et al., 2017) detectan que el problema principal de la ciberseguridad de IoT son los dispositivos. (Frayssinet Delgado et al., 2021) comenta que en general no se tiene una metodología para detectar incidentes de seguridad en instituciones de gobierno. Por lo que el presente documento propone un marco de referencia de seguridad para infraestructura de IoT utilizando IDS (en inglés, Intrusion Detection System), que contemple la integración de gestión de políticas, estándares, arquitectura, pilares de seguridad y que considere el registro de activos, la privacidad, las vulnerabilidades, análisis de amenazas, riesgos, monitoreo de tráfico y utilice tecnología de IDS; con el fin de proteger los datos de la organización y aprovechar el valor económico del negocio.

Capítulo 3 Estado del Arte

Se muestran los marcos de referencia y las soluciones técnicas que se han desarrollado con el fin de asegurar los datos en el IoT. Por una parte, (Ibrahim et al., 2018) usan el NIST CSF para evaluar la ciberseguridad de en la infraestructura de TI en una organización gubernamental y entender los riesgos que presenta. Cuantifican los riesgos y se recomiendan mejorar la administración de recursos humanos, de los procesos y de la tecnología. La información para la evaluación se obtiene a través de una herramienta de NIST CSF, que identifica la situación en curso de la organización y está basada en factores externos e internos de la gestión de riesgo, parámetros legales, requerimientos regulatorios y objetivos de la organización. En los diversos marcos de referencia el hacer una autoevaluación e implementar las políticas de seguridad puede ser complejo. Falta una herramienta flexible y accesible que refleje el contexto actual de ciberseguridad de una organización y simplifique el proceso de implementación y aceptación de los estándares de ciberseguridad.

Referente al marco de referencia NIST para ciberseguridad (Frayssinet Delgado et al., 2021) proponen el uso de una metodología para las organizaciones gubernamentales con servicios digitales. Se observa que la mayoría de las organizaciones gubernamentales no formalizan la ciberseguridad en sus sistemas de TI, no tienen estadísticas de incidencia y no hay personal entrenado. Se aplica una encuesta a 19 organizaciones gubernamentales sobre la gestión de la ciberseguridad. Resultando que el uso del marco de ciberseguridad de NIST influencia la administración de ciberseguridad en las organizaciones gubernamentales, pero no se usa por un nivel bajo de liderazgo en la implementación de medidas de seguridad. Concluye que es imposible evitar todos los ataques, por lo que debe haber un plan y preparación con métodos de detección y

prevención, con entrenamiento a las personas, procesos bien documentados y tecnología en los controles técnicos. Se recomienda adoptar la metodología de NIST para mejorar.

De manera similar (Sulistyowati et al., 2020) proponen un marco de seguridad a través de estándares para la protección de la infraestructura de TI, realizan un análisis de los estándares de seguridad NIST, ISO 27002, COBIT y PCI DSS. Comentan que la medición de un buen nivel de protección es un indicador de conciencia de ciberseguridad para el manejo de información y tecnología de comunicación, para lo que se necesita un estándar de seguridad. Hacen una planeación y dirección de un análisis comparativo con selección de variables; las variables son codificadas con base en los cuatro marcos de referencia, se relacionan para generar nuevas categorías. De los cuatro marcos de referencia, NIST, ISO 27002, COBIT y PCI DSS, se forma un nuevo marco de referencia, que consiste en 21 categorías para mejorar las capacidades de maduración. Se realizará un proceso de validación para el marco de referencia propuesto.

Ficco (2013) esboza un marco de referencia de IoT con un alcance híbrido y jerárquico para eventos de correlación con IDS, pero que no toma en cuenta las vulnerabilidades y análisis de amenazas. Alam et al (2011) propone una arquitectura en capas para IoT, con accesos seguros de dispositivos e interoperabilidad con los atributos de seguridad, pero sólo se enfoca en las fallas del control de accesos. Del mismo modo, Ekelhart et al (2009) propone un marco para manejo de riesgo de información de seguridad, pero sólo se orienta en la gestión del riesgo.

Por otro lado (N. Y. Kim et al., 2018) analizan los hallazgos de seguridad, amenazas, soluciones del sistema ciber físico de seguridad en IoT y evalúan las investigaciones existentes; resaltan las vulnerabilidades de ataques y retos de la seguridad ciber física. También recomiendan las soluciones que encaran las amenazas y discuten el cómo resolver los hallazgos futuros. A través de la revisión literaria, resulta el análisis de las soluciones para monitoreo de la operación de

sistemas, refuerzo de políticas de seguridad de hardware y software, la generación de firmas digitales en microprocesadores, asignación de llaves privadas, protección de controladores y la instalación de circuitos encriptados. Aunque se implementen estas soluciones aún se detectan puntos abiertos en la seguridad ciber física de IoT. Concluyen que se tienen trabajos limitados en el campo de seguridad ciber física (CPS). La seguridad ciber física debe de ser una preocupación constante en ambientes inteligentes de ciudades, industrias, sector de salud.

Por otro lado, (Prokofiev et al., 2017) estudian el IoT como objeto potencial de ciber ataques, detectando que el problema principal de la ciberseguridad de IoT son los dispositivos y el propósito de ganar acceso no autorizado a estos aparatos. Realizan un escaneo de dispositivos en Internet para detectar sistemas inteligentes, con el puerto 23 abierto. Detectan un listado de 396331 dispositivos de IoT que son accesibles vía Telnet, que significa que pueden ser comprometidos por una autenticación débil. Los países con más dispositivos con el puerto telnet abierto fueron China, Estados Unidos y Brasil de los 224 países examinados. Concluyen que el número actual de dispositivos conectados a Internet crece exponencialmente, pero los equipos que proveen seguridad en IoT no lo hacen a la misma velocidad y que muchos dispositivos están accesibles con sus valores de default, lo que provee a los atacantes la posibilidad de acceder a los dispositivos e incluso a atacarlos.

De manera complementaria (Ammar et al., 2018) realizan una encuesta de seguridad de los marcos de referencia principales de IoT. En cada uno se clarifica el propósito de la arquitectura, la esencia de desarrollo de aplicaciones, la compatibilidad de hardware y las funciones de seguridad. Las plataformas revisadas son AWS IoT, ARM Bed OS, Azure IoT suite, Brillo/Weave de Google, Calvin de Ericson, Homekit de Apple, Smart-things de Samsung. Estás fueron seleccionadas por la reputación de los proveedores, el desarrollo de aplicaciones y el uso del marco de referencia.

Estos marcos de referencia tienen un alcance de IoT acorde a la perspectiva y prioridades de su fabricante. A nivel hardware hay un hueco a nivel compatibilidad. A nivel de seguridad, cada marco de referencia encapsula su propia lógica de seguridad, aunque con cierta tendencia en estándares de seguridad. Son robustos e inmunes ante los ataques, sin embargo, las fallas de diseño aún exponen a los usuarios a riesgos significativos de seguridad. Concluyen que se necesita una protección física en los dispositivos IoT, asegurar la privacidad en la arquitectura y ser flexibles.

(Mozzaquatro et al., 2018) crean un marco de referencia enfocado en un tiempo de diseño, que tiene un método dinámico para los servicios de seguridad, y en un tiempo de ejecución, que involucra el monitoreo de IoT. Este marco recopila conocimiento de las alertas y eventos para descubrir nuevos datos implícitos, se integra con un método de orquestación con la Metodología de arquitectura de ingeniería de servicios basada en modelos (en inglés, Model-Driven Service Engineering Architecture) y con el estándar de Formato de intercambio de mensajes de detección de intrusiones (en inglés, Intrusion Detection Message Exchange Format). Sin embargo, aún con este marco se tienen problemas de seguridad relacionados con la tecnología IoT para 5G y entender las amenazas potenciales en el entorno cambiante.

Con otro enfoque, (Vijayakumaran et al., 2020) presentaron la Arquitectura de seguridad cibernética de próxima generación (en inglés, Next Generation Cyber Security Architecture) para aplicaciones IIoT (en inglés, Industrial Internet of Things) que protege en tiempo real la transmisión de los datos de los dispositivos al almacenamiento del servidor de la nube. Provee un nivel de seguridad a través de un mecanismo de autenticación y con una gestión de políticas de un marco de seguridad, que tiene un sistema de defensa autónoma para un ambiente de WiFi; un nuevo nodo cliente se puede convertir en miembro de la infraestructura de IoT con la identidad de un token verificado. También proponen detección en tiempo real de los ataques cuando una sesión

se establece. Dado que este marco de referencia está en la etapa inicial es necesario hacer más trabajos, en general se necesita un enfoque principal en la prevención de las amenazas de ciberseguridad, utilizando opciones como marcos de referencia con ciencia de datos y BIG DATA.

De igual manera (Kandasamy et al., 2020) investigan las vulnerabilidades de seguridad en IoT e introducen un método único de clasificación y cuantificación del riesgo para IoT. Evalúan el riesgo y marcos de referencia que están en desarrollo en las organizaciones gubernamentales. Realizan un análisis de los marcos de referencia, NIST CSF, OCTAVE, TARA, ISO/IEC 27001, ISO/IEC 30141, ISO/IEC 27030. Encontrando que el NIST no cuenta con un enfoque para IoT. Que OCTAVE desarrolla perfiles de activos de la información y administra amenazas y riesgos. TARA mejora la calidad de riesgos y evaluación de control y los estándares ISO/IEC de ciberseguridad administran riesgos y guían la seguridad y privacidad para IoT. Esto lo hacen a través de una revisión de las metodologías de evaluación de riesgos y adecuación en los sistemas IoT. Concluyen que actualmente hay una cobertura de riesgos en IoT a través de marcos de referencia, teorías de aplicación, industrias, vectores y novedades de los riesgos.

Utilizando el modelo ATT&CK (Georgiadou et al., 2021) proponen un marco de referencia de cultura de ciberseguridad, donde asocia factores culturales organizacionales e individuales, diseñado para el sector de energía, pero convive en redes de TI y operación. Sugiere una evaluación y metodología para individuos y organización en dimensiones y dominios. Organiza los indicadores de seguridad cultural en dos niveles, organizacional e individual. En el dominio Organizacional están los activos, continuidad, acceso/confianza, operaciones, defensa de límites y gobierno de seguridad. Y en el dominio Individual está la actitud, conciencia, comportamiento y competencia. Concluyen que con el marco propuesto con la matriz ATT&CK es posible

identificar, clasificar y analizar los huecos de seguridad de la infraestructura, de las políticas, de los procedimientos y estrategias.

De manera similar (Xiong et al., 2021) se basan en la matriz MITRE ATT&CK para proponer un lenguaje de modelado de amenazas para la seguridad de empresas. Se enfoca en describir los activos de sistema, técnicas de ataque, defensas y asociación de activos. Los pasos de ataque en el lenguaje representan técnicas adversarias descritas por MITRE. Se probaron las capacidades del lenguaje con simulación de dos ataques, pero aún se pueden usar otros ataques. El lenguaje sirve para evaluar la ciberseguridad de una empresa como un sistema total contra ciberataques. Aunque este modelo tiene una cobertura de ataques importante se pueden utilizar otras fuentes como CVE y CWE.

Relacionado con la matriz MITRE ATT&CK y referenciado con el marco NIST (Kwon et al., 2020) presentan la herramienta "Diccionario de Ciber amenazas (CTD)" para que se tenga un mapa sistemático de defensa de ataques. Lo que realizan es, determinar los nuevos ataques, descubrir técnicas de ataque de ATT&CK ICS, desarrollar métodos de detección, mitigar vulnerabilidades, priorizar las vulnerabilidades y diseñar soluciones prácticas para prevenir amenazas. Para descubrir la posición actual de ciberseguridad recomiendan una herramienta web de NIST CSF, que al no proveer información de amenazas de red se puede complementar con la matriz ATT&CK. Con este diccionario se puede identificar el tipo de ataque que está afectando el sistema y las tácticas de detección y mitigación; puede ser reactivo y proactivo. Adicional a CTD, las herramientas de mapeo de defensa-ataque deben crearse para el personal de ciberseguridad.

También se realizan investigaciones para resolver el tema de seguridad en IoT desde un enfoque técnico, como (Tewari & Gupta, 2017) que proponen un protocolo de autenticación mutua ultraligera para etiquetar los dispositivos de IoT, para que tengan un bajo costo computacional y

almacenamiento, pero no tiene en cuenta el entorno de comunicación. Posteriormente, (Alaiz-Moreton et al., 2019) investigan cómo la tecnología de IDS, que es una herramienta de seguridad puede detectar riesgos y defender de ataques de manera rápida, a través de métodos de detección basados en firmas y anomalías; esto lo hacen usando modelos de clasificación, como métodos de ensamblaje y modelos de aprendizaje profundo. Este modelo creado puede ser empleado en un trabajo futuro en un IDS, implementado en una computadora estándar en la infraestructura de IoT.

En el giro de sector de salud (Ould-Yahia et al., 2017) proponen un modelo computacionalmente inteligente y con una estrategia de marco de referencia para medir las vulnerabilidades de seguridad en el ambiente de IoT, cuyo propósito es censar las posibles amenazas de dispositivos de los pacientes que se mueven en diferentes ubicaciones para poder revisar de manera personal el resultado de las métricas. Las soluciones van encaminadas a los sistemas de salud y a los protocolos de seguridad para proteger datos y los canales de comunicación, inicialmente proporciona un control de la salud y de los dispositivos de IoT, como limitante tiene que no considera todos los sensores. Esto se prueba en un ambiente de simulación donde no se considera todas las interfaces y utiliza inteligencia computacional.

Alternamente (Calabretta et al., 2018) propone una solución de mejora del protocolo Message Queue Telemetry Transport (MQTT) basada en el algoritmo de seguridad AugPake y en tokens para autenticar y garantizar la autorización, diseñado para dispositivos de comunicación de poco consumo de energía y requerimientos mínimos de ancho de banda. Esta propuesta es eficiente porque negocia la llave de sesión sin certificadores ni validaciones, ni revocaciones y ha sido extendida para usarse en Active MQ y programación Java.

En contraste (Kanuch & Macko, 2019) optimizan el protocolo de seguridad existente Protocolo de Identidad de Huésped (en inglés, Host Identity Protocol) para la infraestructura IoT,

llamando protocolo E-HIP. Evalúan el modelo propuesto en un esquema de comunicación de dispositivos reales, implementando un prototipo en forma de una librería de comunicación. Consiguientemente verifican el protocolo propuesto como una modificación del código abierto OpenHIP y lo aplican en dispositivos reales. Como resultado obtienen mayor eficiencia en el uso de energía en un 20%, comparado con otros métodos de optimización de HIP.

Por otro lado, (Diro & Chilamkurti, 2018) diseñan e implementan aprendizaje profundo distribuido para detección de ciber ataques en IoT social. El aprendizaje profundo distribuido consiste en que el procesamiento y la comunicación deben de ser lo más cercano a la fuente de datos. Siendo que el IoT social es cuando se aplica a elementos de una ciudad inteligente. Se experimenta con el aprendizaje profundo en un solo nodo para un sistema centralizado y en muchos nodos para la detección del ataque en el sistema distribuido, usando el conjunto de datos NSL-KDD. En el sistema distribuido, la precisión de detección incremento de 96% a 99% y la tasa de alarmas falsas paso del 6.57% al 0.85%. En la evaluación se muestra mejora en la precisión, en la tasa de detección, en la tasa de falsas alarmas y en el desempeño de métricas, por lo que el mecanismo de detección distribuido con aprendizaje profundo es más efectivo que los mecanismos de detección centralizados.

Capítulo 4 Marco Teórico

4.1 Internet de las Cosas

El Internet de las Cosas (en inglés Internet of Things - IoT) es una tecnología emergente que facilita la conectividad y procesamiento de datos con dispositivos electrónicos. La recolección de datos se realiza a través de sensores y se interconecta por Internet, su uso se ha extendido en los sectores de medicina, seguridad, entre otros (Khan et al., 2019). La tecnología de IoT permite tener conexiones entre objetos inteligentes y humanos en cualquier momento y lugar, lo que facilita la toma de decisiones (Shammar & Zahary, 2020).

Los dispositivos de IoT son heterogéneos y limitados en recursos de computación y energía, por lo que tienen susceptibilidad a amenazas y ataques de seguridad. Si se llegará a explotar las vulnerabilidades de seguridad de los dispositivos puede provocar falta de disponibilidad o accesos no autorizados; para enfrentar estos retos de seguridad en el IoT, se han realizado diversas investigaciones (Mahmoud et al., 2015). El incremento en la implementación de dispositivos y las aplicaciones que se usan en IoT, ha generado una expansión sin planeación y sin una correcta seguridad y privacidad en la arquitectura de IoT (Obaidat et al., 2020).

Se presentan los conceptos generales del Internet de las Cosas descritos en anteriores investigaciones científicas (ver Tabla 4.1).

El IoT contiene dispositivos que publican contenido y servicios a través de una política y una nomenclatura (Babar et al., 2010). Asimismo, los aparatos electrónicos tienen conexión a Internet y utilizan sensores (Alqassem & Svetinovic, 2014). Esta agrupación de dispositivos y

servicios han tenido crecimiento en los sectores de transporte, salud, energía, empresarial, social y personal (Mahmoud et al., 2015). El uso de IoT también se incrementa en la ciencia, industria, ingeniería, salud, asistencia de personas e influye en actividades cotidianas (Sklavos & Zaharakis, 2016). Con esta infraestructura se pretende tener escalabilidad, movilidad y conexión inalámbrica para los dispositivos especializados (Babar et al., 2010).

Tabla 4.1 Definición del término de “Internet de las Cosas”

Definición “El Internet de las Cosas ...”
... contiene dispositivos que publican contenido y servicios a través de una política y una nomenclatura (Babar et al., 2010).
... conecta objetos diarios al Internet, equipados con funcionalidades computacionales. Los cuales interactúan entre ellos a través de sensores a través de aplicaciones y servicios (Alqassem & Svetinovic, 2014).
... es una agrupación de dispositivos y servicios que han tenido crecimiento en los sectores de transporte, salud, energía, empresarial, social y personal (Mahmoud et al., 2015).
... conecta millones de dispositivos, con diversas tecnologías (Mohsin et al., 2016).
... es cuando las computadoras tienen información sobre las cosas recolectando datos sin intervención humana y se interconectan a través de Internet. Son accesibles en cualquier tiempo y lugar con confiabilidad de datos (Nawir et al., 2016).
... conecta a objetos físicos y cotidianos a Internet, identificándose a sí mismos a través de radio frecuencia, códigos de respuesta rápida, sensores y tecnología inalámbrica (Singh & Singh, 2016).
... es una nueva tecnología en la industria que asiste e influye en actividades cotidianas, contando con conexiones de aparatos con sensores, monitores y controladores (Sklavos & Zaharakis, 2016).
... se refiere a dispositivos inteligentes, como bulbos, cerraduras, cámaras, termostatos, alarmas que se conectan a Internet, intercambiando información remotamente (Ammar et al., 2018).
... es un nuevo paradigma que permite la interacción entre humanos y cosas, a través de dispositivos inteligentes que transmiten información en una infraestructura descentralizada (Alshehri & Hussain, 2018).
... es un conjunto de objetos interconectados que brinda servicios y comparte información para varias aplicaciones caseras o industriales que se conectan hacia Internet (Tewari & Gupta, 2018).
... posee dispositivos identificados de manera única, que pueden analizar datos, tomar decisiones y formar una red de interconexión a Internet (Hayajneh et al., 2020).
... es un sistema que interconecta dispositivos y servicios de software, incrementando la calidad de vida de las personas (Mabodi et al., 2020).

Fuente: Elaboración propia

El IoT conecta millones de dispositivos, con diversas tecnologías (Mohsin et al., 2016). Dentro del paradigma del IoT se utilizan dispositivos inteligentes, que son objetos ordinarios, como pueden ser bulbos, cerraduras, cámaras, termostatos (Ammar et al., 2018). Los servicios de IoT son accesibles en la nube en cualquier tiempo y lugar (Nawir et al., 2016) y se recomienda que la información intercambiada debe ser analizada para no perder su valor (Singh & Singh, 2016).

Estos aparatos son identificados de manera única en la infraestructura distribuida y descentralizada de IoT (Alshehri & Hussain, 2018), de los cuales se puede analizar datos, tomar decisiones y formar una red de interconexión a Internet (Hayajneh et al., 2020). La arquitectura del IoT está conformado por capas, siendo el esquema básico de tres capas, sensores, middleware y aplicación (Tewari & Gupta, 2018).

4.2 Ciberseguridad en IoT

El disponer con seguridad en IoT tendrá beneficios y ventajas, por el contrario de no tenerla podría haber interrupción en el servicio y causar efectos fatales (Nawir et al., 2016). La seguridad en IoT debe ser resistente a los ataques, controlar la autenticación de datos, accesos, la privacidad e identidad de los clientes, contar con comunicación y almacenamiento seguro y asegurar la disponibilidad de servicios (Babar et al., 2010). Para mantener privadas las conexiones y la transmisión de información (Alqassem & Svetinovic, 2014) se debe contar con confidencialidad, integridad y disponibilidad de los datos (Mahmoud et al., 2015).

La seguridad en IoT es uno de los factores más importantes, debido a la heterogeneidad y tamaño de los dispositivos de la infraestructura. Por lo que se necesita la implementación de esquemas que aseguren la confiabilidad de los usuarios y transacciones seguras de información (Sklavos & Zaharakis, 2016). Se tienen detectados varios retos en la seguridad en IoT, como son el control de accesos y gestión de identidades de equipos híbridos. Otro hallazgo es que los

protocolos de comunicación actuales no están diseñados para IoT (Alshehri & Hussain, 2018). En consiguiente se debe tomar en cuenta la superficie y vectores de ataque propios de la infraestructura de IoT, siendo que las herramientas de análisis tradicionales tampoco no son suficientes (Mohsin et al., 2016).

A continuación, se presentan los conceptos generales de ciberseguridad de IoT descritos en anteriores investigaciones científicas (ver Tabla 4.2).

Tabla 4.2 Definición de “Seguridad en IoT”

Definición “La seguridad de IoT ...”
... debe ser resistente a los ataques, considerar la autenticación de datos, el control de accesos, la privacidad de los clientes, identificar usuarios, almacenar y administrar la identidad y comunicar seguramente (Babar et al., 2010).
... mantiene privadas las conexiones y la transmisión de información. Está compuesta de mecanismos de seguridad para disminuir ataques y vulnerabilidades de IoT (Alqassem & Svetinovic, 2014).
... tiene como objetivo la confidencialidad, integridad y disponibilidad, con limitaciones de los componentes heterogéneos (Mahmoud et al., 2015).
... es considerar la superficie de ataque en la infraestructura, los vectores de ataque en servicios virtuales y las herramientas de análisis (Mohsin et al., 2016).
... es tener una comunicación segura para servicios, con beneficios y ventajas, puede ser aplicada a casas inteligentes, salud, transporte, etc (Nawir et al., 2016).
... es un factor importante para asegurar la información conectada en una red (Vashi et al., 2017).
... es uno de los factores más importantes, debido a la heterogeneidad y tamaño de los dispositivos de la infraestructura (Sklavos & Zaharakis, 2016).
... tiene como reto el control de accesos, la gestión de administración y la identidad de equipos heterogéneos (Alshehri & Hussain, 2018).

Fuente: Elaboración propia

4.3 Estándares de seguridad de IT

Algunos marcos de referencia para seguridad que se han usado en infraestructura de TI son NIST CSF, NIST SP 800-53, COBIT5, ISO/IEC 27001:2013, ISA 62443-2-1:2009. Otros marcos de referencia de seguridad que se han desarrollado son, Comité de Organizaciones Patrocinadoras de la Comisión Treadway (en inglés, Committee of Sponsoring Organizations of the Treadway

Comission), los 20 principales controles críticos de seguridad (en inglés, Council on CyberSecurity Top 20 Critical Security Controls), Estándar de buenas prácticas (en inglés, Standard of Good Practice), Comité Técnico de Ciberseguridad (en inglés, Cyber Security Technical Commitee), Arquitectura de seguridad empresarial aplicada de Sherwood (en inglés, Sherwood Applied Business Security Architecture), Sstándar de aseguramiento de la información (en inglés, Information assurance standard), Alianza de confianza de información de salud (en inglés, Health Information Trust Alliance), Corporación de Confiabilidad Eléctrica de América del Norte Protección de Infraestructura Crítica (en inglés, North American Electric Reliability Corporation Critical Infrastructure protection), Arquitectura de código abierto (en inglés, Open Source Architecture) y Guía de buenas prácticas 13 (en inglés, Good Practice Guide 13) (Ibrahim et al., 2018).

4.3.1 Modelo de madurez de capacidad de ciberseguridad

El modelo de madurez de capacidad fue presentado en 2019 por el departamento de energía, con indicadores y patrones que representan capacidad y desarrollo en ciberseguridad, consiste en:

- Reforzar las capacidades de ciberseguridad de la organización,
- Permitir a las organizaciones evaluar y medir las capacidades de ciberseguridad,
- Compartir conocimiento, mejores prácticas,
- Permitir a la organización priorizar acciones e inversiones (Sulistyowati et al., 2020).

4.3.2 Marco de referencia NIST

El marco de referencia de NIST (Frayssinet Delgado et al., 2021) es un lenguaje común para entender, manejar y expresar los riesgos de ciberseguridad externos e internos. Identifica y prioriza las acciones para reducirlos en cualquier tipo de organización. Este marco consiste en tres

partes, 5 Funciones de alto nivel, 23 Categorías con cuestiones técnicas, personas, procesos y 108 Subcategorías. (Sulistyowati et al., 2020) comenta que en 2018 se actualizó ciberseguridad NIST CFS con control técnico, análisis de eventos e incidentes y funciones (ver Tabla 4.3).

Tabla 4.3 *Marco de referencia NIST CSF*

Funciones	Categorías	Descripción general
Identificar	Administración de activos Ambiente de negocio Gobierno Evaluación de riesgo Estrategia de administración de riesgo Administración de riesgo en la cadena de suministro	Conocimiento del entorno, activos, datos
Proteger	Administración de identidad y control de acceso Conciencia y entrenamiento Seguridad de datos Procedimiento y procesos de protección de información Mantenimiento Tecnología de protección	Implementaciones para limitar los eventos de ciberseguridad
Detectar	Eventos y anomalías Monitoreo continuo de seguridad Proceso de detección	Identificar rápidamente eventos de ciberseguridad
Respuesta	Plan de respuesta Comunicación Análisis Mitigación Mejoras	Desarrollar e implementar actividades para evitar impacto de eventos de ciberseguridad.
Recuperación	Plan de recuperación Mejoras Comunicación	Desarrollar y recuperar las capacidades después de un incidente de ciberseguridad.

Nota. Adaptado (Frayssinet Delgado et al., 2021) (Sulistyowati et al., 2020)

El NIST CSF pretende mejorar la ciberseguridad de la infraestructura crítica en una organización. Toma en cuenta que cualquier organización sin importar su tamaño utiliza las funciones de identificar, proteger, detectar, responder y recuperar. Estas funciones tienen

categorías y subcategorías con puntos de referencia a estándares, como CIS CSC, COBIT 5, ISA 62443, ISO/IEC 27001 y NIST SP 800-53. Es un estándar que puede ser personalizado en el nivel táctico (Bob Chaput, 2017).

4.3.3 Organización Internacional de Estandarización

En la Organización Internacional de Estandarización (en inglés, International Organization for Standardization) definen las Técnicas de Seguridad de Tecnologías de la Información ISO/IEC 27002, éstas proveen una guía de implementación para manejar la seguridad, en su versión de 2015 contiene 15 controles (Calder, 2008). El ISO/IEC 27002:2005 es de los mejores estándares de seguridad, que enfatiza el manejo de riesgo y que se basa en requerimientos legales, como no divulgación de datos personales, protección de información interna y de derechos de protección intelectual, también tiene políticas de seguridad de información, asignación de responsabilidades, escalación de problemas y administración de la continuidad del negocio (Nastase et al., 2009).

4.3.3.1 ISO/IEC 27002

Es para manejar y controlar los sistemas de información de las organizaciones para mantener la confidencialidad, integridad y disponibilidad. En el ISO/IEC 27002 no se tiene una forma particular de control, sino que se deja que el cliente seleccione los controles necesarios. Tiene 18 secciones, con 14 controles de seguridad y 35 categorías (Sulistyowati et al., 2020). El estándar de ISO/IEC 27002 está relacionado a controles de seguridad de información para servicios en la nube de proveedores y también de clientes finales. El proveedor y los clientes deben documentar de manera apropiada los roles y responsabilidades de seguridad (Kandasamy et al., 2020). El ISO 27002:27013 contiene 14 cláusulas, donde cada una tiene categorías de seguridad con un objetivo de control y más controles opcionales. Cada control es desarrollado por tareas y puede ser categorizado en clases de gobernación, administración, técnica y legal (Sengupta, 2015).

4.3.3.2 ISO/IEC 27001/2013

El estándar ISO 27001 tiene influencia notoria en la seguridad de la información para mantener la triada de seguridad en la información. Esto se valida con un análisis estadístico y a través de la observación. Al implementar los dominios de seguridad de ISO 27001 se notan mejoras en la confidencialidad, integridad y disponibilidad (Sulay et al., 2020).

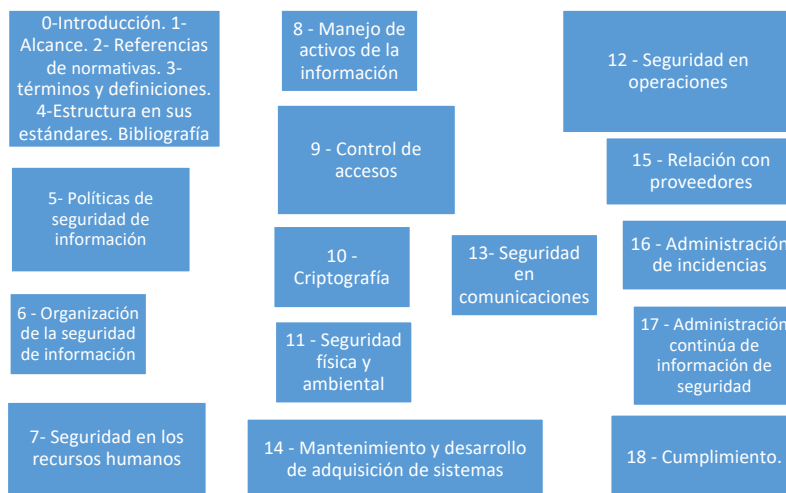
ISO/IEC 27001:2013 está relacionado con Gestión de Sistemas de Información de Seguridad (Information Security Management System). El ISMS es un marco de referencia que identifica, evalúa y trata los riesgos de información de una organización. La estructura del estándar es introducción, alcance, referencias normativas, términos, definiciones, contexto de la organización, liderazgo, planeación, soporte, operación, evaluación de desempeño, mejora (Kandasamy et al., 2020). El ISO/IEC 27001:2013 es un estándar internacional de seguridad de información para las organizaciones de todo tipo y tamaño, donde cada organización selecciona los controles que le ajusten. La estructura incluye introducción, alcance, referencias de normativas, términos y definiciones, estructura en sus estándares, bibliografía, políticas de seguridad de información, organización de la seguridad de información, seguridad en los recursos humanos, manejo de activos de la información, control de accesos, criptografía, seguridad física y ambiental, seguridad en operaciones, seguridad en comunicaciones, mantenimiento y desarrollo de adquisición de sistemas, relación con proveedores, administración de incidencias, administración continua de información de seguridad y cumplimiento (Kandasamy et al., 2020) (Ver Figura 4.1).

4.3.3.3 ISO/IEC 27035

Los controles de seguridad de información pueden ser complejos, indefinidos, falla en el servicio y trabajar parcialmente, los incidentes efectivamente permiten identificar y analizar riesgo. El manejo de incidentes incluye la detección y la corrección de controles para responder a

incidencias, minimizar impacto, recolectar evidencia forense. Normalmente involucra la explotación de vulnerabilidades no controladas (Kandasamy et al., 2020).

Figura 4.1 Marco de referencia ISO/IEC 27001:2013



4.3.4 Matriz MITRE ATT&CK

La matriz MITRE ATT&CK sirve contra los ataques cibernéticos en una infraestructura digital. Es una base de datos de técnicas, tácticas y conocimiento común para simulación, desarrollo de defensa y evaluaciones. Las tácticas definen un objetivo de un ataque con la pregunta ¿Por qué? Las técnicas describen los medios de los adversarios para implementar una táctica con la pregunta ¿Cómo? ¿Qué?. Las sub-técnicas son más específicos para los objetivos de adversarios. Los procedimientos implementan las técnicas de adversarios. Y las mitigaciones definen las contramedidas para prevenir técnicas, con la pregunta ¿Qué hacer? Puede tratarse de los modelos ATT&CK para empresas, nube, móviles y para la industria (Georgiadou et al., 2021).

4.3.5 Modelo Core COBIT 2019

Para gobierno y gestión de objetivos, tiene 5 dominios en la organización que se dividen en dos áreas de procesos, el gobierno y administración. El gobierno contiene procesos de

gobernación, proceso de evaluación, dirección y monitoreo. Y la administración está compuesta de cuatro dominios, planeación, construcción, implementación y monitoreo (Sulistyowati et al., 2020).

4.3.6 Estándar de seguridad de datos de la industria de tarjetas de pago

Es un estándar de seguridad de datos para pago de tarjetas de crédito, débito y ATM (en inglés, Payment Card Industry Data Security Standard) para todas las entidades que procesan, almacenan y transmiten a los tarjeta habientes. Provee requerimientos básicos de seguridad que ayuda a las organizaciones para programas seguridad. Con 250 sub-requerimientos, agrupado en 6 objetivos y 12 requerimientos principales. Sirve para identificar vulnerabilidades, reportar correcciones de activos y remediar (Sulistyowati et al., 2020).

4.3.7 OCTAVE

La metodología de Evaluación de amenazas, activos y vulnerabilidades operativamente críticas (en inglés, Operationally Critical Threat, Asset and Vulnerability Evaluation) optimiza los riesgos de seguridad de información de tal manera que una organización puede tener resultados con poca inversión de tiempo, personas y otros recursos (Caralli et al., 2007). El OCTAVE incluye principios, atributos y entregables y sus tres fases son: crear perfiles de amenazas basados en activos, identificar las vulnerabilidades de la infraestructura y desarrollar planes y estrategias de seguridad. Estos métodos permiten a una organización a desarrollar prioridades de seguridad basados en el negocio (Pyka & Sobieski, 2012).

Algunos métodos que evalúan los riesgos en la infraestructura de IT son COBIT, Manual de seguridad de TI de Austria, EBIOS, ISO/IEC 27007, MARION, MEHARI, OCTAVE Allegro, entre otros. En la Universidad de Langlangbuana se evalúa con OCTAVE Allegro las amenazas, las vulnerabilidades operacionales y el análisis de riesgos. Se utiliza este marco de referencia

porque necesita pocos recursos y no necesita experiencia. A través de un estudio cualitativo se contacta personas claves de la universidad y del área administrativa y de redes computacionales. Después de la implementación de controles de seguridad de ISO/IEC 27002 se obtiene una reducción del riesgo acorde a la evaluación de OCTAVE Allegro. Se le recomienda a la universidad una política para la seguridad de sistemas de información, manuales y procedimientos de seguridad (Jufri et al., 2017).

4.3.8 Marco de seguridad Lubua

El marco de referencia de seguridad Lubua establece que los objetivos de una política de seguridad deben asegurar la confidencialidad, disponibilidad e integridad en la información en la infraestructura de seguridad y debe tomar en cuenta la comunicación entre personas claves de la empresa. Está compuesta por 7 categorías y está enfocado en la continuidad del negocio (Wazoel Lubua & Pretorius, n.d.).

4.4 Protocolos de aplicación

4.4.1 Protocolo TLS

Por un lado (Satapathy & Livingston, 2016) discuten la arquitectura de SSL y TLS y presentan los ataques contra SSL/TLS y los factores que influyen. Siendo que SSL/TLS son protocolos usados para confianza de servicios sobre la capa de transporte para una conexión entre clientes y servidores. Los clientes y servidores intercambian parámetros como ID de sesión, encriptación, certificado X509, técnicas de compresión, estado MAC del cliente/servidor y vectores de inicialización. SSL/TLS tienen fallas en la seguridad que pueden generar ataques

activos y pasivos, como Beast, Crime, Time, Breach, Lucky13, RC4 Biases, Renegociación SSL, Poodle, Truncado, Bar Mitzvah.

En una revisión literaria (Alashwali & Rasmussen, 2018) crean una taxonomía de los ataques de degradación de TLS respecto a cuatro vectores, al elemento del protocolo, al tipo de vulnerabilidad, al método de ataque y al nivel de daño que causa. Los ataques de degradación de TLS detectados son retroceso de la suite de cifrado, retroceso de versión, retroceso de la llave de intercambio, retroceso de llave de intercambio DHE, ataque Poodle, ataque Logjam, ataque Freak, ataque Drown, ataque de retroceso de Forward Secrecy, ataque Sloth, retroceso de versión, retroceso de versión de baile, retroceso HelloRetry.

4.4.2 Protocolo MQTT

El protocolo de transporte de telemetría con cola para mensajes (en inglés, Message Queue Telemetry Transport), fue estandarizado en ISO/IEC 20922 y aceptado en OASIS, es usado para comunicación en ambientes de IoT con el modelo publicar-suscribir, donde los clientes no necesitan actualizarse, disminuyendo el uso de recursos y es óptimo para ambientes con poco ancho de banda. El servidor es llamado broker y envía las actualizaciones a los clientes; los clientes no se mandan mensajes entre ellos sino usan al broker para esto. Cada mensaje MQTT contiene un tema, organizado en una estructura de árbol con los clientes se suscriben o publican (Dinculeană & Cheng, 2019).

4.4.2.1 Seguridad de MQTT

La seguridad de MQTT puede estar cubierto por los elementos, del broker que usa listas de control de accesos, la encriptación implementada entre el cliente-broker o nodo-nodo,

complemento de TLS o DTLS (en inglés, Datagram Transport Layer Security) y la encriptación usando AES (en inglés, Advanced Encryption Standard) (Dinculeană & Cheng, 2019).

4.4.2.2 Vulnerabilidades de MQTT

La mayoría de las vulnerabilidades de MQTT están expuestas en las configuraciones por default. Estos hallazgos pueden ser falta de autenticación, falta de autorización, falta de confidencialidad, falta de integridad. Cuando se implementa incorrectamente estos parámetros en el protocolo MQTT, se pueden explotar vulnerabilidades como DoS o ejecución remota de comandos (Hernández Ramos et al., 2018).

Por otro lado (Hernández Ramos et al., 2018) crean un marco que permite usar una técnica difusa basado en una plantilla para el protocolo MQTT. Experimentan con procesamiento de paquetes usando MOQUETTE o MOSQUITO para problemas reportados como Denegación de Servicio o reinicio de comunicación de los brokers. Muestran que el desempeño en la técnica de difusión presentada es una buena opción para usar en las arquitecturas de red con un bajo procesamiento en la energía de los sensores. Después de aplicar la herramienta a clientes y brokers, el difusor fue capaz de detectar fallas que podían causar DoS. Por lo que el uso de una técnica de difusión basada en plantillas para aplicaciones que implementan MQTT puede descubrir vulnerabilidades de seguridad, facilitando portabilidad (Hernández Ramos et al., 2018)

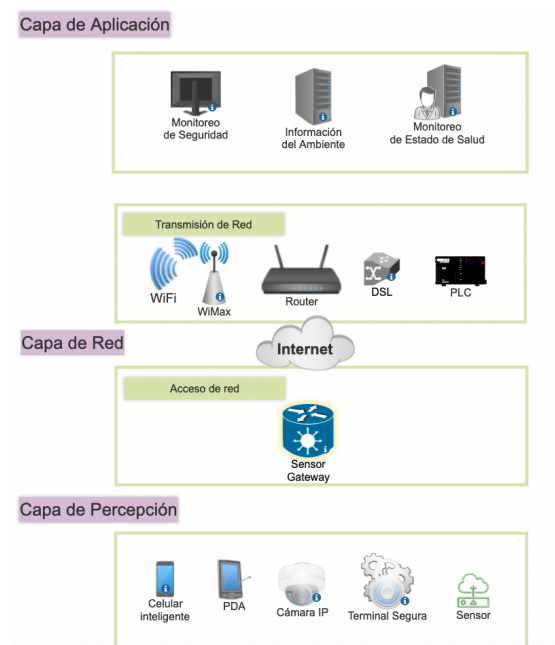
De manera alterna (Vaccari et al., 2020) explotan una vulnerabilidad de MQTT, que permite a un cliente no autorizado configurar el comportamiento del servidor. El ataque propuesto es SlowITe, que genera denegación de servicio de tasa baja enfocado para MQTT. Consideran texto plano y encriptado y comparan los efectos de la amenaza. Cuando SlowITe se prueba sobre MQTT soportado en TLS/SSL, también se detecta DoS. Incrementándose el ancho de banda requerido para ejecutar SlowITe cuando se usa la capa de SSL/TSL. Como resultado tienen un ataque

exitoso, que lleva a la víctima a DoS limitando los recursos. Esto fue con un enfoque al protocolo de aplicación MQTT usado en IoT para identificar los ataques de denegación de servicio. Exploraron la posibilidad de establecer el parámetro de Keep-Alive en el servidor, configurando así el comportamiento del servidor en término de tiempos de conexiones. Concluyen que SlowITe es una vulnerabilidad del protocolo MQTT que debe de ser evitada (Vaccari et al., 2020).

4.5 Arquitectura de red de IoT

(Huang & Hsieh, 2013) presentan la arquitectura de IoT, donde los nodos de sensor están en la capa perceptual. Después los datos se envían a la capa de red, a través de la puerta de enlace del sensor, transmitiéndose por la red con modelos de comunicación como 3G, WiMax, redes Wireless en LTE, xDSL y redes cableadas. Pasando los datos a la capa de aplicación, en la que se puede presentar aplicaciones de monitoreo de seguridad, procesamiento de información del ambiente, monitoreo de estado de salud de los sensores (ver Figura 4.2).

Figura 4.2 *Arquitectura de red*

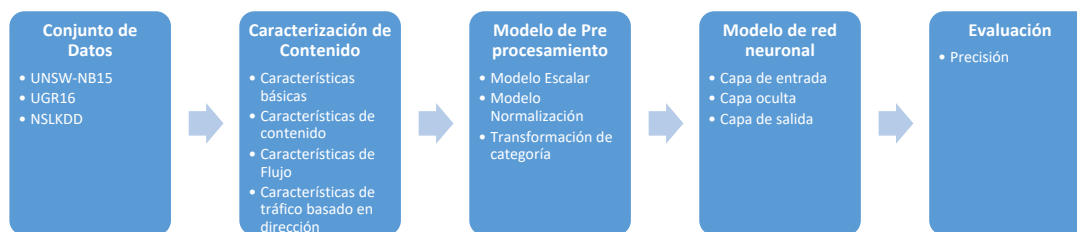


Nota. Adaptado (Huang & Hsieh, 2013)

4.6 Sistema de detección de intrusos

(Larriva-Novo et al., 2021) propone un modelo de detección de intrusos más preciso por el incremento del número y complejidad de los ataques de ciberseguridad. Evalúa las bases de datos, UGR16, UNSW-NB12 y KDD99, con funciones de normalización y de escalares usando técnicas de preprocesamiento de datos. Este modelo de procesamiento se basa en las características de conexión básica, características de contenido, características de estadística y funciones basadas en tráfico y características de tráfico basadas en dirección. Muestra que aplicando la categorización del tráfico de red y varias técnicas de preprocesamiento, la precisión puede ser de más del 45%, de los posibles ataques (Ver Figura 4.3).

Figura 4.3 Evaluación NIDS



Nota. Adaptado (Larriva-Novo et al., 2021)

Se ha propuesto una taxonomía de las técnicas de IDS basadas en los atributos de estrategia, tipo de análisis, tipo de intrusión en IoT y método de detección de ataque. Acorde a la estrategia de implementación en IoT, puede ser centralizado, distribuido o híbrido. En cuanto a la estrategia de análisis de IDS para IoT, puede ser basada en anomalías, en firmas o específicas. La clasificación de los tipos de intrusos de IoT, puede ser físicos, de red, de software y encriptados. La clasificación de técnicas de detección de ataques para IoT que pueden ser técnica de aprendizaje de máquina y aprendizaje profundo. Es recomendable que los IDS utilicen bases de datos

estandarizadas, técnicas de correlación de alertas y métodos híbridos de detección de amenazas (Thakkar & Lohiya, 2021).

La tendencia del uso de aprendizaje de máquina en los IDS debe considerar el modelo de operación, un uso eficiente de datos, técnicas de optimización y la seguridad de datos. Dado que el no revisar los resultados que dan estas técnicas de IA puede provocar problemas, pérdida de productividad o pérdida de ganancia (Goasduff, 2021).

4.6.1 Análisis comparativo de IDS

Dentro de las propuestas para mejorar la tecnología de IDS, se propone un modelo híbrido de IDS, con conjunto de datos Aegean de WiFi (AWID), identifica intrusos y ataques de día cero con baja tasa de alarmas falsas. La técnica que usa es aprendizaje de máquina y procesos de agrupamiento (Nivaashini M. et al., 2021).

Algo similar se plantea para proteger servicios críticos, basado en aprendizaje de máquina, compuesto por aprendizaje federado (en inglés, Federated Learning) y aprendizaje activo (AL: Active Learning) con conjuntos de datos locales (Kelli et al., 2021).

Adicional, se presenta un IDS para SDN. En el plano de control se instala un IDS basado en flujos, y en el plano de datos se implementa un IDS basado en firmas. Basado en un clasificador de aprendizaje de máquina para el IDS de flujo y en el software Snort para el IDS de firmas, se usa el conjunto de datos NSL-KDD (Muthamil Sudar & Deepalakshmi, 2021).

Equivalentemente, se genera un modelo de clasificación de nuevo binario y multiclase de Redes Neuronales Convolución (CNN) para identificar anomalías con el conjunto de datos NSLKDD. Resulta en una alta precisión del 98%, tasa de detección y entrenamiento (Akhtar & Feng, 2021).

También se propone el uso de Inteligencia Artificial (en inglés, Artificial Intelligence) para el IDS, con la red neuronal convolucional óptima y red de memoria de corto tiempo. Se usan los conjuntos de datos CSIC-2010, CICIDS2017. Experimental con resultados de exactitud de 91-93%, precisión de 86-98% (A. Kim et al., 2020).

Por otro lado, se crea un IDS para detectar comportamiento anormal con el protocolo MQTT. Basado en aprendizaje de máquina y aprendizaje profundo con los conjuntos de datos NSL-KDD, USNW-NB15. Como resultado se mejoran las métricas de detección con un rendimiento de máximo 1.5 seg cada vez que se lanza el ciberataque (Aveleira-Mata et al., 2021).

4.6.2 Ciberataques contra IDS

Las ciber amenazas hacia la infraestructura de IoT pueden ser de caja blanca, en la que el atacante conoce el sistema objetivo, caja negra, donde el atacante no conoce las características o configuración del sistema a vulnerar, pero podría llegar a conocerlo, y de caja gris, donde el adversario tiene conocimiento limitado del sistema a atacar (Biggio & Roli, 2018).

4.6.2.1 Ataques adversarios de aprendizaje de máquina de IDS

Los métodos y técnicas tradicionales contra las ciber amenazas no son apropiados para las vulnerabilidades en IoT, por lo que es necesario mejorar las soluciones de seguridad. Se han aplicado técnicas de aprendizaje de máquina para detectar las amenazas de seguridad en IoT, donde las redes neuronales clasifican los ataques en IDS. Sin embargo, en el aprendizaje de máquina en IoT se tiene el impacto de ataques adversarios. El aprendizaje profundo basado en IDS puede identificar DoS con una confiabilidad del 93%, pero si se despliegan ataques adversarios la detección baja al 24%. Una opción para mejorar el desempeño del aprendizaje profundo basado

en IDS para IoT es usando una variante de Red Neuronal de Avance (Feed-forward Neural Network), que es conocida como Red Neuronal de Propia Normalización (Self-normalizing Neural Network) y usar el conjunto de datos BoT-IoT. FNN es degradado significativamente por amenazas adversarias, de la tasa de predicción de 95% baja al 24%. Pero SNN es más resistente a estos ataques adversarios, con una mejora del 9% en el desempeño (Ibitoye et al., 2019).

Los IDS pueden utilizar aprendizaje de máquina, aunque estas técnicas son vulnerables a ataques adversarios, disminuyendo así su confiabilidad y su efectividad en la detección de amenazas. Los ataques adversarios involucran la aplicación de perturbaciones no identificadas en el aprendizaje de máquina, detectando incorrectamente los eventos maliciosos. Pueden ser de,

- Envenenamiento, es la manipulación del conjunto de datos para influenciar la detección.
- Interferencia de tiempo, que es la ofuscación de la detección, cambiando su sensibilidad.
- Ataque de evasión, que es la clasificación errónea de los datos maliciosos.

En estas amenazas el atacante puede tener control de los datos entrenados, del modelo de detección, del conjunto de características muestras, de oracle o de la manipulación a fondo (Apruzzese et al., 2021).

Las amenazas adversarias usan la búsqueda local, la optimización combinatoria y la programación convexa para encontrar la perturbación adversaria que comprometa el rendimiento del aprendizaje de máquina. Se han generado perturbaciones para aprendizaje de máquina profundo usando el método de signo de gradiente rápido (en inglés, Fast Gradient Sign Method) y ataque de mapa de prominencia basado en jacobiano (en inglés, Jacobian Based Saliency Map Attack). También se han creado y validado ataques adversarios basados en red adversaria generativa (en inglés, Generative Adversarial Networks) que pueden evadir un IDS con parámetros de caja negra, preservando el funcionamiento de la red. Un IDS puede defenderse de los ataques

adversarios optando por un entrenamiento de las posibles perturbaciones, aunque sólo dará mejora contra los ejemplos adversarios para los que fue entrenado. Como mecanismo de defensa se tiene una opción de entrenamiento adversario basado en GAN, que mejora el desempeño de IDS ante perturbaciones adversarias, manteniendo el comportamiento de la red (Usama et al., 2019).

Adicional se expone un ataque adversario de GAN, llamado attackGAN, que es de caja negra y evade al IDS asegurando la funcionalidad de la red. AttackGAN es basado en Wasserstein GAN y tiene mayor tasa de éxito en ataque de caja negra contra IDS comparado con los métodos de FGSM, descenso del gradiente del proyecto (en inglés, Project Gradient Descent), ataque CW y algoritmos basados en GAN. Este ataque se valida experimentalmente usando el conjunto de datos NSL-KDD. Con lo que se resalta que para desarrollar sistemas de seguridad de red se recomienda usar los ataques adversarios y la defensa de juegos (Zhao et al., 2021).

El aprendizaje de máquina también se ha utilizado para seguridad de redes inalámbricas y ha permitido controlar dispositivos y detectar anomalías. Sin embargo, ha sido vulnerable a ataques adversarios de aprendizaje de máquina, provocando pérdida del rendimiento del radio de comunicaciones inalámbricas. Algunos ataques adversos que se pueden ejecutar en IoT son exploratorios, evasivos y causantes. Estos ataques se presentan en las redes inalámbricas de la siguiente manera,

- Ataque de interferencia - el transmisor monitorea el estado del canal (ocupado) y transmite cuando el canal está en espera. Resultando ruido e interferencia si el canal está ocupado y ruido si el canal esta inactivo.
- Ataque de envenenamiento de espectro – el atacante cambia las características del estado del canal para que el transmisor decida erróneamente transmitir.

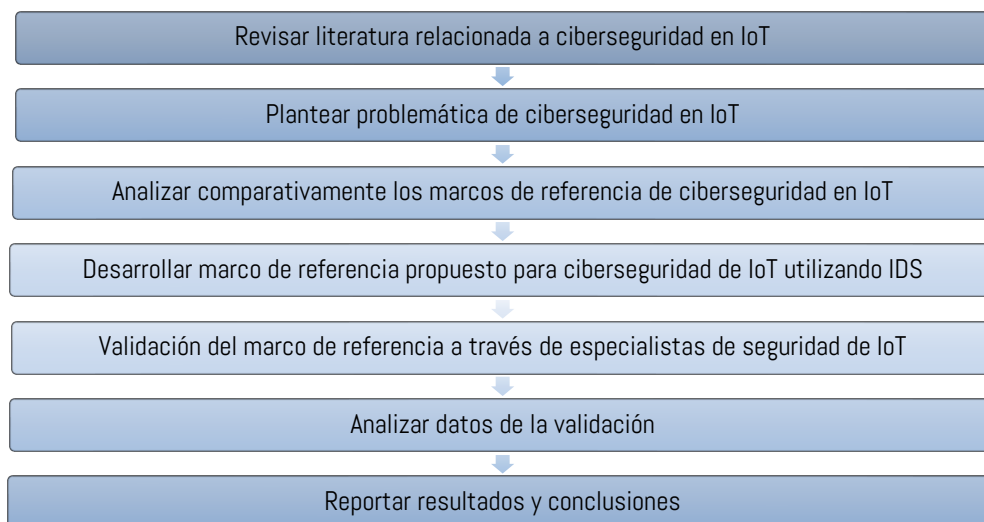
- Ataque de violación de prioridad – el atacante fuerza al transmisor a tomar decisiones incorrectas, como un ataque de evasión.

Como mecanismo de defensa se propone que el transmisor de IoT selectivamente haga acciones incorrectas para que el ataque exploratorio no suceda, mostrando su efectividad en el rendimiento del transmisor (Sagduyu et al., 2019).

5 Metodología

La metodología por utilizar en la presente investigación será cuantitativa y correlacional y consiste en hacer la revisión de literatura relacionada a ciberseguridad en infraestructura de IoT, para después plantear la problemática de ciberseguridad en IoT. Posteriormente se analiza comparativamente los marcos de referencia de ciberseguridad en IoT y se desarrolla el marco de referencia para ciberseguridad de IoT utilizando IDS. En seguida se evalúa el marco de referencia de seguridad propuesto para la infraestructura de IoT, a través de encuestas a los especialistas de seguridad de una empresa de servicios de IoT. La toma de la muestra será probabilística, considerando un error máximo aceptable del 5% y un nivel de confianza del 95%. La recolección de los datos se hace mediante un cuestionario con confiabilidad y validez, que contiene preguntas cerradas, es autoadministrado y utiliza la escala de Likert. El resultado de las encuestas es analizado mediante el programa Minitab, explorando los datos con estadística descriptiva y medidas de variabilidad. Finalmente se reportan los resultados y conclusiones (ver Figura 5.1).

Figura 5.1 Metodología de la investigación



5.1 Análisis comparativo de modelos de seguridad

Se realiza el análisis comparativo de los marcos de ciberseguridad utilizados en las organizaciones, para considerarse en la infraestructura de IoT, NIST CSF, ISO/IEC 27002, OCTAVE Allegro, (Sulistyowati et al., 2020), ISA/IEC 62443 y marco de referencia de Lubua (Wazoel Lubua & Pretorius, n.d.). Mostrado en Tabla 5.1.

Tabla 5.1 *Análisis comparativo de los marcos de ciberseguridad*

Modelo	Enfoque	Estructura	Funciones
NIST CSF (Framework for Improving Critical Infrastructure Cybersecurity, 2018)	Riesgos de ciberseguridad externos e internos. Identifica y prioriza las acciones para reducirlos.	Centro: 5 Funciones de alto nivel Niveles de implementación: 23 Categorías con cuestiones técnicas, personas, procesos Perfiles: 108 Sub- categorías	1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar
ISO/IEC 27002 (Calder, 2008) (Sengupta, 2015)	Recomienda controles de seguridad de la información, derivados de riesgos en la confidencialidad, integridad y disponibilidad.	18 controles	0. Introducción 1. Alcance 2. Referencias de normativas 3. Términos y definiciones 4. Estructura en sus estándares. Bibliografía. Cláusulas 5. Políticas de seguridad de información 6. Organización de la seguridad de información 7. Seguridad en los recursos humanos 8. Manejo de activos de la información 9. Control de accesos 10. Criptografía. 11. Seguridad física y ambiental 12. Seguridad en operaciones 13. Seguridad en comunicaciones 14. Mantenimiento y desarrollo de adquisición de sistemas 15. Relación con proveedores 16. Administración de incidencias

				17. Administración continúa de información de seguridad 18. Cumplimiento
OCTAVE Allegro (Ali & Awad, 2018)	Proceso de riesgos de seguridad informática Con recursos limitados	4 funciones que incluyen 8 pasos		1. Establecer Dirección 2. Perfil de Activos 3. Identificar Amenazas 4. Mitigar amenazas
ISA 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems, 2020)	Guía para seguridad en la automatización industrial y el control de sistema a través de su ciclo de vida con seguridad, integridad y confiabilidad.	Compuesto de secciones General Políticas Procedimientos Sistemas Componentes	4 y	- 62443-1-1 Terminología, conceptos y modelos - 62443-1-2 Glosario de términos y abreviaciones - 62443-1-3 Métricas de sistema de seguridad - 62443-1-4 Ciclo de vida y casos de uso de seguridad - 62443-2-1 Establecer un programa de seguridad - 62443-2-2 Evaluar los programas de seguridad - 62443-2-3 Administración de parches en el ambiente - 62443-2-4 Requerimientos del programa de seguridad para servicio de proveedores - 62443-2-5 Guía de implementación para dueños de activos - 62443-3-1 Tecnologías de seguridad - 62443-3-2 Evaluación de riesgos de seguridad - 62443-3-3 Requerimientos del sistema de seguridad y niveles de seguridad - 62443-4-1 Desarrollo de productos de seguridad en los requerimientos de ciclo de vida - 62443-4-2 Requerimientos de seguridad técnicas en los componentes
Marco de referencia de seguridad Lubua (Wazoel Lubua & Pretorius, n.d.)	Política de seguridad para asegurar la continuidad de negocios	7 categorías		- Seguridad de datos - Gobierno de servicios de red e Internet - Dispositivos usados por la compañía - Seguridad física

-
- Reportes y manejo de incidentes
 - Monitoreo y Cumplimiento
 - Administración de políticas
-

Se realiza un análisis comparativo de los marcos de ciberseguridad de infraestructura NIST CSF, ISO/IEC 27002, OCTAVE Allegro (Sulistyowati et al., 2020), ISA/IEC 62443 y marco de referencia de Lubua (Wazoel Lubua & Pretorius, n.d.). Dentro de estos se detectan categorías que engloban los mismos objetivos y entregables, por lo que se agrupan en nuevas categorías basadas en la metodología de OCTAVE Allegro, se selecciona este marco porque no necesita un alto grado de experiencia de los riesgos; es fácil de utilizar, sirve a largo plazo y se enfoca en los activos de la información (Ali & Awad, 2018) (Ver Figura 5.2).

Inicialmente el análisis se realiza con un proceso de código (Sulistyowati et al., 2020), donde se asignan variables a cada categoría de los marcos de seguridad, asignando el código “NC” al modelo NIST CSF, “IO” a ISO/IEC 27002, “OA” para OCTAVE Allegro, “IA” al modelo ISA/IEC 62443 y “LU” al marco de referencia Lubua (ver Tabla 5.2).

Tabla 5.2 *Proceso de codificación de los marcos de seguridad*

Marco de referencia	Código asignado	Ejemplo de código para categoría
NIST CSF	NC	Categoría 1 NC0 Categoría 2 NC1
ISO/IEC 27002	IO	Categoría 1 IO0 Categoría 2 IO1
OCTAVE Allegro	OA	Categoría 1 OA0 Categoría 2 OA1
ISA/IEC 62443	IA	Categoría 1 IA0 Categoría 2 IA1
Lubua	LU	Categoría 1 LU0 Categoría 2 LU1

Después se analizan los marcos de referencia y las categorías con objetivos y entregables similares (Sulistyowati et al., 2020) se asocian en categorías basadas en el marco de seguridad OCTAVE Allegro. Es decir, la categoría NC1 del modelo NIST es similar a la categoría IO1 del modelo ISO/IEC 27002, el OA0 del modelo OCTAVE Allegro, la IA2 en ISA/IEC 62443 (ver Tabla 5.3). Generándose las categorías Establecer el alcance, Administración de activos de información, Políticas y procedimientos, Proteger operación, Identificar amenazas, Mitigar amenazas y Cumplimiento.

Tabla 5.3 *Análisis comparativo entre los marcos de referencia*

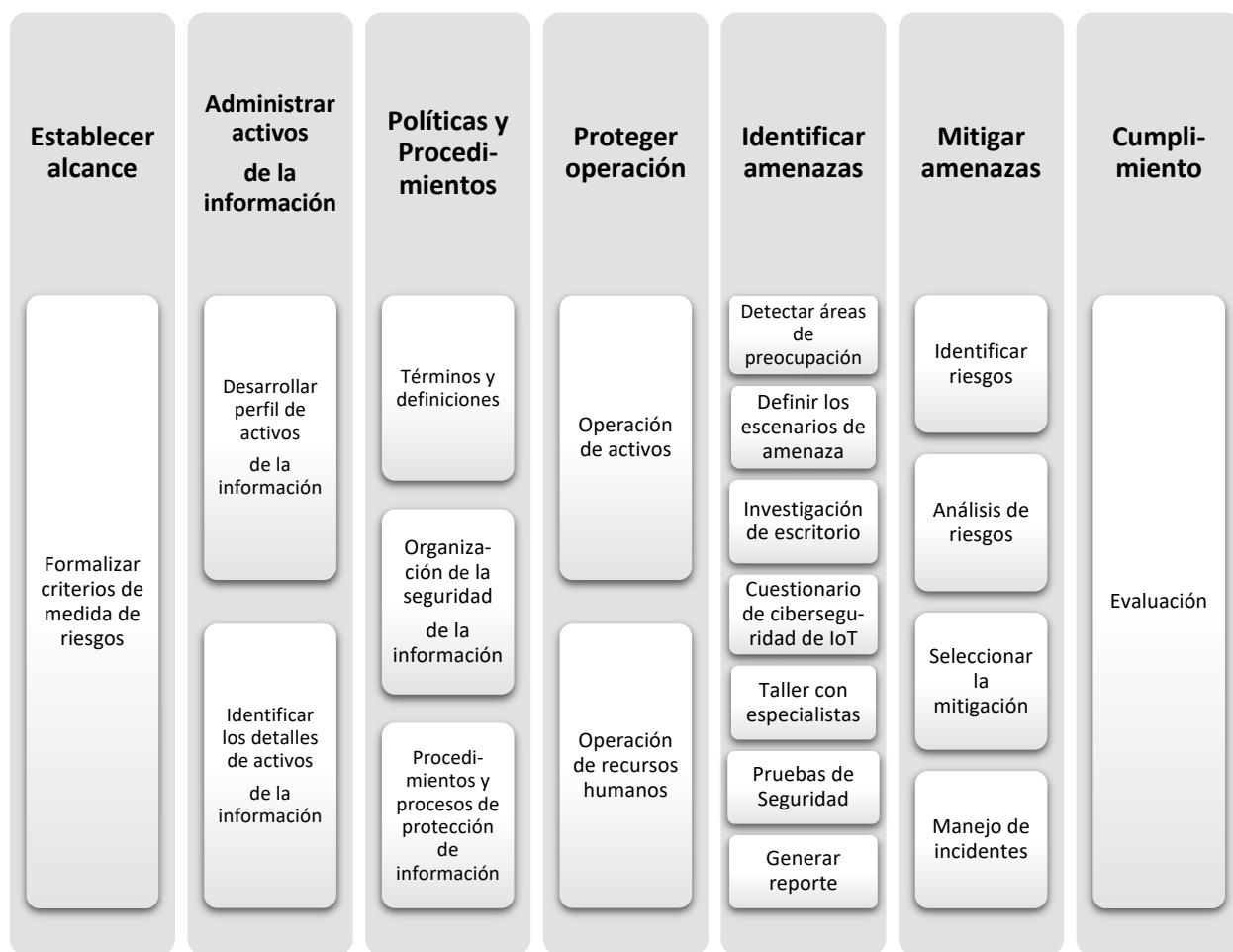
Modelo	NIST CSF	ISO/IEC 27002	OCTAVE Allegro	ISA/IEC 62443	Lubua
Establecer alcance	NC1	IO1	OA0	IA2	
Administración de activos	NC0	IO8	OA1 OA2		LU2
Políticas y Procedimientos	NC9 NC2	IO2 IO3 IO4 IO6		IA0 IA1 IA4 IA5 IA7 IA8	LU1 LU6
Proteger operación	NC5 NC6 NC7 NC8 NC10	IO7 IO9 IO10 IO11 IO12 IO13 IO14 IO15			LU0 LU3 LU5
Identificar Amenazas	NC3 NC4 NC12 NC13 NC14		OA3 OA4	IA9 IA10 IA11	
Mitigar amenazas	NC15 NC16 NC17 NC18		OA5 OA6 OA7		LU4
Cumplimiento		IO17 IO18			LU6

6 Marco de referencia de seguridad para dispositivos IoT,

MaRCIoT

Con el resultado de este análisis comparativo se puede observar el desarrollo del marco de referencia de seguridad para dispositivos IoT, mostrado en Figura 6.1.

Figura 6.1 Marco de referencia de seguridad para IoT utilizando IDS. Elaboración propia.



6.1 Estructura de MaRCIoT

6.1.1 Establecer dirección

El uso efectivo de TI es crítico para el éxito de la estrategia del negocio, por lo que deben de estar alineadas (Nastase et al., 2009). Inicialmente se indicará la dirección del análisis del riesgo y se formalizarán los criterios de medición de riesgos acorde a la misión y visión de la empresa. Se indica el impacto y mitigación de los riesgos en caso de presentarse en los departamentos de una organización de IoT. Para facilitar esta actividad, se tendrán formatos estandarizados para identificar los impactos en la reputación/confianza, clientes, financiero, productividad, penalidades legales y áreas de la organización. (Caralli et al., 2007), catalogados en bajo, medio bajo, medio, medio alto y alto (ver Tabla A1).

6.1.2 Administración de activos de la información

6.1.2.1 Desarrollo de perfil de activos de la información

Se crea el perfil de los activos de IoT de la organización, contando con herramientas automatizadas para escanear la red y dispositivos y tener información consistente (Webb & Hume, 2018), el resguardo de la información se hará en un formato (ver Tabla A2).

6.1.2.2 Identificar los contenedores de los activos de la información

Se identificará los contenedores de los activos de la información de IoT, con información como es su ubicación, el tipo de acceso, el responsable, el tipo físico o lógico y si se trata de un elemento técnico, físico o humano. Controlados por la propia organización o por un tercero (Caralli et al., 2007).

6.1.3 Políticas y Procedimientos

6.1.3.1 Términos y definiciones

Se trata de un glosario de definiciones formales relacionadas a la especialidad de seguridad de información, términos técnicos, esto para evitar ambigüedades y permitan entender el estándar (2021a), también tendrá el contenido relacionado con definiciones y términos de IoT.

6.1.3.2 Organización de la seguridad de la información

Se trata de la definición de roles y responsabilidades para lograr la seguridad de información. Es importante tener roles claros para evitar disconformidades. Esto debe establecer las relaciones entre el personal interno y externo (2021a).

6.1.3.3 Procedimientos y procesos de protección de información

Se trata de una línea base de configuración para los sistemas de IoT para que se mantenga el funcionamiento a través de los principios de seguridad ("An Introduction to the Components of the Framework", 2021).

6.1.4 Proteger operación

6.1.4.1 Operación de activos

Consiste en una administración de seguridad física y ambiental, seguridad de operaciones y de comunicaciones, control de accesos de los sistemas y de los dispositivos de IoT, implementación de criptografía, mantenimiento y desarrollo de los sistemas (2021a).

6.1.4.2 Operación de recursos humanos

El personal interno de la organización y los proveedores deben de tener una educación constante de ciberseguridad, para que sus responsabilidades cumplan las políticas y procedimientos de seguridad de datos (2021a).

6.1.5 Identificar amenazas

Dentro del paso de identificación de amenazas se detectan áreas de preocupación, se definen los escenarios de amenaza, se hace una investigación de escritorio, se hace un cuestionario de ciberseguridad de IoT, se organiza un taller con especialistas (Brass et al., 2018) de TI, se realizan pruebas de seguridad y se genera un reporte.

6.1.5.1 Detectar áreas de preocupación

Para este paso se listan las posibles situaciones que amenazan a los activos de información y a los datos, referidos como áreas de preocupación. El propósito es hacer una captura rápida de las posibles condiciones de amenazas. Se documenta el riesgo de información de activo, donde se asocia la amenaza y el impacto. Se califica al riesgo, el plan de mitigación y las actividades. Los riesgos se pueden agrupar de diferentes maneras en la organización (Caralli et al., 2007).

6.1.5.2 Definir los escenarios de amenaza

Con la información recolectada se definen los escenarios de amenaza. Los escenarios de amenazas están divididos en los técnicos, físicos y de usuarios (Caralli et al., 2007). Para detectar las amenazas técnicas y físicas se utilizará la base de datos de MITRE ATT&CK ICS ("attackics", 2021) (ver Tabla 6.1).

Tabla 6.1 Base de datos de MITRE ATT&CK ICS

MITRE ATT&CK ICS		
Descripción	Estructura	Técnicas
Base de datos de técnicas, tácticas y conocimiento común para simulación, desarrollo de defensa y evaluaciones. Describe el comportamiento de adversarios en una red Industrial	11 tácticas 81 técnicas 50 mitigaciones	1. Acceso Inicial 2. Ejecución 3. Persistencia 4. Escalación de privilegios 5. Evasión 6. Descubrimiento 7. Movimiento lateral 8. Colección 9. Comando y control 10. Funciones de inhibición de respuestas 11. Control de procesos impares

Para identificar las amenazas a los usuarios se usará colaboración abierta. Se define el problema de las amenazas de ciberseguridad en los datos, siendo que los especialistas de TI aporten ideas de cómo solucionarlo. Además, se obtiene información de los sensores, de proveedores de servicios, de redes sociales y de los usuarios finales. Los proveedores de servicios proporcionan la información de los servicios que administran, en las redes sociales se identifica mal uso y se extrae información a través de herramientas. Mientras que se capacita a los usuarios finales para reportar comportamientos inadecuados, ataques, ofensas y para almacenar de manera segura los datos. Esto ayudará a prevenir de las amenazas y coordinar a los individuos contra los ataques (Nieto et al., 2019).

6.1.5.3 Investigación de escritorio sobre guías de seguridad

Se realiza una investigación de escritorio sobre las herramientas que utiliza la empresa, es decir, si ya cuenta con alguna guía de seguridad de IoT, códigos de práctica, especificaciones prácticas de algún organismos públicos o privados (Brass et al., 2018).

6.1.5.4 Cuestionario de ciberseguridad de IoT

Se integra un cuestionario para recolectar y analizar resultados de las prácticas de seguridad de la organización y generar estrategias en la organización. Se utilizan preguntas del cuestionario del modelo de cuestionamientos para la evaluación y mejora, que indica la importancia de revisar y desarrollar las capacidades de ciberseguridad por parte de los proveedores y administradores de servicio. Sirve para tener una consciencia situacional de la madurez de la ciberseguridad de la organización y poder hacer autoevaluaciones para la infraestructura crítica. El cuestionario cuenta con preguntas enfocadas y situacionales (Yigit Ozkan & Spruit, 2019) (ver Tabla A5).

6.1.5.5 Taller con los especialistas y desarrolladores de IoT

Se realizará un taller con los especialistas y desarrolladores de IoT (Brass et al., 2018) para explorar el estado de implementación de las medidas de ciberseguridad de IoT.

6.1.5.6 Pruebas de seguridad

Se detectan vulnerabilidades a través de herramientas especializadas (Shinde & Ardhapurkar, 2016). Se realizan pruebas de seguridad, a través de la explotación de las vulnerabilidades para evaluar la severidad, impacto y explotación, considerando pruebas de penetración con herramientas de Titán y CertifyIT (Matheu-García et al., 2019). Se diseña la prueba, la implementación y la ejecución. Después se instala el ambiente controlado para ejecutar y analizar las pruebas de manera sistemática.

6.1.5.7 Generar reporte

Finalmente se genera un reporte (Shinde & Ardhapurkar, 2016) con el resultado de las subcategorías de detección de áreas de preocupación, definición de los escenarios de amenaza,

investigación de escritorio, cuestionario de ciberseguridad de IoT, taller con especialistas (Brass et al., 2018) de TI y las pruebas de seguridad.

6.1.6 Mitigación de amenazas

Una vez que ya fueron analizadas y descubiertas las vulnerabilidades (Shinde & Ardhapurkar, 2016) a través de la categoría de Identificar amenazas, se procede a identificar riesgos, analizar riesgos y a seleccionar la forma en la que se mitigan las amenazas.

6.1.6.1 Identificar riesgos

El resultado de la categoría de Identificar amenazas sirve de entrada para la fase de identificación de riesgos. Se gestiona la identificación, evaluación y comunicación de riesgos. Basados en los criterios de riesgos de seguridad de información, reconociendo lo relacionado a la pérdida de seguridad y disponibilidad de la información, con el fin de reducir riesgos y maximizar los beneficios de las aplicaciones de IoT (Kandasamy et al., 2020) (ver Tabla A4).

6.1.6.2 Análisis de riesgos

Se trata de una medición cuantitativa del impacto de una amenaza, que considera la importancia de las áreas impactadas (Ali & Awad, 2018) (ver Tabla A3).

6.1.6.3 Seleccionar la mitigación

Se determina que riesgos identificados requieren mitigación y se desarrolla una estrategia para mitigarlos. Priorizando los riesgos por su valor (Ali & Awad, 2018).

6.1.6.3.1 Detección de Intrusos

La defensa contra ataques ha sido con firewalls, antivirus y sistemas de control de accesos de dispositivos inteligentes, también con los sistemas detectores de intrusos (IDS), que están enfocados en monitorear accesos no autorizados u otro ataque. Los IDS pueden ser basados en

detección de firmas y anomalías (Larriva-Novo et al., 2021). Métodos como firewall y control de accesos se enfocan en proveer confidencialidad y autenticidad de datos, pero aún se tienen amenazas de seguridad. Por lo que se necesitan mecanismos de defensa como IDS, capaz de examinar las actividades de red en los dispositivos conectados y generar alertas. El IDS debe de manejar, clasificar y correlacionar las alertas generadas para los protocolos usados en redes IoT (Thakkar & Lohiya, 2021). El IDS es viable, por no necesitar mucha capacidad computacional en los equipos remotos, y las reglas pueden enfocarse a los requisitos del protocolo (Aveleira-Mata et al., 2021).

Una estrategia de la seguridad de datos utilizando un IDS basado en aprendizaje de máquina es conocer al adversario, ser proactivo y protegerse a sí mismo. El aprendizaje de máquina y las técnicas de reconocimiento no son la respuesta definitiva a las amenazas y para prevenir el riesgo de ataques no conocidos, se puede seguir un modelo proactivo, que consiste en anticipar al atacante, primero identificando las amenazas relevantes contra el sistema, diseñando y simulando ataques, después diseñando contramedidas necesarias, finalmente repitiendo el proceso hasta el desarrollo. Para la mitigación de amenazas adversarias también es necesario que los algoritmos de aprendizaje de máquina detecten desconocidos no conocidos usando métodos robustos para anomalías, detección de novedades e incluso con intervención humana (Biggio & Roli, 2018)

Al usar aprendizaje de máquina en el IDS, es importante mantener el control de los datos entrenados, del modelo de detección, del conjunto de características, de Oracle y de la manipulación a fondo. Esto puede ser con las medidas para controlar el acceso a los sistemas y al registro de eventos de IDS, gestionar los privilegios altos de administración para los sistemas de IDS, separar la instalación del modelo de detección y las máquinas de NIDS, mantener en resguardo el proceso de análisis del tráfico, instalar mecanismos de detección complementarios al

IDS para evitar el proceso de ingeniería inversa, almacenar separadamente el registro de los eventos del IDS y diferenciar los posibles ataques (Apruzzese et al., 2021).

6.1.7 Cumplimiento

6.1.7.1 Evaluación

La organización debe de ser revisada o auditada por una organización independiente y entregar el reporte al encargado de ciberseguridad y a la dirección de la empresa. Se debe realizar una evaluación de que los empleados y sistemas están cumpliendo con las políticas de seguridad, procedimientos (2021a).

6.2 Operación del MaRCIoT

El modo de operación del MaRCIoT inicia con Establecer el alcance para Formalizar criterios de riesgos de seguridad. Después se establece la sección de Políticas y Procedimientos, donde se listan los Términos y definiciones sobre IoT y ciberseguridad, se crea la Organización de Seguridad de Información y los Procedimientos y procesos de protección de información. Los Procedimientos y procesos de protección de información servirán de guía para que otras categorías, definan los objetivos, pasos, responsabilidades y entregables. Las categorías a las que dará información son Operación de activos, Operación de recursos humanos, Detectar áreas de preocupación, Definir los escenarios de amenaza, Investigación de escritorio, Cuestionario de ciberseguridad de IoT, Taller con especialistas, Pruebas de Seguridad, Identificar riesgos, Selección de la mitigación, Análisis de riesgos y Manejar incidentes.

Una vez definidos los procedimientos se procederá a Administrar activos de la información, donde se crea el Perfil de activos de la información y se Identifica activos de información, se

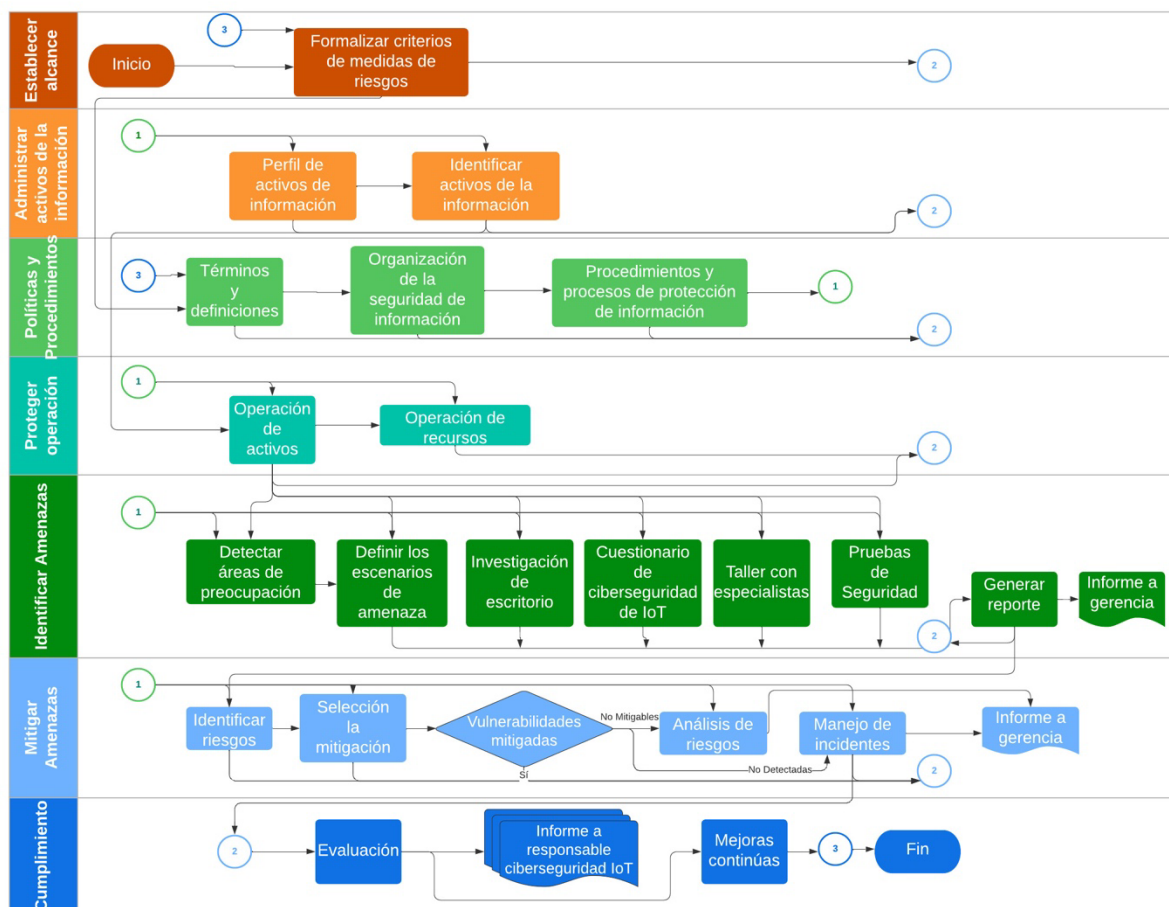
continúa con la categoría de Proteger operación conformado por Operación de activos y Operación de Recursos humanos.

La Operación de activos dará cabida a una de las categorías más importantes Identificar Amenazas, que está compuesta por Detectar áreas de preocupación, Definir los escenarios de amenaza, Investigación de escritorio, Cuestionario de ciberseguridad de IoT, Taller con especialistas y las Pruebas de Seguridad, que tendrán como resultado Generar un reporte para que sea entregado y evaluado por gerencia.

Al tener identificadas las amenazas se seguirá con Mitigar Amenazas, a través de identificar riesgos, analizar de riesgos y seleccionar la mitigación. Si las vulnerabilidades pueden ser mitigadas se procede con la evaluación, pero si las amenazas no pudieron ser mitigables se realiza un Análisis de riesgos. Si alguna vulnerabilidad es explotada se atenderá bajo la categoría de Manejo de incidentes.

En las subcategorías de Identificar Amenazas se documentan los resultados y se integra un Informe para entregar al encargado de ciberseguridad y dirección de la empresa. De igual manera cada subcategoría será evaluada y el resultado conformará un Informe que se entregará al responsable de ciberseguridad de IoT. Basados en estos resultados se realizan Mejoras continuas en las categorías de Formalizar criterios de medidas de riesgos de seguridad, en Términos y definiciones, en la Organización de seguridad de información y en los Procedimientos y procesos de protección de información (ver figura 6.2).

Figura 6.2 *Modo de operación de MaRCIoT (elaboración propia)*



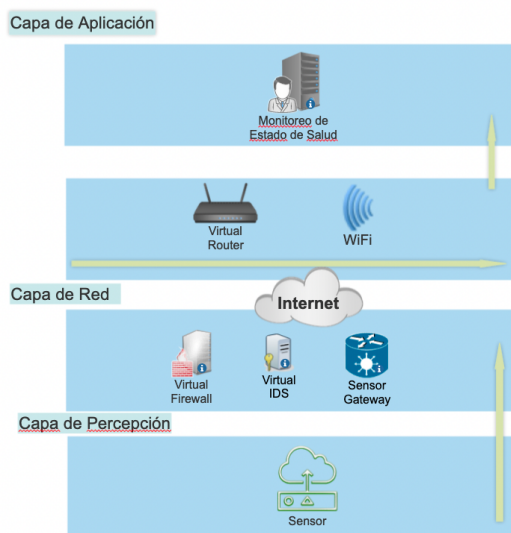
6.3 Políticas y Procedimientos del MaRCIoT

6.3.1 Procedimientos y procesos de protección de información de MaRCIoT

Dentro de la categoría de Políticas y Procedimiento del MaRCIoT en la subcategoría Procedimientos y procesos de protección de información se define la Arquitectura de MaRCIoT. Que considera la arquitectura de IoT con la capa de percepción, de red y de aplicación. En la capa de percepción se tendrá un sensor de IoT que enviará los datos recolectados a la puerta de enlace para que salga por un firewall y un IDS virtual, este último estará sobre la plataforma de código

abierto. Adicional se usará una salida de Internet para que el sensor pueda comunicarse con la plataforma de monitoreo de estado de salud localizado en la nube de Internet (ver Figura 6.3).

Figura 6.3 *Arquitectura de MaRCIoT para las pruebas*



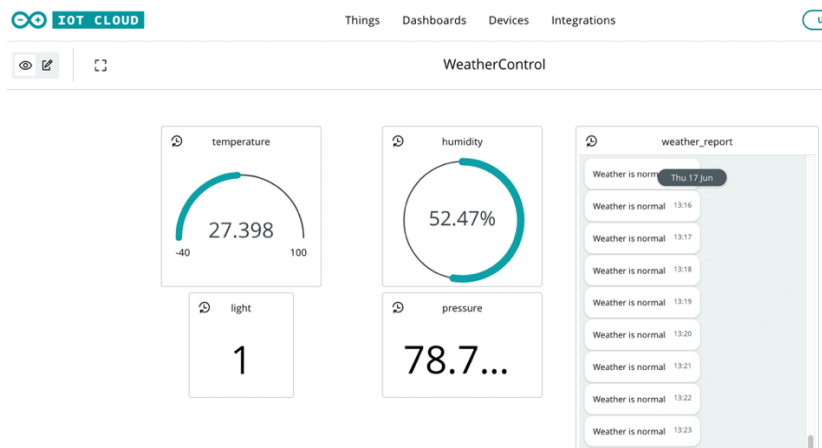
6.4 Proteger operación de MaRCIoT

Dentro de la subcategoría de Operación de activos en la categoría de Proteger operación se lista el detalle de las capas de la arquitectura del modelo de ciberseguridad de IoT para las pruebas.

- a) Capa de aplicación – en este nivel esta la aplicación que se interconecta con el sensor de temperatura, para la recepción y análisis de datos. Para lo que se utiliza una plataforma de Arduino en la nube IoT que recolecta y despliega los datos del sensor (ver Figura 6.4)

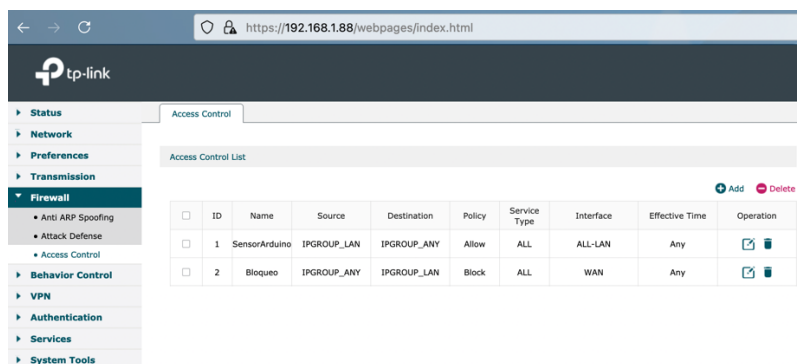
En la aplicación se configura una Estación del estado del clima, que registra y monitorea las condiciones de temperatura, humedad, luz y presión del medio ambiente. Se accede por la URL, <https://create.arduino.cc/>.

Figura 6.4 *Plataforma de la nube de IoT para recolección de datos del sensor*



- b) Capa de red – en este nivel se instalará un firewall virtual y un IDS de plataforma abierta Suricata, después la comunicación se enviará a Internet a través de una red inalámbrica.
- Firewall– está instalado en un dispositivo TP-Link R605, donde se permite el tráfico desde la red interna hacia Internet y se bloquea todo el tráfico desde Internet a la red interna (ver Figura 6.5).

Figura 6.5 Firewall que pertenece a la capa de red



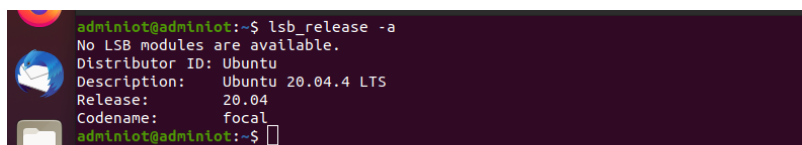
ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
1	SensorArduino	IPGROUP_LAN	IPGROUP_ANY	Allow	ALL	ALL-LAN	Any	[Edit] [Delete]
2	Bloqueo	IPGROUP_ANY	IPGROUP_LAN	Block	ALL	WAN	Any	[Edit] [Delete]

- IDS en plataforma abierta – se usará el IDS de plataforma abierta con Suricata. Dado que (Park & Ahn, 2017) analizaron y compararon el procesamiento y la tasa de detección de Snort y Suricata, a través de la experimentación en ambientes operativos. Resultando que Snort es un IDS de código abierto con limitaciones para los requerimientos actuales, como el procesamiento de un sólo proceso, pero aventajando en su estabilidad

y detección de paquetes. Por otro lado, Suricata cubre las desventajas de Snort, procesa los paquetes en un ambiente de múltiples procesos. Concluyen que, si el usuario quiere implementar un IDS con poco CPU, Snort es una mejor solución, pero si se necesita mejor tasa de detección Suricata es la opción.

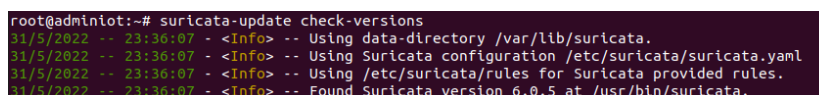
Se instala una máquina virtual con sistema operativo Ubuntu 20.04.4 (ver Figura 6.6), donde se configura el software Suricata con la versión 6.0.5 (ver Figura 6.7).

Figura 6.6 Máquina virtual para IDS



```
adminiot@adminiot:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.4 LTS
Release:        20.04
Codename:       focal
adminiot@adminiot:~$
```

Figura 6.7 IDS en plataforma Suricata



```
root@adminiot:~# suricata-update check-versions
31/5/2022 -- 23:36:07 - <Info> -- Using data-directory /var/lib/suricata.
31/5/2022 -- 23:36:07 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
31/5/2022 -- 23:36:07 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
31/5/2022 -- 23:36:07 - <Info> -- Found Suricata version 6.0.5 at /usr/bin/suricata.
```

- Punto de acceso (en inglés, Access Point) – se utiliza un dispositivo M4 WiLink 3 para la propagación de la red inalámbrica para la comunicación del sensor Arduino Oplà hacia Internet (ver Figura 6.8).
- Switch – configurado en un dispositivo TP-Link R605. En este se configurará un puerto en modo “espejo” del puerto físico donde está conectado el Punto de Acceso. Esto para monitorear el tráfico del sensor y de la PC de pruebas (ver Figura 6.9).
- Router – se usará un dispositivo TP-Link R605 para la recepción del enlace de Internet. También tendrá el servicio de asignación de IPs dinámicas, DHCP (en inglés, Dynamic Host Configuration Protocol) (ver Figura 6.10).

Figura 6.8 Punto de acceso para red inalámbrica

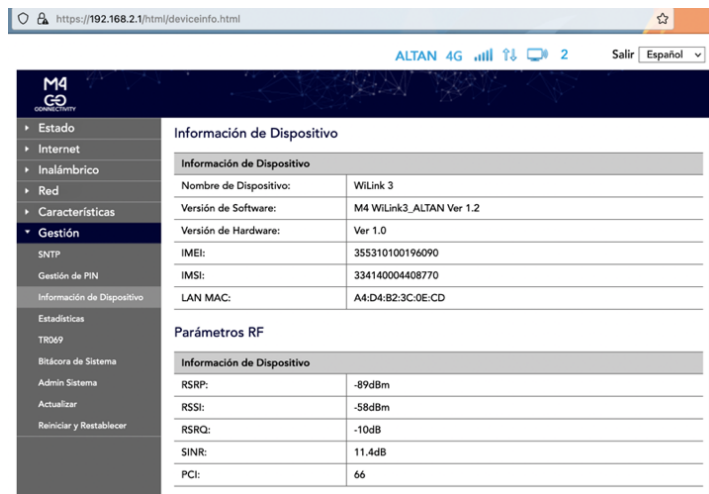


Figura 6.9 Switch con puerto en modo “espejo”

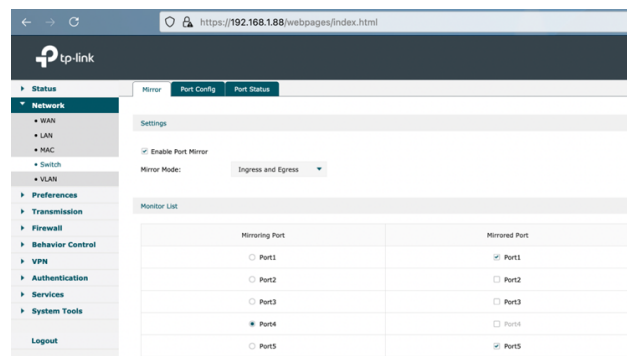
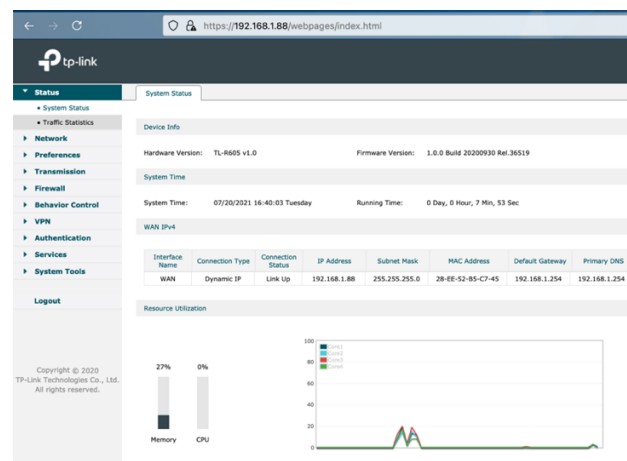


Figura 6.10 Router para conexión hacia Internet



- Internet residencial - utiliza el modem Huawei Hg8145v5 y un ancho de banda de 30 Mbps con el proveedor de Internet infinitum.
- c) Capa de percepción – para las pruebas se selecciona el dispositivo de Arduino Oplà, con sensores de temperatura, presión atmosférica, humedad de IoT. Siendo que (Morais et al., 2019) clasifican en 19 categorías la dinámica de IoT, considerando aplicaciones, escenarios y sensores, proveyendo una técnica de integración analítica de calificación de sensores. Las categorías son ambiente, movimiento, eléctrico, bio-sensores, identificación, posicionamiento, presencia, visión de máquina, interacción, acústica, fuerza/carga, hidráulico, químico, información de objeto. E identifican que la gran mayoría de sensores se encuentran en la clasificación de sensores de ambiente, siendo los más comunes los sensores que monitorean la temperatura, luz y humedad (ver Figura 6.11), por lo que estos últimos son seleccionados en la fase de pruebas.

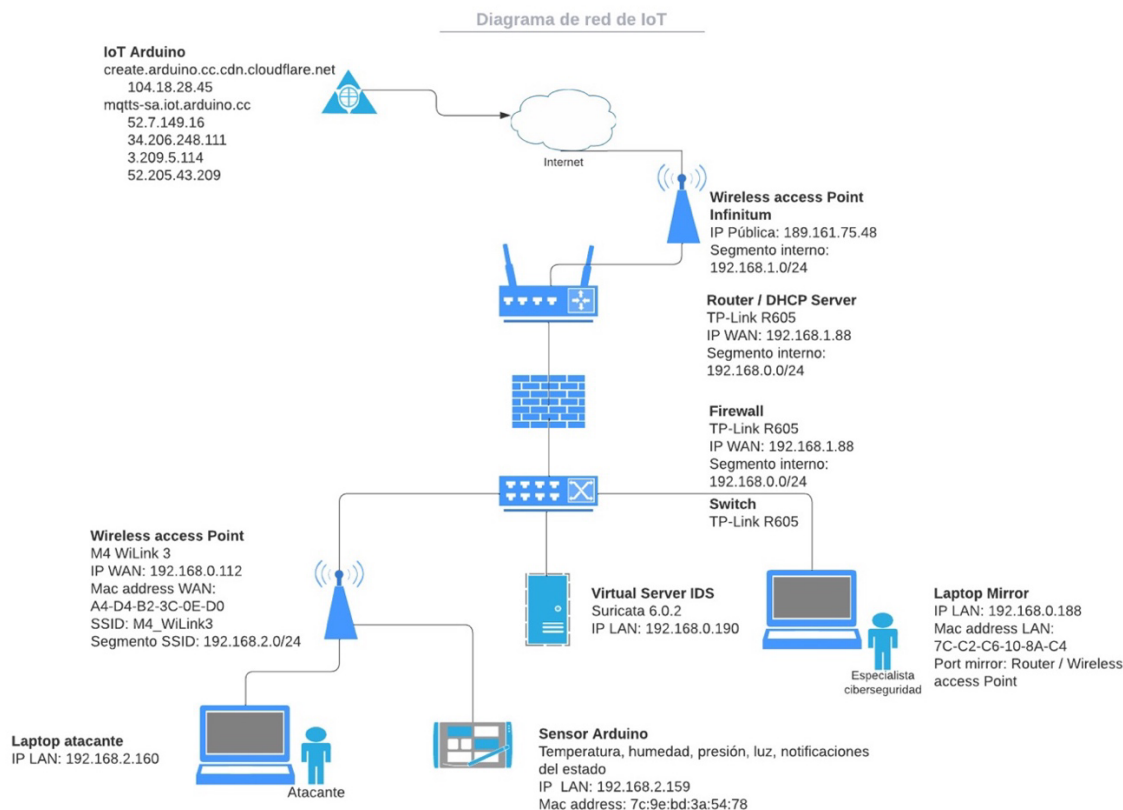
Figura 6.11 *Dispositivo sensor de Ardino Oplà*



6.4.1 Diagrama de red de MaRCIoT

Se muestra un diagrama de red del modelo de ciberseguridad de IoT para las pruebas (ver Figura 6.12).

Figura 6.12 Diagrama de red del modelo de ciberseguridad de IoT



Se tiene configuradas las zonas internas, DMZ y externas; utilizando los segmentos de red de la siguiente manera, para la zona interna inalámbrica el 192.168.2.0/24, para la zona interna cableada el 192.168.0.0/24 y para la red de la DMZ el 192.168.1.0/24 (Ver Tabla 6.2).

Tabla 6.2 Direcciones IP asignadas en modelo de ciberseguridad de IoT para las pruebas

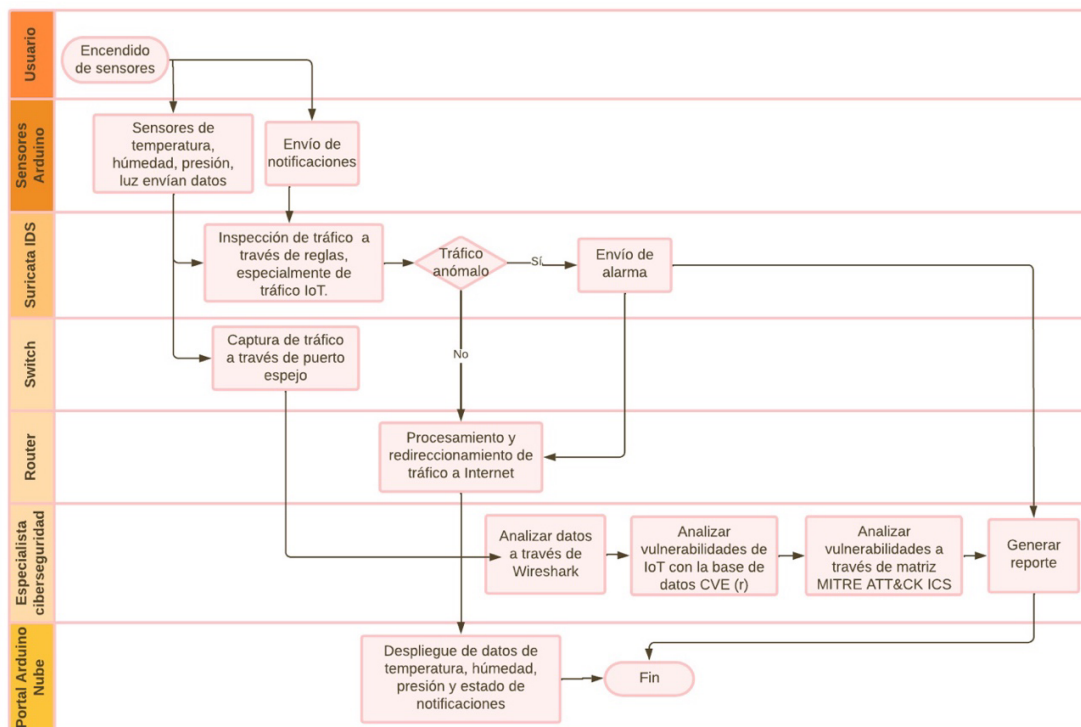
Zona	Componentes	Dirección IP	Descripción
Interna inalámbrica	Laptop de pruebas	192.168.2.160	Laptop para enviar tráfico de simulación de ataque de seguridad
Interna inalámbrica	Sensores Arduino	192.168.2.159	Sensores Arduino Oplà de temperatura, humedad, presión y luz del medio ambiente
Interna cableada	Punto de acceso inalámbrico	192.168.0.112	Dispositivo M4 WiLink 3 que propaga la red inalámbrica para los sensores Arduino

Interna cableada	Laptop de puerto espejo	192.168.0.188	Equipo que detecta el tráfico de la red, a través de un puerto en modo espejo.
Interna cableada	IDS	192.168.0.190	Detector de intrusos sobre la plataforma de Suricata versión 6.0.5.
Zona DMZ	Firewall/Router/Servidor DHCP	192.168.1.88	Dispositivo de red, TP-Link R605, con funcionalidades de firewall, router y servidor DHCP.
Internet	Plataforma de la nube IoT	104.18.28.45	Plataforma en Internet que recolecta la información que es enviada por los sensores de Arduino en una red local. Se accede por la URL, create.arduino.cc/cdn.cloudflare.net

6.4.2 Flujo de operacional de MaRCIoT

Se muestra el diagrama operacional de las pruebas del MaRCIoT (ver Figura 6.13).

Figura 6.13 Diagrama operación de las pruebas del modelo de ciberseguridad de IoT, MaRCIoT



Se indican las funciones del usuario, de los sensores Arduino de temperatura, humedad, presión y la notificación del estado; del IDS en plataforma Suricata para inspeccionar tráfico. Se apuntan las funcionalidades del switch y router para procesamiento y envío del tráfico hacia Internet. También se señalan las actividades que realizan los especialistas de seguridad de IT. Y como último paso se demuestra la funcionalidad del portal de la nube de Arduino, que es desplegar la información que fue enviada por los sensores.

6.4.3 Análisis del tráfico normal a través de Wireshark

Se activan los sensores de Arduino Oplà y se configuran con conexión a la red inalámbrica para la salida a Internet. El tráfico de los sensores de humedad, temperatura, presión y luz se envía hacia la plataforma de la nube de IoT de Arduino en Internet.

Se configura en el switch un puerto en modo espejo, donde se detecta el tráfico que se transfiere entre los sensores de Arduino hacia Internet. Se analiza esta captura de tráfico utilizando la herramienta Wireshark a lo que se tienen los siguientes comentarios:

La comunicación entre el sensor y la plataforma IoT (ver Figura 6.14) tiene los siguientes datos. La dirección IP origen es la 192.168.0.112, que pertenece al dispositivo AP y la dirección IP destino es la 52.7.149.16 que corresponde a Amazon Technologies Inc y esta comunicación utiliza el protocolo: TLS v1.2.

Figura 6.14 Comunicación entre el sensor y plataforma IoT

No.	Time	Source	Destination	Protocol	Length	Info
413	7.855665	192.168.0.112	52.7.149.16	TLSv1.2	132	Application Data
416	7.918432	52.7.149.16	192.168.0.112	TCP	60	8883 → 44287 [ACK] Seq=1 Ack=1435 Win=60568 Len=0
417	8.034291	192.168.0.112	52.7.149.16	TLSv1.2	149	Application Data
420	8.097852	52.7.149.16	192.168.0.112	TCP	60	8883 → 44287 [ACK] Seq=1 Ack=1530 Win=60568 Len=0
423	8.936194	192.168.0.112	52.7.149.16	TLSv1.2	132	Application Data
438	8.998727	52.7.149.16	192.168.0.112	TCP	60	8883 → 44287 [ACK] Seq=1 Ack=1608 Win=60568 Len=0
459	9.057954	192.168.0.112	52.7.149.16	TLSv1.2	149	Application Data
462	9.121089	52.7.149.16	192.168.0.112	TCP	60	8883 → 44287 [ACK] Seq=1 Ack=1783 Win=60568 Len=0
483	10.016926	192.168.0.112	52.7.149.16	TLSv1.2	132	Application Data
490	10.079265	52.7.149.16	192.168.0.112	TCP	60	8883 → 44287 [ACK] Seq=1 Ack=1781 Win=60568 Len=0
501	10.184224	192.168.0.112	52.7.149.16	TLSv1.2	149	Application Data
504	10.246891	52.7.149.16	192.168.0.112	TCP	60	8883 → 44287 [ACK] Seq=1 Ack=1876 Win=60568 Len=0
525	10.287688	192.168.0.112	52.7.149.16	TLSv1.2	85	Application Data
534	10.358407	52.7.149.16	192.168.0.112	TCP	60	8883 → 44287 [ACK] Seq=1 Ack=1907 Win=60568 Len=0
536	10.358547	52.7.149.16	192.168.0.112	TLSv1.2	85	Application Data
537	10.389596	192.168.0.112	52.7.149.16	TCP	60	44287 → 8883 [ACK] Seq=1907 Ack=32 Win=4491 Len=0

Se observa que los protocolos utilizados son el TLS v.2 en la capa de transporte y el MQTT como protocolo de aplicación de datos (ver Figura 6.15).

Figura 6.15 *Protocolo de aplicación de datos*

```

Transport Layer Security
  TLSv1.2 Record Layer: Application Data Protocol: mqtt
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 90
    Encrypted Application Data: 0000000000000000d0b1d5a2bdcc95792c9607f3c435d5f0ca1b204555a30b6e274548c62...
    [Application Data Protocol: mqtt]
  
```

Se listan las URLs/IPs de la plataforma de IoT para la administración de los datos que fueron enviados desde los sensores de humedad, presión, temperatura y luz (ver Tabla 6.3).

Tabla 6.3 *Comunicación destino para plataforma de IoT de Arduino Oplà*

Descripción	URLs	IPs
Plataforma de administración de Oplà IoT Arduino	create.arduino.cc	create.arduino.cc.cdn.cloudflare.net
	create.arduino.cc.cdn.cloudflare.net	104.18.28.45
Transferencia de datos desde los sensores Arduino	mqttps-sa.iot.arduino.cc	52.7.149.16 34.206.248.111 3.209.5.114 52.205.43.209
	arduino-prod-cd-7d4guw5p2tbeio38.edge.tenants.auth0.com	104.16.184.248
	login.arduino.cc	arduino-prod-cd-7d4guw5p2tbeio38.edge.tenants.auth0.com
	arduino-prod-cd-7d4guw5p2tbeio38.edge.tenants.auth0.com	104.16.184.248
	api2.arduino.cc	18.208.79.82, 52.200.135.167, 34.228.138.192, 34.194.93.225
	content.arduino.cc	content.arduino.cc.cdn.cloudflare.net

El tráfico detectado pertenece al protocolo TLS en un 33.6% (ver Figura 6.16).

Figura 6.16 *Cantidad de tráfico, protocolo TLS*

Protocolo	Porcentaje	Cantidad	Porcentaje	Cantidad	Cantidad	Cantidad
Transmission Control Protocol	79.0	30964	75.0	7901052	86k	17708
VSS Monitoring Ethernet trailer	1.7	661	0.0	1322	14	661
Transport Layer Security	33.6	13149	67.7	7125270	77k	12581
Malformed Packet	0.0	4	0.0	0	0	4
Internet Group Management Protocol	0.1	46	0.0	368	4	46
Internet Control Message Protocol	0.2	74	0.1	5806	63	74

6.4.4 Inspección del tráfico utilizando IDS en la plataforma Suricata

Con base en el análisis del tráfico realizado con la herramienta de Wireshark y Suricata, se detecta que los datos de los sensores de humedad, temperatura, presión y luz utilizan en la capa de transporte el protocolo TLS v1.2 y el protocolo MQTT en la aplicación de datos. La inspección se realizará en la capa de aplicación de datos, por lo que el enfoque se realizará sobre MQTT. Para esta inspección del tráfico se usa el detector de intrusos de código abierto, Suricata versión 6.0.5. Este cuenta con una estructura de archivos referentes a la configuración, firmas, entre otros (ver Figura 6.17).

Figura 6.17 Estructura de Suricata 6.0.5

github	github: work around rustic mingw issue	2 months ago
benches	Initial add of the files.	12 years ago
contrib	src: remove files	2 years ago
doc	doc: Grammar Correction	20 days ago
etop	etop: fix gre encapsulation in xdp_b	3 months ago
etc	classification: sync and update	5 months ago
lua	lua output: Update example script to match style of user doc exam...	3 years ago
m4	prelude: update URL	5 years ago
python	doc: Improve grammar, spelling and clarifications	11 months ago
sa	general: Cleanup bool usage	3 months ago
rules	ike: set event for multiple server proposals	3 months ago
rust	modbus: do not claim to handle gaps	20 days ago
scripts	templates: fix typos	4 months ago
src	detect/prep: convert to FAIL/PASS API	20 days ago
suricata-update	python: fixes for installing from path with spaces	2 years ago
clang-format	common: Add clang-format file	11 months ago
gitignore	libsuricata-config: program to print build flags	5 months ago
COPYING	GPL license sync with official gpl-2.0.txt	6 years ago
ChangeLog	changelog: update for 6.0.1	6 months ago
LICENSE	GPL license sync with official gpl-2.0.txt	6 years ago
Makefile.am	install: better warning on install-fail and don't fail	4 months ago
Makefile.cvs	Initial add of the files.	12 years ago
README.md	github: add codecov badge	6 months ago
acsite.m4	configure: check for _Int and friends	15 months ago
autogen.sh	autogen/rust: remove Cargo.lock	4 years ago
config.rpath	Add file needed for some autotools version.	8 years ago
configure.ac	util/etop: fix deprecation warning	3 months ago
doxygen.cfg	doxygen: update config from 1.8.4 to 1.8.17	17 months ago
libsuricata-config.in	libsuricata-config: program to print build flags	5 months ago
suricata.yam1.in	mgt: move subsubsub limits into app-layer config	29 days ago
threshold.config	docs: replace redmine links and enforce https on old urls	4 years ago
README.md		

Nota. (GitHub - OISF/suricata:Suricata git repository maintained by the OISF, 2021)

La captura de tráfico también es analizada con la herramienta Suricata 6.0.3, donde se procesa el archivo pcap con las reglas predeterminadas de la herramienta (ver Figura 6.18) y se tienen los siguientes comentarios:

Figura 6.18 *Análisis de tráfico con Suricata*

```
root@ubuntu:/home/adminubuntu# suricata -c /etc/suricata/suricata.yaml -r /home/adminubuntu/Documents/
capt-mirror-lan-wan-3.pcapng -l /var/log/suricata
21/7/2021 -- 01:09:39 - <Notice> - This is Suricata version 6.0.3 RELEASE running in USER mode
21/7/2021 -- 01:09:49 - <Notice> - all 9 packet processing threads, 4 management threads initialized,
engine started.
21/7/2021 -- 01:09:49 - <Notice> - Signal Received. Stopping engine.
21/7/2021 -- 01:09:50 - <Notice> - Pcap-file module read 1 files, 23480 packets, 5887904 bytes
root@ubuntu:/home/adminubuntu#
```

Se inspecciona el archivo de reglas, que contiene 27463 firmas de inspección, 1236 reglas del protocolo IP, 4199 reglas de inspección de payload, 21786 reglas de inspección de capa de aplicación y 107 de eventos de decodificación. No hay paquetes con checksum inválidos y se detectan 42 alertas (ver Figura 6.19).

Figura 6.19 *Registro de la inspección de Suricata*

```
root@ubuntu:/home/adminubuntu# tail -17 /var/log/suricata/suricata.log
21/7/2021 -- 01:09:39 - <Notice> - This is Suricata version 6.0.3 RELEASE running in USER mode
21/7/2021 -- 01:09:39 - <Info> - CPUs/cores online: 8
21/7/2021 -- 01:09:39 - <Info> - fast output device (regular) initialized: fast.log
21/7/2021 -- 01:09:39 - <Info> - eve-log output device (regular) initialized: eve.json
21/7/2021 -- 01:09:39 - <Info> - stats output device (regular) initialized: stats.log
21/7/2021 -- 01:09:39 - <Info> - 2 rule files processed. 27459 rules successfully loaded, 0 rules fail
ed
21/7/2021 -- 01:09:39 - <Info> - Threshold config parsed: 0 rule(s) found
21/7/2021 -- 01:09:40 - <Info> - 27463 signatures processed. 1236 are IP-only rules, 4199 are inspecti
ng packet payload, 21786 inspect application layer, 107 are decoder event only
21/7/2021 -- 01:09:49 - <Notice> - all 9 packet processing threads, 4 management threads initialized,
engine started.
21/7/2021 -- 01:09:49 - <Info> - Starting file run for /home/adminubuntu/Documents/capt-mirror-lan-wan
-3.pcapng
21/7/2021 -- 01:09:49 - <Info> - No packets with invalid checksum, assuming checksum offloading is NOT
used
21/7/2021 -- 01:09:49 - <Info> - pcap file /home/adminubuntu/Documents/capt-mirror-lan-wan-3.pcapng en
d of file reached (pcap err code 0)
21/7/2021 -- 01:09:49 - <Notice> - Signal Received. Stopping engine.
21/7/2021 -- 01:09:50 - <Info> - time elapsed 1.322s
21/7/2021 -- 01:09:50 - <Notice> - Pcap-file module read 1 files, 23480 packets, 5887904 bytes
21/7/2021 -- 01:09:50 - <Info> - Alerts: 42
21/7/2021 -- 01:09:50 - <Info> - cleaning up signature grouping structure... complete
root@ubuntu:/home/adminubuntu#
```

Las alertas hacen referencia a que se reenvían paquetes con la etiqueta de tiempo inválido entre el router y un sitio de Internet con IP 142.250.81.10 (ver Figura 6.20).

Figura 6.20 *Alertas de tráfico*

```
root@ubuntu:/var/log/suricata# tail -30 fast.log
06/15/2021-18:17:09.572049 [**] [1:2027758:5] ET DNS Query for .cc TLD [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.88:53750 -> 192.168.1.254:53
06/15/2021-18:17:25.681835 [**] [1:2027758:5] ET DNS Query for .cc TLD [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.88:53750 -> 192.168.1.254:53
06/15/2021-18:17:25.682185 [**] [1:2027758:5] ET DNS Query for .cc TLD [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.88:53750 -> 192.168.1.254:53
06/15/2021-18:17:32.688336 [**] [1:2027758:5] ET DNS Query for .cc TLD [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.88:53750 -> 192.168.1.254:53
06/15/2021-18:17:32.688818 [**] [1:2027758:5] ET DNS Query for .cc TLD [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.88:53750 -> 192.168.1.254:53
06/15/2021-18:17:33.854408 [**] [1:2230003:1] SURICATA TLS invalid handshake message [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 52.7.149.16:8883 -> 192.168.0.112:44287
06/15/2021-18:17:33.854408 [**] [1:2230010:1] SURICATA TLS invalid record/traffic [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 52.7.149.16:8883 -> 192.168.0.112:44287
06/15/2021-18:17:58.739125 [**] [1:2027758:5] ET DNS Query for .cc TLD [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.88:53750 -> 192.168.1.254:53
06/15/2021-18:17:58.739553 [**] [1:2027758:5] ET DNS Query for .cc TLD [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.88:53750 -> 192.168.1.254:53
06/15/2021-18:17:33.893577 [**] [1:2230003:1] SURICATA TLS invalid handshake message [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.0.112:44287 -> 52.7.149.16:8883
06/15/2021-18:17:33.893577 [**] [1:2230010:1] SURICATA TLS invalid record/traffic [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.0.112:44287 -> 52.7.149.16:8883
```

6.5 Identificar amenazas

Dentro de la subcategoría Pruebas de seguridad en la categoría Identificar amenazas se simulan los ataques de ciberseguridad. Se hace uso de la herramienta Kali Linux de código abierto. El IDS Suricata tiene previamente configuradas reglas para inspeccionar el tráfico y que realizan acciones como alertar, pasar, rechazar el tráfico para protocolos básicos de TCP, UDP, ICMP, IP y también para protocolos de aplicación como son HTTP, FTP, TLS, DNS, SSH, SMTP, NTP, DHCP, TFPT, SIP2. Las reglas tienen definido el origen, el destino, los puertos de red utilizados y el flujo de direccionamiento de tráfico. También se configuran las opciones relacionadas a los protocolos de red y a la clasificación de los eventos detectados (6. Suricata Rules — Suricata 6.0.3 documentation, 2021).

Las reglas previamente configuradas están relacionadas a la capa de aplicación, DHCP, DNP, DNS, HTTP, IPSEC, KERBEROS, MQTT, NFS, NTP, SMB, SMTP, SSH, TLS, entre otros. Se muestran las reglas predeterminadas en Suricata para el protocolo de MQTT, en éstas se indica la acción, el protocolo, el origen, el puerto origen, el destino, el puerto destino, las opciones del mensaje, las opciones de la capa de aplicación, la clasificación, el número identificador y la versión

(ver Tabla 6.4). Con estas reglas se alertará cuando a un paquete del protocolo MQTT le falte el evento de conectado, publicado, subscripción, no-subscripción, doble conexión, mensaje, nivel inválido de QoS, mensaje de ID y mensaje de tipo no asignado.

Tabla 6.4 Reglas predeterminadas de MQTT en Suricata

Acción/Protocolo/Origen/Puerto/Destino/Puerto/Opciones	Opción de capa de aplicación	Clasificación	Identificador	Versión
alert mqtt any any -> any any (msg:"SURICATA MQTT CONNECT not seen before CONNACK"	app-layer-event:mqtt.missing_connect	classtype:protocol-command-decode	sid:2229000	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT PUBLISH not seen before PUBACK/PUBREL/PUBREC/PUBCOMP"	app-layer-event:mqtt.missing_publish	classtype:protocol-command-decode	sid:2229001	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT SUBSCRIBE not seen before SUBACK"	app-layer-event:mqtt.missing_subscribe	classtype:protocol-command-decode	sid:2229002	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT UNSUBSCRIBE not seen before UNSUBACK"	app-layer-event:mqtt.missing_unsubscribe	classtype:protocol-command-decode	sid:2229003	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT duplicate CONNECT"	app-layer-event:mqtt.double_connect	classtype:protocol-command-decode	sid:2229004	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT message seen before CONNECT/CONNACK completion"	app-layer-event:mqtt.unintroduced_message	classtype:protocol-command-decode	sid:2229005	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT invalid QoS level"	app-layer-event:mqtt.invalid_qos_level	classtype:protocol-command-decode	sid:2229006	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT missing message ID"	app-layer-event:mqtt.missing_msg_id	classtype:protocol-command-decode	sid:2229007	rev:1)
alert mqtt any any -> any any (msg:"SURICATA MQTT unassigned message type (0 or >15)"	app-layer-event:mqtt.unassigned_msg_type	classtype:protocol-command-decode	sid:2229008	rev:1)

6.5.1 Simulación de ataques de ciberseguridad

Se realizan simulaciones de ataques de ciberseguridad hacia los sensores Arduino. Como primer ataque simulado, se hace una búsqueda de la contraseña a los sensores Arduino utilizando fuerza bruta a través de la herramienta Hydra. Se intenta establecer la comunicación por el puerto de red SSH. Como resultado la conexión fue refutada por el dispositivo Arduino, por lo que no se pudo obtener la contraseña (ver Figura 6.21).

Figura 6.21 Búsqueda de contraseña con herramienta Hydra.

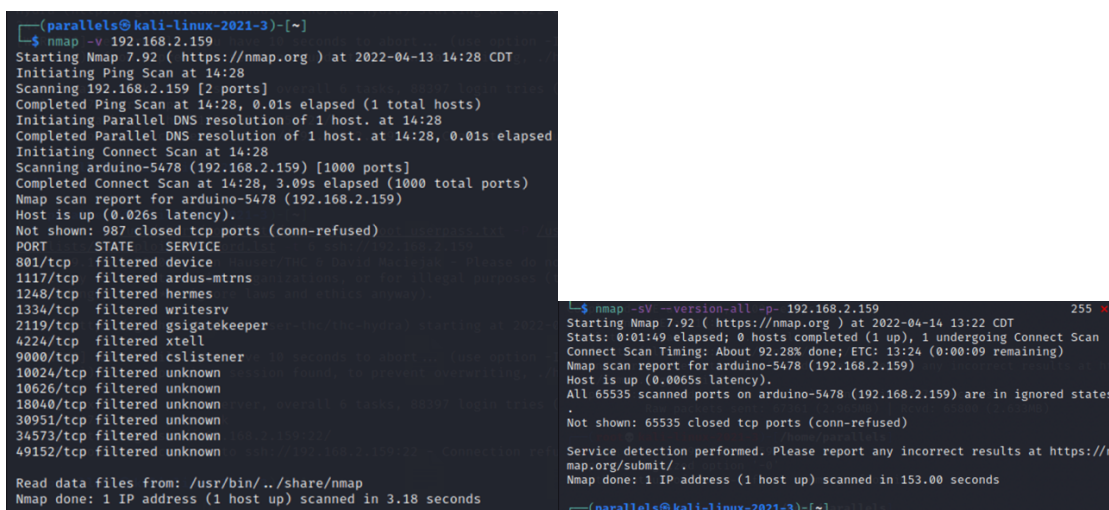
```
(parallels@kali-linux-2021-3)-[~]
$ hydra -l /usr/share/wordlists/metasploit/root_userpass.txt -P /usr/share/wordlists/metasploit/password.lst -i 6 ssh://192.168.2.159
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-13 14:24:49
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 6 tasks per 1 server, overall 6 tasks, 88397 login tries (l:1/p:88397), ~14733 tries per task
[DATA] attacking ssh://192.168.2.159:22/
[ERROR] could not connect to ssh://192.168.2.159:22 - Connection refused

(parallels@kali-linux-2021-3)-[~]
```

El siguiente ataque de ciberseguridad, es el escaneo de los puertos de red en el sensor de Arduino, utilizando las herramientas de nmap y sslscan. Con nmap se detecta en el primer escaneo los puertos tcp abiertos 801, 1117, 1248, 1334, 2119, 4224, 9000, 10024, 10626, 18040, 30951, 34573, 49152, usando el comando “nmap -v 192.168.2.159”. En el segundo escaneo los puertos se muestran en estado ignorado con el comando “nmap -sV --version-all -p- 192.168.2.159” (ver Figura 6.22). Con sslscan se muestra el puerto de red SSH cerrado al ejecutar el comando “sslscan 192.168.2.159” (Figura 6.23).

Figura 6.22 Escaneo de puertos en los sensores de Arduino.



```
(parallels@kali-linux-2021-3)-[~]
$ nmap -v 192.168.2.159
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 14:28 CDT
Initiating Ping Scan at 14:28
Scanning 192.168.2.159 [2 ports]
Completed Ping Scan at 14:28, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:28
Completed Parallel DNS resolution of 1 host. at 14:28, 0.01s elapsed
Initiating Connect Scan at 14:28
Scanning arduino-5478 (192.168.2.159) [1000 ports]
Completed Connect Scan at 14:28, 3.09s elapsed (1000 total ports)
Nmap scan report for arduino-5478 (192.168.2.159)
Host is up (0.026s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
801/tcp    filtered device
1117/tcp   filtered ardu-mtrns
1248/tcp   filtered hermes
1334/tcp   filtered writesrv
2119/tcp   filtered gsgatekeeper
4224/tcp   filtered xtell
9000/tcp   filtered cslistener
10024/tcp  filtered unknown
10626/tcp  filtered unknown
18040/tcp  filtered unknown
30951/tcp  filtered unknown
34573/tcp  filtered unknown
49152/tcp  filtered unknown

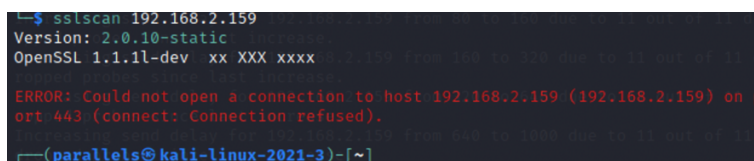
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds

(parallels@kali-linux-2021-3)-[~]
$ nmap -sV --version-all -p- 192.168.2.159
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-14 13:22 CDT
Stats: 0:01:49 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.28% done; ETC: 13:24 (0:00:09 remaining)
Nmap scan report for arduino-5478 (192.168.2.159)
Host is up (0.0065s latency).
All 65535 scanned ports on arduino-5478 (192.168.2.159) are in ignored states
Not shown: 65535 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 153.00 seconds

(parallels@kali-linux-2021-3)-[~]
```

Figura 6.23 Escaneo de puertos en los sensores de Arduino.



```
--$ sslscan 192.168.2.159
Version: 2.0.10-static
OpenSSL 1.1.1l-dev xx XXX xxxx

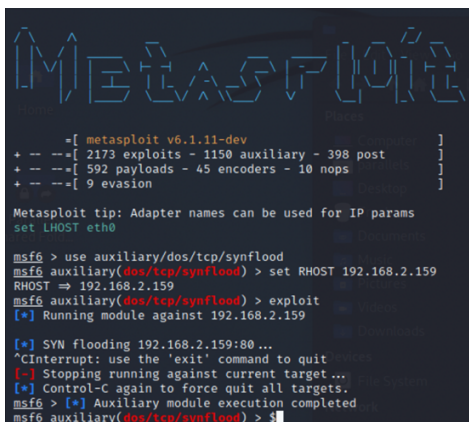
ERROR: Could not open a connection to host 192.168.2.159 (192.168.2.159) on p
ort 443 (connect: Connection refused).

(parallels@kali-linux-2021-3)-[~]
```

Después se simula un ataque DoS a los sensores Arduino por el puerto 80 (ver Figura 6.24) y por el puerto 8443 (ver Figura 6.25), usando la herramienta Metasploit. Cuando el ataque DoS se realiza por el puerto 80 el sensor Arduino sigue mandando información con lentitud a la

plataforma de IoT en la nube, sin embargo, cuando se realiza dirigido al puerto 8443 el sensor ya no puede comunicarse con la plataforma de IoT en la nube, esto porque es el puerto que utiliza el dispositivo para transmisión de datos.

Figura 6.24 *Ataque DoS a los sensores de Arduino por el puerto 80*



```

Metasploit

=[ metasploit v6.1.11-dev ]
+ -- --[ 2173 exploits - 1150 auxiliary - 398 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 9 evasion ]

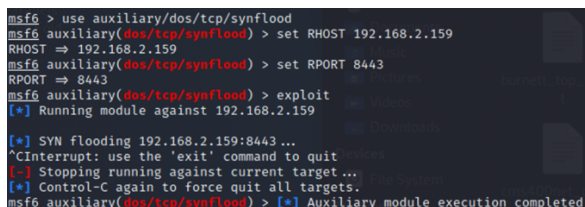
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.2.159
RHOST => 192.168.2.159
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.2.159

[*] SYN flooding 192.168.2.159:80...
^CInterrupt: use the 'exit' command to quit
[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
msf6 > [*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >

```

Figura 6.25 *Ataque DoS a los sensores de Arduino por el puerto 8443*



```

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.2.159
RHOST => 192.168.2.159
msf6 auxiliary(dos/tcp/synflood) > set RPORT 8443
RPORT => 8443
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.2.159

[*] SYN flooding 192.168.2.159:8443...
^CInterrupt: use the 'exit' command to quit
[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
msf6 auxiliary(dos/tcp/synflood) > [*] Auxiliary module execution completed

```

6.7.3 Análisis del tráfico a través de Wireshark

Se configura en el switch un puerto en modo espejo para detectar el tráfico que se transfiere de los sensores Arduino hacia la nube pública de IoT. Seguido, se analiza el tráfico generado durante la simulación de ataques usando la herramienta Wireshark. Se detecta un incremento en los paquetes transmitidos a 2000 paquetes/segundo (ver Figura 6.26) durante el escaneo de los puertos de red, es decir, es una transmisión de 7.56 Mbs en 6.56 minutos (ver Figura 6.27).

Figura 6.26 Escaneo de puertos de red a los sensores Arduino. Paquetes/segundo.

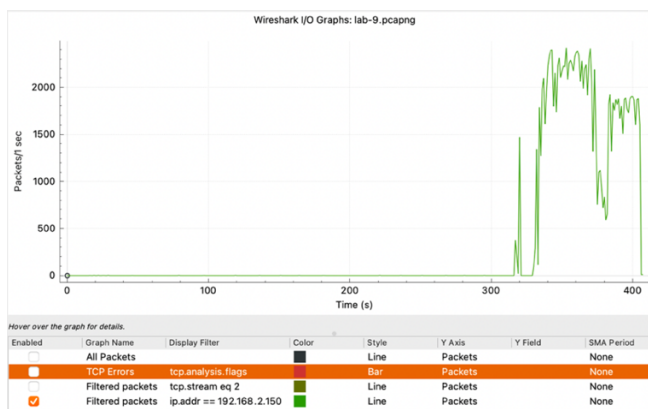
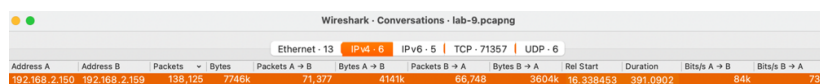


Figura 6.27 Escaneo de puertos de red a los sensores Arduino. Bytes/segundo.



El ataque de DoS se realiza desde una IP pública asignada por Kali Linux hacia los sensores Arduino por el puerto 8443 (ver Figura 6.28). Durante la simulación de ataques DoS se aumenta la transmisión de paquetes, en 80 segundos, se detectan picos de 5000 paquetes/segundo (ver Figura 6.29). Se observa la transmisión de 15 Mbs en 77 segundos (ver Figura 6.30). Los paquetes que son enviados masivamente tienen el estado SYN (ver Figura 6.31).

Figura 6.28 Ataque DoS a los sensores Arduino. Paquetes/segundo.

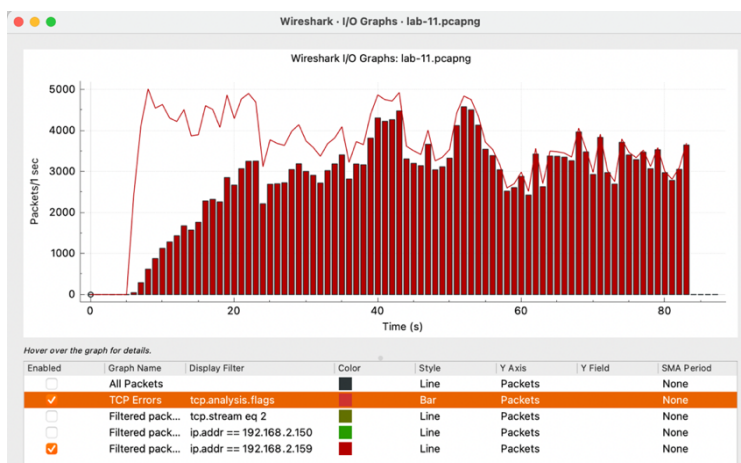
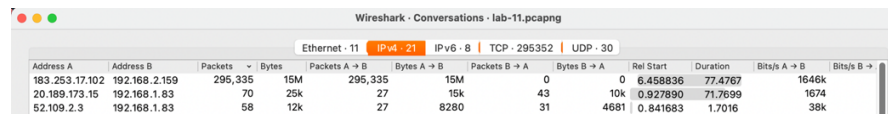
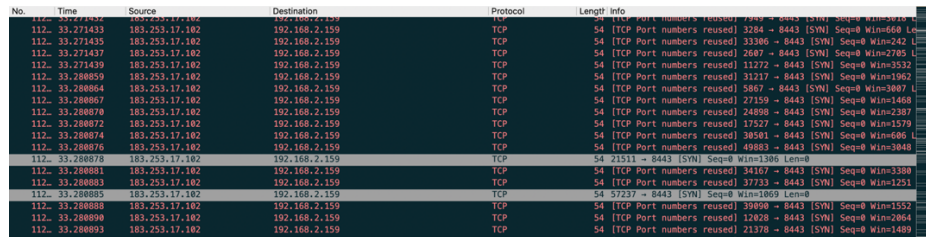


Figura 6.29 Ataque DoS a los sensores Arduino. Bytes/segundos

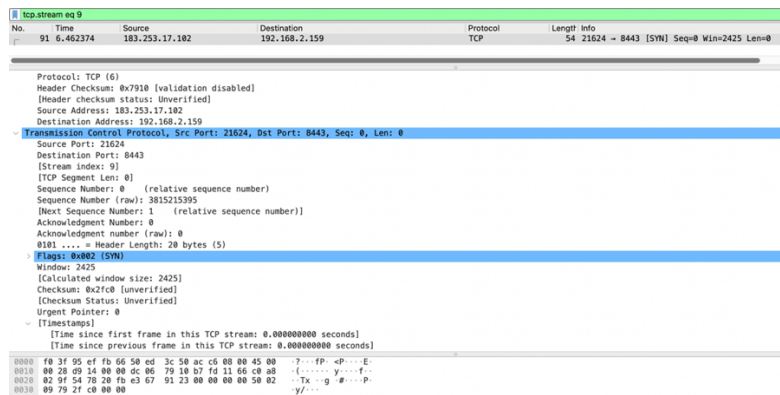


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
183.253.17.102	192.168.2.159	295,335	15M	295,335	15M	0	0	6.458836	77.4767	1646k	
20.189.173.15	192.168.1.83	70	25k	27	15k	43	10k	0.927890	71.7699	1674	
52.109.2.3	192.168.1.83	58	12k	27	8280	31	4681	0.841683	1.7016	38k	

Figura 6.30 Ataque DoS a los sensores Arduino. Detalle paquete.



No.	Time	Source	Destination	Protocol	Length	Info
112.	33.271433	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 3284 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.271435	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 33306 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.271437	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 2687 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.271439	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 11272 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280850	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 31217 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280864	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 5867 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280867	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 27159 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280870	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 24898 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280872	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 17527 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280874	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 36521 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280876	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 49883 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280878	183.253.17.102	192.168.2.159	TCP	54	21511 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280881	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 34167 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280883	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 37223 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280885	183.253.17.102	192.168.2.159	TCP	54	57237 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280888	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 39090 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280890	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 12828 → 8443 [SYN] Seq=0 Win=65535 Len=0
112.	33.280893	183.253.17.102	192.168.2.159	TCP	54	[TCP Port numbers reused] 21378 → 8443 [SYN] Seq=0 Win=65535 Len=0



No.	Time	Source	Destination	Protocol	Length	Info
91	6.462374	183.253.17.102	192.168.2.159	TCP	54	21624 → 8443 [SYN] Seq=0 Win=65535 Len=0

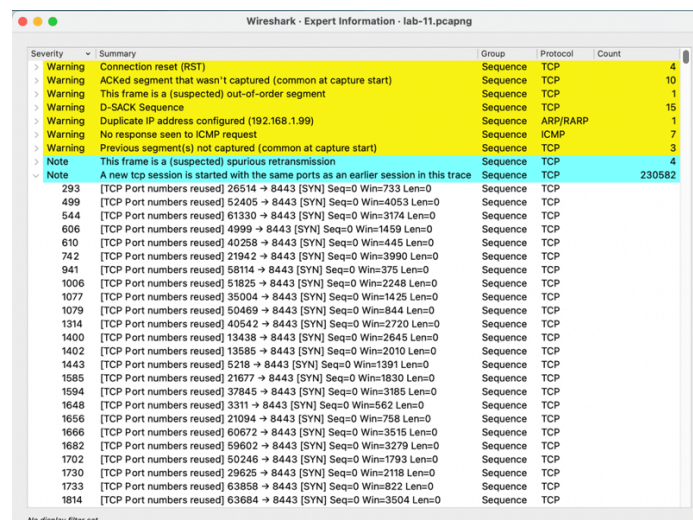
Protocol: TCP (6)
Header Checksum: 0x7910 [validation disabled]
[Header checksum status: Unverified]
Source Address: 183.253.17.102
Destination Address: 192.168.2.159

Transmission Control Protocol, Src Port: 21624, Dst Port: 8443, Seq: 0, Len: 0

Source Port: 21624
Destination Port: 8443
Stream Index: 0
TCP Segment Len: 0
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 381521395
(Next Sequence Number: 1 (relative sequence number))
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0181 = Header Length: 20 bytes (5)
Flags: 0x002 [SYN]
Window: 2425
[Calculated window size: 2425]
Checksum: 0x2f08 [unverified]
[Checksum status: Unverified]
Urgent Pointer: 0
Timestamps
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

0000 f0 3f 95 of fb 66 50 ed 3c 50 ac c5 00 00 45 00 ...?P...P...E
0010 00 20 d9 14 00 00 dc 06 79 10 07 fd 11 66 c0 a8 ...-...y...f...
0020 82 9f 54 70 20 fb e3 67 91 23 00 00 00 50 02 ...Tx...g...P...
0030 00 70 2f c0 00 00 ...y/...

Figura 6.31 Ataque DoS a los sensores Arduino. Paquetes masivos enviados en estado SYN.



Severity	Summary	Group	Protocol	Count
Warning	Connection reset (RST)	Sequence	TCP	4
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	10
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	1
Warning	D-SACK Sequence	Sequence	TCP	15
Warning	Duplicate IP address configured (192.168.1.99)	Sequence	ARP/RARP	1
Warning	No response seen to ICMP request	Sequence	ICMP	7
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	3
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	4
Note	A new tcp session is started with the same ports as an earlier session in this trace	Sequence	TCP	230582
	293 [TCP Port numbers reused] 26514 → 8443 [SYN] Seq=0 Win=733 Len=0	Sequence	TCP	
	499 [TCP Port numbers reused] 52405 → 8443 [SYN] Seq=0 Win=4053 Len=0	Sequence	TCP	
	544 [TCP Port numbers reused] 61530 → 8443 [SYN] Seq=0 Win=3174 Len=0	Sequence	TCP	
	606 [TCP Port numbers reused] 4999 → 8443 [SYN] Seq=0 Win=1459 Len=0	Sequence	TCP	
	610 [TCP Port numbers reused] 40258 → 8443 [SYN] Seq=0 Win=445 Len=0	Sequence	TCP	
	742 [TCP Port numbers reused] 21942 → 8443 [SYN] Seq=0 Win=3990 Len=0	Sequence	TCP	
	941 [TCP Port numbers reused] 58114 → 8443 [SYN] Seq=0 Win=375 Len=0	Sequence	TCP	
	1006 [TCP Port numbers reused] 51825 → 8443 [SYN] Seq=0 Win=2248 Len=0	Sequence	TCP	
	1077 [TCP Port numbers reused] 35004 → 8443 [SYN] Seq=0 Win=1425 Len=0	Sequence	TCP	
	1079 [TCP Port numbers reused] 50469 → 8443 [SYN] Seq=0 Win=844 Len=0	Sequence	TCP	
	1314 [TCP Port numbers reused] 40542 → 8443 [SYN] Seq=0 Win=2720 Len=0	Sequence	TCP	
	1400 [TCP Port numbers reused] 13438 → 8443 [SYN] Seq=0 Win=2645 Len=0	Sequence	TCP	
	1402 [TCP Port numbers reused] 13585 → 8443 [SYN] Seq=0 Win=2010 Len=0	Sequence	TCP	
	1443 [TCP Port numbers reused] 5218 → 8443 [SYN] Seq=0 Win=1391 Len=0	Sequence	TCP	
	1585 [TCP Port numbers reused] 21677 → 8443 [SYN] Seq=0 Win=1830 Len=0	Sequence	TCP	
	1594 [TCP Port numbers reused] 37845 → 8443 [SYN] Seq=0 Win=3165 Len=0	Sequence	TCP	
	1648 [TCP Port numbers reused] 3311 → 8443 [SYN] Seq=0 Win=562 Len=0	Sequence	TCP	
	1656 [TCP Port numbers reused] 21094 → 8443 [SYN] Seq=0 Win=758 Len=0	Sequence	TCP	
	1666 [TCP Port numbers reused] 60672 → 8443 [SYN] Seq=0 Win=3515 Len=0	Sequence	TCP	
	1682 [TCP Port numbers reused] 59602 → 8443 [SYN] Seq=0 Win=3279 Len=0	Sequence	TCP	
	1702 [TCP Port numbers reused] 50246 → 8443 [SYN] Seq=0 Win=1793 Len=0	Sequence	TCP	
	1730 [TCP Port numbers reused] 29625 → 8443 [SYN] Seq=0 Win=2118 Len=0	Sequence	TCP	
	1733 [TCP Port numbers reused] 63858 → 8443 [SYN] Seq=0 Win=822 Len=0	Sequence	TCP	
	1814 [TCP Port numbers reused] 63684 → 8443 [SYN] Seq=0 Win=3504 Len=0	Sequence	TCP	

No display filter set.

6.7.4 Análisis del tráfico a través de IDS Suricata

Se realiza la revisión del tráfico de red a través del IDS Suricata 6.0.5. Se observa que las reglas predeterminadas no tienen reglas configuradas para detectar ataques DoS. Para lo que se procede a la configuración de las reglas para alertar sobre tráfico DoS (*Suricata Detect Dos Attack*, 2022). Posteriormente, se analiza el tráfico de la red simulada en el momento que de los ataques DoS hacia los sensores Arduino IoT. A lo que se reciben por parte de Suricata las alertas de que los paquetes representan un potencial ataque DoS (ver Figura 6.32).

Figura 6.32 Alerta de posible ataque DoS en IDS Suricata

```
root@adminiot:/var/lib/suricata/rules# tail -f /var/log/suricata/fast.log
04/15/2022-05:36:37.711973 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:41652 -> 192.168.2.159:8443
04/15/2022-05:36:42.214189 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:11815 -> 192.168.2.159:8443
04/15/2022-05:36:47.353080 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:26249 -> 192.168.2.159:8443
04/15/2022-05:36:52.504347 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:35631 -> 192.168.2.159:8443
04/15/2022-05:36:57.012484 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:7812 -> 192.168.2.159:8443
04/15/2022-05:37:02.241667 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:34598 -> 192.168.2.159:8443
04/15/2022-05:37:06.878757 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:17990 -> 192.168.2.159:8443
04/15/2022-05:37:11.290088 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:3770 -> 192.168.2.159:8443
04/15/2022-05:37:16.616689 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:28041 -> 192.168.2.159:8443
04/15/2022-05:37:21.465903 [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:21750 -> 192.168.2.159:8443
```

6.7.5 Revisión de vulnerabilidades de CVE

Dado que en la captura de tráfico normal se detecta el uso del protocolo MQTT se procede a revisar las vulnerabilidades de este protocolo en la base de datos publicada por CVE® al 6 de mayo de 2022 (ver Tabla C1) (*CVE - Search Results*, 2022) . En total se listan 76 vulnerabilidades de CVE® relacionadas a MQTT, están relacionadas con herramientas de IoT, donde las más enunciadas son Cesanta Mongoose, Totolink, Eclipse Mosquitto, Sealevel Systems, Zephyr MQTT, Contiki, AWS, RIOT, Qualcomm Technologies, BigIP, Apache ActiveMQ, IBM MessageSlight, AWS FreeRTOS, ZTE routers, entre otros, (ver Tabla 6.5).

Tabla 6.5 Cantidad de vulnerabilidades CVE® MQTT en herramientas IoT

Herramienta IoT	# Vulnerabilidades CVE ® de MQTT
Cesanta Mongoose	9
Totolink	8
Eclipse Mosquitto	8
Sealevel Systems	6
MQTT	5
Zephyr MQTT	3
Contiki	2
AWS	2
RIOT	2
Qualcomm Technologies	2
BigIP	2

Se hace una revisión de las vulnerabilidades tomando en cuenta los principios de la tríada de seguridad: integridad, confiabilidad y disponibilidad. A lo que se detecta que 25 amenazas impactan a la integridad de datos ya sea con ejecución remota no autorizada de código, envío de datos y requerimientos no autorizados, con impersonalización de servidores MQTT o con sobre escritura de archivos (ver Tabla 6.6).

Tabla 6.6 Vulnerabilidades de CVE relacionadas a MQTT (CVE - Search Results, 2022)

Hallazgo de seguridad	Cantidad de vulnerabilidades relacionadas
Ejecución remota no autorizada de código	20
Envío de datos y requerimientos no autorizado	1
Impersonalizar a un servidor MQTT	3
Sobre escritura arbitraria de archivos	1

Se detectan 16 vulnerabilidades asociadas a la afectación de la confidencialidad de datos a través de divulgación no autorizada de información, a que no hay referencia de punteros iniciales y a que existen accesos no autorizados (ver Tabla 6.7).

Tabla 6.7 Cantidad de vulnerabilidades CVE® MQTT que afecta la confidencialidad de datos en IoT

Hallazgo de seguridad	Cantidad de vulnerabilidades relacionadas
Divulgación no autorizada de información	6
No hay referencia del puntero inicial	1
Acceso no autorizado	9

Se observan 40 vulnerabilidades que impactan la disponibilidad de datos a través de ataques de denegación de servicio (DDoS), escritura fuera de límites, fallas de sistema MQTT, fallas de memoria, desbordamiento de búfer y bloqueo no autorizado de tráfico (ver Tabla 6.8).

Tabla 6.8 Cantidad de vulnerabilidades CVE® MQTT que afecta la disponibilidad de datos en IoT

Hallazgo de seguridad	Cantidad de vulnerabilidades relacionadas
DDoS	15
Escritura fuera de límites	2
Falla de sistema MQTT	9
Fallo de memoria	7
Desbordamiento de búfer	5
Bloqueo no autorizado de tráfico	2

6.7.6 Revisión de vulnerabilidades matriz MITRE ATT&CK ICS

Para la revisión de vulnerabilidades también se utiliza el marco de referencia de Tácticas, Técnicas y Conocimiento Común de adversarios, MITRE ATT&CK. Este apoya a direccionar el porqué, como y quien de los ataques cibernéticos en una infraestructura digital (Georgiadou et al., 2021). La matriz ATT&CK ICS para el Sistema de Control Industrial (en inglés Industrial Control

System:ICS) describe el comportamiento de adversarios en una red Industrial, consiste en 11 tácticas, 81 técnicas y 50 mitigaciones (Georgiadou et al., 2021). Las vulnerabilidades del protocolo MQTT que se detectaron en CVE ® son identificadas en la matriz MITRE ATT&CK ICS (*Matrix* | MITRE ATT&CK®, 2022) (ver Tabla 6.9). A continuación, se indican seleccionadas en gris las técnicas relacionadas a las vulnerabilidades de MQTT documentadas en CVE ®.

Tabla 6.9 *Matriz MITRE ATT&CK ICS (Matrix | MITRE ATT&CK®, 2022)*

MITRE ATT&CK® Matrix for ICS											
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shut-down		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information

7 Resultados

El resultado es un marco de referencia, que considera los fundamentos de seguridad en las capas de la arquitectura de IoT. Este podrá ser implementado en cualquier empresa de IoT para reforzar sus servicios de seguridad de la infraestructura. El aporte científico es llenar los vacíos de los marcos de referencia propuestos por Ficco (2013), Alam et al (2011), Ekelhart et al (2009), este marco de referencia de seguridad de IoT, MaRCIoT es validado por la encuesta de especialistas de IT y por el resultado de pruebas en un ambiente controlado de IoT. De manera que el marco de referencia logra establecer el alcance relacionado con la estrategia de la organización, administrar los activos de información, definir las políticas y procedimientos, proteger la operación, identificar las amenazas, mitigar las amenazas y tener cumplimiento en las categorías.

7.1 Validación del marco de seguridad de infraestructura de IoT

Para validar el marco de referencia de seguridad en la infraestructura de IoT se utiliza un cuestionario autoadministrado y anónimo a través de un formulario de página web, con tasa de respuesta alta, el presupuesto de su construcción y aplicación fue bajo y la rapidez con la que se administro fue media, la profundidad de los datos obtenidos es alta. Fue fácil de responder, de analizar y comparar.

El cuestionario fue administrado a 15 especialistas con experiencia de 1 a más de 16 años de experiencia en TI y seguridad de TI, que laboran en una empresa PyME de soluciones de redes y TI establecida hace más de 10 años y en una empresa de TI internacional constituida hace más de 25 años; ambas ubicadas en la ciudad de Puebla, por confidencialidad solicitada no se mencionan los nombres. El formulario fue autoadministrado con 4 preguntas generales y 17 preguntas relacionadas al marco de seguridad en la infraestructura de IoT utilizando la escala Likert. En la

escala de Likert se definen cinco puntos para medir la actitud acerca del marco de referencia de seguridad de IoT utilizando la tecnología IDS. Los puntos de valor utilizados son: Nada importante (1), Poco importante (2), Medianamente importante (3), Sumamente importante (4) e Indispensable (5), mostrado en la Tabla 7.1 y Tabla 7.2.

Tabla 7.1 *Cuestionario de validez de Marco de Referencia de Seguridad de Infraestructura de IoT usando la tecnología IDS. Preguntas generales.*

Marco de referencia de ciberseguridad para la infraestructura de IoT utilizando la tecnología IDS
Por favor hay que indicar que tan importante es cada característica en un marco de referencia de ciberseguridad. Gracias.
Indicar su puesto actual de trabajo
Especialista de Tecnologías de Información
Arquitecto/Consultor en Tecnologías de Información
Especialista de seguridad en Tecnologías de Información
Arquitecto/Consultor de seguridad en Tecnologías de Información
Especialista de tecnología de IoT
Arquitecto/Consultor de tecnología de IoT
¿Cuántos años de experiencia laboral tiene?
1-3 años
4-6 años
7-9 años
10-12 años
13-15 años
> 16 años
¿Qué marcos de referencia de seguridad de información conoce?
NIST
ISO 27001:2013
COBIT
ISA/IEC 62443
Otro
Para usted, ¿Cuál es el principal problema de un marco de referencia en infraestructura de IoT?
La complejidad de implementación
El entendimiento de los entregables

Poca utilidad en protección de amenazas de seguridad

Limitantes de recursos operativos y humanos

Tabla 7.2 *Cuestionario de validez de Marco de Referencia de Seguridad de Infraestructura de IoT usando la tecnología IDS. Preguntas acerca del marco de referencia de seguridad.*

¿Para un marco de referencia de seguridad de IoT tan importante es ... Nada importante (1), Poco importante (2), Medianamente importante (3), Sumamente importante (4) e Indispensable (5)	(1)	(2)	(3)	(4)	(5)
una autoridad responsable del mismo?					
que este apegada a la estrategia del negocio?					
gestión de activos de la información?					
contar con un glosario de términos y definiciones de seguridad de información?					
establecer y formalizar políticas y procedimientos de seguridad de datos?					
comunicar las políticas de seguridad de información?					
una guía oral, aparte de la política principal?					
tener establecido un procedimiento en casos emergentes?					
la implementación de controles de seguridad en la operación, como la autenticación, el control de acceso, encriptación de datos, entre otros?					
capacitar continuamente a los administradores de infraestructura de IoT?					
identificar amenazas a través de un cuestionario de los especialistas?					
identificar amenazas a través de colaboración abierta con los usuarios finales?					
identificar los riesgos de seguridad de información?					
mitigar o aceptar los riesgos de información detectados?					
implementar un sistema de detección de intrusos en la infraestructura de IoT?					
contar con gestión de incidencias de seguridad de información?					
formalizar y comunicar un plan de comunicación en una incidencia de seguridad?					

7.2 Análisis de datos

7.2.1 Confiabilidad del instrumento de medición

Se utiliza la medida de coherencia para medir la confiabilidad del instrumento de medición, recordando que el coeficiente alfa de Cronbach debe tener valor mínimo aceptable de 0.70. Se calcula el coeficiente de Cronbach utilizando Minitab, siendo 0.9283, mostrando fiabilidad. Los valores de la matriz de correlación se mantienen positivos, mostrados en Tabla 7.3 y Tabla 7.4.

Tabla 7.3 Matriz de correlación del coeficiente alfa de Cronbach

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0.2															
2	0.472	0.354														
3	0.148	0.123	0.261													
4	0.491	0.408	0.577	0.302												
5	0.481	0.491	0.463	0.161	0.757											
6	0.491	0.408	0.289	0.553	0.444	0.312										
7	0.339	0.468	0.378	0.592	0.6	0.394	0.873									
8	0.764	0.068	0.577	0.553	0.444	0.312	0.722	0.6								
9	0.105	0.196	0.139	0.688	0.08	0.096	0.48	0.288	0.48							
10	0.058	0.647	0.305	0.677	0.484	0.318	0.484	0.591	0.264	0.55						
11	0.546	0.325	0.525	0.411	0.606	0.274	0.606	0.571	0.606	0.428	0.461					
12	0.464	0.535	0.756	0.395	0.764	0.7	0.491	0.607	0.491	0.105	0.49	0.546				
13	0.218	0.408	0.577	0.302	0.722	0.535	0.167	0.327	0.167	0.08	0.484	0.417	0.764			
14	0.413	0.421	0.596	0.484	0.841	0.552	0.459	0.526	0.459	0.22	0.576	0.496	0.788	0.841		
15	0.464	0.2	0.472	0.395	0.764	0.481	0.491	0.607	0.491	0.105	0.49	0.546	0.464	0.491	0.601	
16	0.342	0.452	0.213	0.334	0.492	0.345	0.185	0.262	0.185	0.163	0.699	0.322	0.342	0.492	0.508	0.645

Tabla 7.4 Estadística de las categorías del marco de referencia de ciberseguridad

Variable	Total Cuenta	Míni mo	Máxi mo	Medi a	Desviación Estándar
E-autoridad	15	1	5	4.467	0.516
E-negocio	15	1	5	4.200	0.414
E-activos-información	15	1	5	4.333	0.488
E-glosario	15	1	5	4.200	0.561
E-políticas	15	1	5	4.600	0.507
E-comunicar-políticas	15	1	5	4.400	0.632
E-guía-oral	15	1	5	3.600	0.507
E-procedimiento-emergente	15	1	5	4.533	0.516
E-control-seguridad	15	1	5	4.600	0.507
E-identificar-escritorio	15	1	5	4.067	0.704
E-identificar-cuestionario	15	1	5	3.533	0.640
E-identificar-usuarios	15	1	5	3.867	0.743
E-identificar-riesgos	15	1	5	4.467	0.516

E-mitigar-riesgos	15	1	5	4.600	0.507
E-IDS	15	1	5	4.400	0.737
E-gestión-incidencias	15	1	5	4.467	0.516
E-comunicar-incidencias	15	1	5	4.267	0.458
Total	15	1	5	72.60	6.555
				0	

Dentro de las respuestas de los 15 especialistas se encuentran 4 (26.7%) especialistas de TI y 4 (26.7%) especialistas de seguridad de TI. Existen 10 especialistas (66.7%) con más de 7 años de experiencia en TI y en seguridad de TI. El marco de referencia de seguridad más conocidos es el ISO 27001:2013 por 13 (86.7%) especialistas, seguido por COBIT conocido por 8 especialistas (53.3%) y en tercer lugar está el NIST por 7 (46.7%) especialistas. Se detecta que los principales problemas de un marco de referencia en infraestructura de IoT es el entendimiento de los entregables, opinando por 10 especialistas (66.7%), seguido por la complejidad de la implementación por 7 especialistas (46.7%). Los procedimientos son considerados como el principal elemento del marco de referencia de seguridad de IoT por 9 (69.1%) especialistas, seguido de la estructura por 7 especialistas (53.8%).

Se mide la actitud de los especialistas de IT y de seguridad de IT que tienen hacia los elementos del marco de seguridad de infraestructura de IoT, donde se detectó que 8 (53.3%) consideran “sumamente importante” tener una autoridad responsable, 12 (80.0%) seleccionan como “sumamente importante” que este apegado a la estrategia del negocio. Se indica que la gestión de activos de información es “sumamente importante” por 10 (66.7%) especialistas. El glosario de términos y definiciones es “sumamente importante” para 10 (66.7%) especialistas y 9 (60.0%) especialistas señalan como “indispensable” establecer y formalizar políticas y procedimientos. Es “indispensable” comunicar las políticas de seguridad acorde a 7 (46.7%) especialistas.

Una guía oral aparte de la política principal se toma en cuenta como “sumamente importante” por 9 especialistas (60.0%). También se menciona que es “indispensable” tener un procedimiento en casos de emergencia por parte de 8 (53.3%) especialistas. Otro elemento “indispensable” para 9 (60.0%) especialistas es la implementación de controles de seguridad en la operación, como son autenticación, control de accesos, encriptación de datos, entre otros. Se muestra como “sumamente importante” por 8 (53.3%) especialistas identificar las amenazas a través de investigación de escritorio. El identificar amenazas a través de un cuestionario de los especialistas es considerado “medianamente importante” por 7 (50%) especialistas. Otra manera de identificar amenazas es a través de colaboración abierta con los usuarios finales, que se considera “sumamente importante” por 10 (66.7%) especialistas.

El identificar los riesgos de seguridad de información es “sumamente importante” acorde a 8 especialistas (53.3%). Es “indispensable” mitigar o aceptar los riesgos de información basados en 9 (60.0%) especialistas. También es “sumamente importante” para 9 (64.3%) especialistas seleccionar un método de mitigación de riesgos de información señalado. Es “indispensable” implementar un sistema de detección de intrusos, señalado por 8 (53.4%) especialistas. La gestión de incidencias de seguridad de información es “sumamente importante” acorde a 8 (53.3%) especialistas y 11 (73.3%) de los especialistas muestran como “sumamente importante” formalizar y comunicar un plan de comunicación en las incidencias de seguridad (ver Figuras B.1 – B.17).

8 Conclusiones / Trabajos Futuros

El IoT es una tecnología emergente que aún tiene puntos de mejoras en ciertos aspectos, como es en la protección a la información. Hay investigaciones para mejorar la seguridad en IoT, pero aún se tienen deficiencias en la autenticación, autorización, encriptación, manejo de incidentes, reconocimiento de amenazas y vulnerabilidades, entre otros. De igual manera, aunque existen estándares de seguridad que pueden llegar a ser complejos.

Para lo que se propone un marco de referencia validado para ciberseguridad de IoT usando la tecnología de IDS. La metodología consiste en revisar literatura de los marcos de referencia de ciberseguridad ya existentes para infraestructura de IoT. Después se describe y analiza comparativamente los marcos de referencia de seguridad NIST CSF, ISO 27001:2013, OCTAVE Allegro, ISA/IEC 6443 y marco Lubua. Este análisis consiste en detectar las funciones y entregables similares para generar nuevas categorías. Se valida el marco de referencia de seguridad en la infraestructura de IoT, MaRCIoT, a través de la administración de cuestionarios a especialistas de IT y de seguridad de IT.

Dentro de los 15 especialistas se encuentran personal de TI y de seguridad de TI con más de 7 años de experiencia y que conocen más los marcos de referencia de seguridad de ISO 27001:2013, COBIT y NIST. Detectan que los principales problemas de un marco de referencia de seguridad es el entendimiento de los entregables y la complejidad de la implementación. Acorde a los resultados, dentro de los elementos de un marco de seguridad se consideran “medianamente importante” identificar amenazas a través de un cuestionario de los especialistas. Los siguientes elementos se estiman como “sumamente importante”, una autoridad responsable, una estrategia apegada al negocio, una gestión de activos, un glosario de términos y definiciones, una guía oral

adicional a la política principal, identificación de las amenazas a través de investigación de escritorio y por colaboración abierta con usuarios finales, gestión de riesgos, formalización y comunicación de un plan de comunicación de las incidencias de seguridad y gestión de incidencias de seguridad de información

Clasifican como “indispensables” establecer y formalizar políticas y procedimientos, comunicar las políticas de seguridad, tener un procedimiento en casos de emergencia, implementar controles de seguridad en la operación, mitigar o aceptar los riesgos de información detectados e implementar un sistema de detección de intrusos.

Estos componentes están incluidos en el Marco de Referencia de Ciberseguridad IoT, MaRCIoT. El cual está formado por las categorías Establecer el alcance, Administración de activos de información, Políticas y procedimientos, Proteger operación, Identificar amenazas, Mitigar amenazas y Cumplimiento.

La contribución de esta investigación es el tener un estándar que integre una guía para implementar las políticas de seguridad y al mismo tiempo el análisis de riesgos dentro de la infraestructura de IoT. Que considera la estrategia del negocio, recursos humanos, proceso de incidencia, mejora continua, entre otros. También pretende simplificar la implementación por no necesitar un alto grado de pericia de los especialistas. Este marco de referencia usa la tecnología de IDS porque permite hacer el monitoreo e inspección de tráfico de red sin consumir recursos de los nodos de IoT. Sin embargo, se debe de tener en cuenta que esta tecnología también presenta vulnerabilidades de seguridad como son los ataques adversos y el riesgo podría decrementarse con medidas de prevención, con ciertas técnicas de detección de intrusos, con la implementación de sistemas complementarios de seguridad y con el seguimiento de políticas de seguridad. Es

importante mencionar que las tecnologías de seguridad de datos deben de ser evaluadas constantemente por la rapidez con la que se generan nuevos tipos de ciberataques.

Como trabajo futuro se contempla la implementación de MaRCIoT a través de un caso de uso en una empresa que proporcione servicios de IoT en el sector privado.

Referencias

- Akhtar, M. S., & Feng, T. (2021). Deep Learning-Based Framework for the Detection of Cyberattack Using Feature Engineering. *Security and Communication Networks*, 2021. <https://doi.org/10.1155/2021/6129210>
- Alaiz-Moreton, H., Aveleira-Mata, J., Ondicol-Garcia, J., Muñoz-Castañeda, A. L., & Benavides, C. (2019). Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol. *Complexity*, 2019, 1–11.
- Alashwali, E. S., & Rasmussen, K. (2018). What's in a downgrade? A taxonomy of downgrade attacks in the TLS protocol and application protocols using TLS. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 255, 468–487. https://doi.org/10.1007/978-3-030-01704-0_27
- Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors (Switzerland)*, 18(3), 1–17. <https://doi.org/10.3390/s18030817>
- Alqassem, I., & Svetinovic, D. (2014). A taxonomy of security and privacy requirements for the Internet of Things (IoT). *IEEE International Conference on Industrial Engineering and Engineering Management, 2015-Janua*, 1244–1248. <https://doi.org/10.1109/IEEM.2014.7058837>
- Alshehri, M. D., & Hussain, F. K. (2018). A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). *Computing*. <https://doi.org/10.1007/s00607-018-0685-7>
- Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8–27. <https://doi.org/10.1016/j.jisa.2017.11.002>
- Aveleira-Mata, J., Muñoz-Castañeda, Á. L., García-Ordás, M. T., Benavides-Cuellar, C., Benítez-Andrades, J. A., & Alaiz-Moreton, H. (2021). IDS prototype for intrusion detection with machine learning models in IoT systems of the Industry 4.0. *Dyna (Spain)*, 93(3), 270–275. <https://doi.org/10.6036/10011>
- Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). *Communications in Computer and Information Science*, 89 CCIS, 420–429. https://doi.org/10.1007/978-3-642-14478-3_42
- Bauer, H., Burkacky, O., & Knochenhauer, C. (2017). Security in the internet of things. *Mckinsey&Company*, 1–9. <https://doi.org/10.4018/978-1-5225-5736-4.ch006>
- Bonebrake, C. (2022). *Facility Cybersecurity Framework Core Assessment*. FCF Faculty Cybersecurity. <https://facilitycyber.labworks.org/assessments/coreAssessment>
- Brass, I., Tanczer, L., Carr, M., Elsdén, M., & Blackstock, J. (2018). Standardising a moving target: The development and evolution of IoT security standards. *IET Conference Publications*, 2018(CP740), 1–9. <https://doi.org/10.1049/cp.2018.0024>
- Calabretta, M., Pecori, R., Vecchio, M., & Veltri, L. (2018). MQTT-Auth : a Token-based Solution to Endow MQTT with Authentication and Authorization Capabilities. *Journal of Communications Software and Systems*, 14(4), 320–332.
- Calder, A. (2008). *ISO27001/ISO27002 : A Pocket Guide*. IT Governance Publishing .
- Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. <http://www.sei.cmu.edu/publications/pubweb.html>

- Castillo, A., & Thierer, A. D. (2015). Projecting the Growth and Economic Impact of the Internet of Things. *SSRN Electronic Journal*, 1–10. <https://doi.org/10.2139/ssrn.2618794>
- Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, 36(2), 346–357. <https://doi.org/10.1016/j.giq.2018.09.007>
- Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks*, 144, 17–39. <https://doi.org/10.1016/j.comnet.2018.07.017>
- CVE - Search Results. (2022, May 6). The MITRE Corporation. <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mqtt>
- de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1–7. <https://doi.org/10.1016/j.giq.2017.02.007>
- Dinculeană, D., & Cheng, X. (2019). Vulnerabilities and limitations of MQTT protocol used between IoT devices. *Applied Sciences (Switzerland)*, 9(5). <https://doi.org/10.3390/app9050848>
- El-hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni 3, A. (2019). A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors*, 19(1141), 1–44. <https://doi.org/10.3390/s19051141>
- Framework for Improving Critical Infrastructure Cybersecurity*. (2018). <https://doi.org/10.6028/NIST.CSWP.04162018>
- Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC*, 10(2), 123–141. <https://doi.org/10.17993/3ctic.2021.102.123-141>
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, 21(3267), 1–14.
- Hayajneh, A. A., Bhuiyan, M. Z. A., & McAndrew, I. (2020). Improving internet of things (IoT) security with software-defined networking (SDN). *Computers*, 9(1). <https://doi.org/10.3390/computers9010008>
- Hernández Ramos, S., Villalba, M. T., & Lacuesta, R. (2018). MQTT Security: A Novel Fuzzing Approach. *Wireless Communications and Mobile Computing*, 2018. <https://doi.org/10.1155/2018/8261746>
- Huang, J. de, & Hsieh, H. C. (2013). Design of gateway for monitoring system in IoT networks. *Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-IThings-CPSCOM 2013*, 1876–1880. <https://doi.org/10.1109/GreenCom-iThings-CPSCOM.2013.348>
- Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk : a holistic analysis of cyber risk assessment frameworks , risk vectors , and risk ranking process. *EURASIP Journal on Information Security*, 8, 2–18.
- Kanuch, P., & Macko, D. (2019). E-HIP: An Energy-Efficient OpenHIP-Based Security in Internet of Things Networks. *Sensors*, 19(4921), 2–17. <https://doi.org/10.3390/s19224921>

- Kelli, V., Argyriou, V., Lagkas, T., Fragulis, G., Grigoriou, E., & Sarigiannidis, P. (2021). Ids for industrial applications: A federated learning approach with active personalization. *Sensors*, 21(20). <https://doi.org/10.3390/s21206743>
- Khan, A., Siddiqui, S., Irshad, M., Ali, S., Saleem, M., & Iqbal, S. (2019). Analytical Method to Improve the Security of Internet of Things with Limited Resources. *EAI Endorsed Transactions on Internet of Things*, 5(18), 163502. <https://doi.org/10.4108/eai.13-7-2018.163502>
- Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access*, 8, 70245–70261. <https://doi.org/10.1109/ACCESS.2020.2986882>
- Kim, N. Y., Rathore, S., Ryu, J. H., Park, J. H., & Park, J. H. (2018). A Survey on Cyber Physical System Security for IoT : Issues , Challenges , Threats , Solutions. *Journal of Information Processing Systems*, 14(6), 1361–1385.
- Kwon, R., Ashley, T., Castleberry, J., McKenzie, P., & Gupta Gourisetti, S. N. (2020). Cyber threat dictionary using MITRE ATTCK matrix and NIST cybersecurity framework mapping. *2020 Resilience Week, RWS 2020*, 106–112. <https://doi.org/10.1109/RWS50334.2020.9241271>
- Larriva-Novo, X., Villagrà, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. *Sensors (Switzerland)*, 21(2), 1–15. <https://doi.org/10.3390/s21020656>
- Lu, Y., & Xu, L. da. (2019). Internet of things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 2103–2115. <https://doi.org/10.1109/JIOT.2018.2869847>
- Mabodi, K., Yusefi, M., Zandiyani, S., Irankhah, L., & Fotuhi, R. (2020). Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. *Journal of Supercomputing*. <https://doi.org/10.1007/s11227-019-03137-5>
- Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) Security : Current Status , Challenges and Prospective Measures. *The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015) Internet*, 336–341.
- Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards and Interfaces*, 62, 64–83. <https://doi.org/10.1016/j.csi.2018.08.003>
- Matrix | MITRE ATT&CK®. (2022, April 21). MITRE ATT&CK. <https://attack.mitre.org/matrices/ics/>
- Mohsin, M., Anwar, Z., Husari, G., Al-shaer, E., & Rahman, M. A. (2016). IoTSAT : A Formal Framework for Security Analysis of the Internet of Things (IoT). *2016 IEEE Conference on Communications and Network Security (CNS) IoTSAT*:
- Morais, C. M. de, Sadok, D., & Kelner, J. (2019). An IoT sensor and scenario survey for data researchers. *Journal of the Brazilian Computer Society*, 25(1). <https://doi.org/10.1186/s13173-019-0085-7>

- Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., & Jardim-goncalves, R. (2018). An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors*, 18(3053), 1–21. <https://doi.org/10.3390/s18093053>
- Muthamil Sudar, K., & Deepalakshmi, P. (2021). An intelligent flow-based and signature-based IDS for SDNs using ensemble feature selection and a multi-layer machine learning-based classifier. *Journal of Intelligent and Fuzzy Systems*, 40(3), 4237–4256. <https://doi.org/10.3233/JIFS-200850>
- Nastase, P., Nastase, F., & Ionescu, C. (2009). Challenges generated by implementation of the IT standards COBIT 4.1, ITIL V3 and ISO/IEC 27002 in enterprises. *Economic Computation and Economic Cybernetics Studies and Research*. www.itsmfi.org
- Nawir, M., Amir, A., Yaakob, N., Lynn, O. B., & Engineering, C. (2016). Internet of Things (IoT): Taxonomy of Security Attacks. *2016 3rd International Conference on Electronic Design (ICED), August 11-12, 2016, Phuket, Thailand*, 321–326.
- Nieto, A., Acien, A., & Fernandez, G. (2019). Crowdsourcing Analysis in 5G IoT: Cybersecurity Threats and Mitigation. *Mobile Networks and Applications*, 24(3), 881–889. <https://doi.org/10.1007/s11036-018-1146-4>
- Nivaashini M., Thangaraj P., Sountharajan S., Suganya E., & Soundariya R.S. (2021). Effective Feature Selection for Hybrid Wireless IoT Network Intrusion Detection Systems Using Machine Learning Techniques. *Ad Hoc & Sensor Wireless Networks*, 49, 175–206.
- Obaidat, M. A., Obeidat, S., Holst, J., Hayajneh, A. Al, & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, 9(2), 2–43. <https://doi.org/10.3390/computers9020044>
- Ould-Yahia, Y., Banerjee, S., Bouzefrane, S., & Boucheneb, H. (2017). Exploring Formal Strategy Framework for the Security in IoT towards e-Health Context using Computational Intelligence. *Internet of Things and Big Data Technologies for Next Generation Healthcare*, 23(October), 63–90. <https://doi.org/10.1007/978-3-319-49736-5>
- Pan, J., & Yang, Z. (2018). Cybersecurity challenges and opportunities in the new “edge computing + iot” world. *SDN-NFVSec 2018 - Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, Co-Located with CODASPY 2018, 2018-Janua*, 29–32. <https://doi.org/10.1145/3180465.3180470>
- Park, W., & Ahn, S. (2017). Performance Comparison and Detection Analysis in Snort and Suricata Environment. *Wireless Pers Commun*, 94, 241–252. <https://doi.org/10.1007/s11277-016-3209-9>
- Prokofiev, A. O., Smirnova, Y. S., & Silnov, D. S. (2017). The Internet of Things cybersecurity examination. *Proceedings - 2017 Siberian Symposium on Data Science and Engineering, SSDSE 2017*, 44–48. <https://doi.org/10.1109/SSDSE.2017.8071962>
- Pyka, M., & Sobieski, Ś. (2012). Implementation of the OCTAVE methodology in security risk management process for business resources. *Advances in Intelligent and Soft Computing*, 118, 235–252. https://doi.org/10.1007/978-3-642-25355-3_21
- Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems*. (2020). www.awa.csis.org/programs/technology-policy-program/significant-cyber-incidents
- Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R., & Huth, M. (2018). Economic impact of IoT cyber risk - Analysing past and present to predict the future

- developments in IoT risk analysis and IoT cyber insurance. *IET Conference Publications*, 2018(CP740). <https://doi.org/10.1049/cp.2018.0003>
- Safkhani, M., & Shariat, M. (2018). Implementation of secret disclosure attack against two IoT lightweight authentication protocols. *Journal of Supercomputing*, 74(11), 6220–6235. <https://doi.org/10.1007/s11227-018-2538-8>
- Satapathy, A., & Livingston, J. (2016). A Comprehensive Survey on SSL/ TLS and their Vulnerabilities. *International Journal of Computer Applications*, 153(5), 31–38. <https://doi.org/10.5120/ijca2016912063>
- Sengupta, A. (2015). Modeling dependencies of ISO/IEC 27002:2013 security controls. *Communications in Computer and Information Science*, 536, 354–367. https://doi.org/10.1007/978-3-319-22915-7_33
- Shammar, E. A., & Zahary, A. T. (2020). The Internet of Things (IoT): a survey of techniques, operating systems, and trends. In *Library Hi Tech* (Vol. 38, Issue 1, pp. 5–66). Emerald Group Holdings Ltd. <https://doi.org/10.1108/LHT-12-2018-0200>
- Shinde, P. S., & Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*. <https://doi.org/10.1109/STARTUP.2016.7583912>
- Singh, S., & Singh, N. (2016). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, 1577–1581. <https://doi.org/10.1109/ICGCIoT.2015.7380718>
- Sklavos, N., & Zaharakis, I. D. (2016). Cryptography and security in internet of things (IoTs): Models, schemes, and implementations. In V. V Badra M. Pau G. (Ed.), *2016 8th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2016*. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/NTMS.2016.7792443>
- Smith, N. (2014). PROTECTING CONSUMERS IN THE AGE OF. *St. John's Law Review*, 93, 851–882.
- Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178–188. <https://doi.org/10.1016/j.future.2018.09.063>
- Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, 4(4), 225–230.
- Suricata Detect Dos Attack*. (2022, May 6). Open Source Libs. <https://opensorcelibs.com/lib/suricata-detect-dos-attack>
- Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *Journal of Supercomputing*, 73(3), 1085–1102. <https://doi.org/10.1007/s11227-016-1849-x>
- Tewari, A., & Gupta, B. B. (2018). Security , Privacy and Trust of different Layers in Internet-of-things (IoTs) Framework. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2018.04.027>
- Thakkar, A., & Lohiya, R. (2021). A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. *Archives of*

- Computational Methods in Engineering*, 28(4), 3211–3243. <https://doi.org/10.1007/s11831-020-09496-0>
- Vaccari, I., Aiello, M., & Cambiaso, E. (2020). SlowITe, a novel denial of service attack affecting MQTT. *Sensors (Switzerland)*, 20(10). <https://doi.org/10.3390/s20102932>
- Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. (2017). Internet of Things (IoT): A vision, architectural elements, and security issues. *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, 492–496. <https://doi.org/10.1109/I-SMAC.2017.8058399>
- Vijayakumaran, C., Muthusenthil, B., & Manickavasagam, B. (2020). A reliable next generation cyber security architecture for industrial internet of things environment. *International Journal of Electrical and Computer Engineering*, 10(1), 387–395. <https://doi.org/10.11591/ijece.v10i1.pp387-395>
- Wazoel Lubua, E., & Pretorius, P. D. (n.d.). *Cyber-security Policy Framework and Procedural Compliance in Public Organisations*. <https://thelawdictionary.org/policy-framework/>
- Webb, J., & Hume, D. (2018). Campus IoT collaboration and governance using the NIST cybersecurity framework. *IET Conference Publications*, 2018(CP740), 1–7. <https://doi.org/10.1049/cp.2018.0025>
- Xiong, W., Legrand, E., Aberg, O., & Lagerström Robert. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 1–21.
- Yigit Ozkan, B., & Spruit, M. (2019). A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11398 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-12085-6_5
- Cve.mitre.org. 2021. *CVE -Search Results*. [online] Available at: <<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mqtt>> [Accessed 21 July 2021].
- GitHub. 2021. *GitHub - OISF/suricata: Suricata git repository maintained by the OISF*. [online] Available at: <<https://github.com/OISF/suricata>> [Accessed 21 July 2021].
- Suricata.readthedocs.io. 2021. 6. *Suricata Rules — Suricata 6.0.3 documentation*. [online] Available at: <<https://suricata.readthedocs.io/en/suricata-6.0.3/rules/index.html>> [Accessed 21 July 2021].
- Technique Matrix - attackics*. Collaborate.mitre.org. (2021). Retrieved 1 August 2021, from https://collaborate.mitre.org/attackics/index.php/Technique_Matrix.

attackics. Collaborate.mitre.org. (2021). Retrieved 1 August 2021, from https://collaborate.mitre.org/attackics/index.php/Main_Page.

Iso.org. (2021a). Retrieved 1 August 2021, from <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en>.

Resources.sei.cmu.edu. (2021b). Retrieved 1 August 2021, from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf.

8 Anexo A

Tabla A.1 Formato para alcance de la estrategia. Impacto de los ciberataques en la estrategia de la organización.

Área de impacto//Nivel de Impacto	Bajo (1)	Medio Bajo (2)	Medio (3)	Medio Alto (4)	Alto (5)
Impacto de ciberataques en reputación/confianza de cliente					
Afectación a la reputación					
Cantidad de recursos necesarios para recuperar la reputación					
Pérdida de clientes por pérdida de confianza					
Impacto de ciberataques en las finanzas					
Costo de operación					
Pérdida de ingresos					
Impacto de ciberataques en la productividad					
Incremento diario de horas laborables para los especialistas					
Impacto de ciberataques en penalidades legales					
Costo de multas					
Número de demandas					
Número de investigaciones por parte del gobierno					
Impacto de ciberataques en las áreas de la organización					
Ciberseguridad					
Telecomunicaciones					
Ventas					
Preventas					
Finanzas					
Compras					
Publicidad					
Recursos Humanos					

Nota. Adaptado en Octave Allegro (Caralli et al., 2007).

Tabla A.2 Perfil de activos.

Activo de Información								
Identificador	Activo	Descripción	Razón de importancia	Responsables	Personal autorizado para acceso (confidencialidad)	Personal autorizado para modificar (integridad)	Tiempo activo (disponibilidad)	Prioridad de seguridad

Nota. Adaptado en Octave Allegro (Caralli et al., 2007).

Tabla A.3 Formato de Riesgos de Activos de Información.

Riesgo de Activos de Información					
Activo de información	Posible ciberataque ¿Quién, por qué y cómo?	Vulnerabilidad relacionada al posible ciberataque	Probabilidad de que suceda el ciberataque		Área de impacto
				Alta	Reputación
				Medio	Confianza de clientes
				Bajo	Financiero
					Productividad
					Multas y Penalidades legales
Resultado		Consecuencias	Acción contra la amenaza		Actividades de mitigación
	Divulgación			Aceptar	
	Modificación			Aplazar	
	Destrucción			Mitigar	
	Interrupción			Transferir	

Nota. Adaptado en Octave Allegro (Caralli et al., 2007).

Tabla A.4 Cuestionario de afectación de la triada de seguridad en un activo de información.

Actividades/ Nivel de intencionalidad	Confidencialidad	Integridad	Disponibilidad
Defecto de software			
Defecto de hardware			
Falla de sistema			
Ejecución de código malicioso			
Interrupción de corriente eléctrica			
Problema de red			
Desastre natural			

Nota. Adaptado en Octave Allegro (Caralli et al., 2007).

Tabla A.5 Cuestionario de evaluación de ciberseguridad

No	Categorías Totalmente en desacuerdo (1), En desacuerdo (2), Ni en de acuerdo ni en desacuerdo (3), De acuerdo (4) e Totalmente de acuerdo (5)	(1)	(2)	(3)	(4)	(5)
	Establecer alcance					
	Formalizar criterios de medida de riesgos					
1	¿Se tiene establecida y comunicada la estrategia del negocio, misión, visión, objetivos a los especialistas de IoT?					
2	¿Se tienen identificados y comunicados los servicios críticos de IoT?					
3	¿Se tienen establecidas las dependencias de los servicios críticos de IoT?					
	Administrar activos de información					
	Desarrollar el perfil de activos de la información					
4	¿Se tiene un inventario de los dispositivos y sistemas de IoT?					
5	¿Se tiene un inventario de plataformas y aplicaciones dentro de las instalaciones de IoT?					
6	¿Se tiene priorizados y clasificados los dispositivos de ciberseguridad?					
7	¿Se tiene mapeadas las redes de comunicaciones?					
	Identificar los detalles de activos de la información					
8	¿Se tienen identificados los atributos en los activos de información acorde a la estrategia del negocio?					
	Políticas y Procedimientos					
	Términos y definiciones					
9	¿Se tiene definidos los términos y definiciones relacionados a la seguridad de información?					
	Procedimientos y procesos de protección de información					
10	¿Se tiene establecido y comunicada una política de ciberseguridad organizacional?					
11	¿Se administran y entienden requerimientos legales de ciberseguridad?					
12	¿Se tiene una política de administración de riesgos?					

13	¿Se tiene identificado, establecido los procesos de administración de riesgos por la dirección?					
14	¿Están los proveedores de los sistemas de información identificados en la administración de riesgos?					
15	¿Los contratos con los proveedores solicitan las medidas para alcanzar los objetivos de programas de ciberseguridad ?					
16	¿Se evalúan las actividades de seguridad que los proveedores realizan en la infraestructura de IoT?					
17	¿Se tiene una política de control de accesos?					
18	¿Se tiene un proceso de control de cambios de configuración?					
19	¿Se tiene una política para generación y resguardo de línea base de configuraciones?					
20	¿Se tiene una política de respaldos de configuraciones?					
21	¿Se tiene una política de recuperación de configuraciones?					
22	¿Se tiene una política de destrucción de información y deshecho de equipos?					
23	¿Se tiene un procedimiento de monitoreo y correlación de eventos detectados?					
24	¿Se cuenta con un proceso de atención de eventos detectados?					
25	¿Existen procedimientos para analizar y notificar las vulnerabilidades de la infraestructura de IoT?					
Organización de la seguridad de la información						
26	¿Se tienen establecidos los roles y responsabilidades de los empleados de ciberseguridad, tanto internos y externos?					
27	¿Se tienen roles y responsabilidades de los proveedores de servicios de IoT?					
28	¿Se tiene una política de gestión de dispositivos móviles, asignación, cancelación, control ?					
29	¿Se tiene una política de gestión de aplicaciones en los dispositivos móviles?					
30	¿Se tienen políticas de seguridad de información específicas para dispositivos móviles?					
Proteger operación						
Operación de activos						
31	¿Se gestiona el acceso a las instalaciones físicas?					
32	¿Se tiene controlado el acceso remoto a los sistemas críticos?					
34	¿Esta implementado el control de acceso, para que las credenciales estén verificadas, revocadas y auditadas?					
33	¿Los usuarios se firman a los sistemas con un único ID?					
34	¿Se revisan periódicamente los accesos de las cuentas?					
35	¿Se tienen habilitado el registro de auditoría a las cuentas de administrador?					
36	¿Los accesos se asignan acorde a los privilegios y tareas específicas?					
37	¿La asignación de los accesos es supervisada?					

38	¿Se tiene una línea base de configuración de seguridad referente a los equipos/sistemas de la infraestructura de IoT?					
39	¿Se cuenta con redes segregadas basado en las funcionalidades de los sistemas?					
40	¿Los datos están guardados en un medio encriptado?					
41	¿La transferencia de datos se hace en un medio encriptado?					
42	¿Se garantiza la disponibilidad de la infraestructura de IoT?					
43	¿Se tienen mecanismos de revisión de integración para verificar la infraestructura de IoT?					
44	¿Se tiene un ambiente de desarrollo y pruebas separado al productivo?					
45	¿Se tiene contemplados mantenimientos a los activos de información?					
46	¿Se protegen los datos almacenados en medios removibles?					
Operación de recursos humanos						
47	¿Los especialistas/administradores de la infraestructura de IoT conocen los roles o responsabilidades?					
48	¿Los especialistas/administradores de seguridad de IoT conocen los roles o responsabilidades?					
49	¿Los proveedores conocen sus roles y responsabilidades?					
50	¿Todos los especialistas/administradores están entrenados en ciberseguridad?					
51	¿Todos los especialistas/administradores reciben comunicación constante de las políticas de seguridad?					
52	¿Los especialistas de seguridad cuentan con entrenamiento constante en ciberseguridad?					
53	¿La coordinación de las personas está integrada con las políticas de seguridad?					
54	¿Se comparte la situación de ciberseguridad a los especialistas?					
Identificar Amenazas						
Detectar áreas de preocupación						
55	¿Se analizan los eventos monitoreados para detectar amenazas de seguridad?					
56	¿Se correlacionan los eventos monitoreados?					
57	¿Los eventos monitoreados son clasificados y priorizados?					
58	¿Los eventos generan alertas para su atención?					
59	¿Se revisan los eventos a través de un detector de intrusos?					
60	¿Se tienen registros de eventos para ser revisados, auditados y documentados?					
61	¿Se comunica el impacto de los eventos detectados?					
62	¿Se monitorea la red y la infraestructura de IoT para detectar amenazas de seguridad?					
63	¿Se monitorean los accesos de los especialistas a los sistemas/infraestructura de IoT?					
64	¿Se monitorean los accesos de los usuarios finales a los sistemas/infraestructura de IoT?					

65	¿Se monitorean los accesos de los proveedores a los sistemas/infraestructura de IoT?					
Definir los escenarios de amenaza						
66	¿Se tienen detectadas las técnicas y tácticas de las amenazas de seguridad?					
67	¿Se tienen detectadas las amenazas de seguridad dirigidas a los usuarios finales?					
68	¿Se tienen detectadas las amenazas relacionadas a desastres naturales?					
Investigación de escritorio						
69	¿Se tiene identificadas las herramientas de seguridad que se utilizan en la infraestructura de IoT?					
70	¿Las herramientas implementadas en la infraestructura de IoT cubren los requerimientos de la política de seguridad?					
Cuestionario de ciberseguridad de IoT						
71	¿Se tiene algún medio para conocer las prácticas de seguridad de los especialistas de IoT?					
72	¿Se tiene algún medio para conocer las prácticas de seguridad de los usuarios finales?					
Taller con especialistas						
73	¿Hay alguna práctica para conocer la situación de operación de los especialistas de IoT?					
74	¿Se recolectan las ideas, opiniones y retroalimentaciones de los especialistas de IoT sobre la seguridad de información?					
Pruebas de Seguridad						
75	¿Se detectan las vulnerabilidades a través de herramientas especializadas de IT?					
76	¿Se detectan las vulnerabilidades realizando pruebas de simulación de ataques?					
Generar reporte						
77	¿Se documentan las amenazas y vulnerabilidades de seguridad detectadas?					
78	¿Se dan a conocer las amenazas y vulnerabilidades a los responsables de dirección?					
Mitigar amenazas						
Identificar riesgos						
79	¿Se cuenta con identificación de las vulnerabilidades de los activos de información?					
80	¿Se recopila información de vulnerabilidades de diversas fuentes?					
81	¿Se documentan las amenazas internas y externas de seguridad de información?					
82	¿Se tienen detectados los impactos al negocio de las amenazas de seguridad?					
83	¿Los riesgos están priorizados y documentados?					
Análisis de riesgos						
84	¿Se mitigan las vulnerabilidades reportadas o se documentan como aceptados?					

Seleccionar la mitigación						
85	¿Se tienen implementados dispositivos de infraestructura de seguridad?					
86	¿Se tiene implementado un detector de intrusos en la red?					
87	¿Se tiene implementado un dispositivo correlacionar de eventos?					
Manejo de incidentes						
88	¿Se entiende el impacto de las incidencias?					
89	¿Los incidentes son atendidos y mitigados?					
90	¿Se implementa un plan de atención durante una incidencia?					
91	¿Se realizan revisiones después de atención de incidencias?					
92	¿La revisión de incidencias incluye lecciones aprendidas?					
93	¿Se tiene un plan de recuperación de incidencias?					
94	¿Se tiene definido un tiempo medio para reparar, remplazar, restaurar una funcionalidad en caso de ciber ataque?					
95	¿Se tiene definido un tiempo medio para reaccionar a un ciberataque?					
96	¿Se tiene manejo de reputación después de las incidencias?					
97	¿Se tiene un plan de comunicación durante y después de las incidencias?					
98	¿Se tiene contemplado un análisis forense después de una incidencia?					
Cumplimiento						
Evaluación						
99	¿Se revisan frecuentemente el marco de seguridad implementado en la infraestructura de IoT?					
100	¿Se revisan regularmente las políticas de seguridad de información de IoT?					

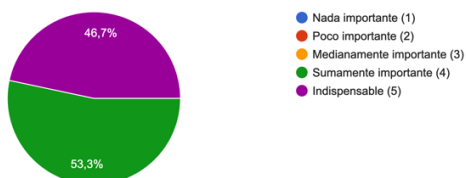
Nota. Adaptado (Bonebrake, 2022) (Yigit Ozkan & Spruit, 2019)

9 ANEXO B

A. Validación MaRCIoT. Resumen de preguntas

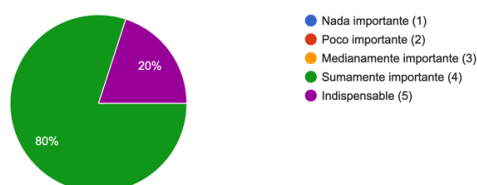
1. ¿Para un marco de referencia de seguridad de IoT que tan importante es tener una autoridad responsable del mismo?

Figura B.1. Autoridad responsable



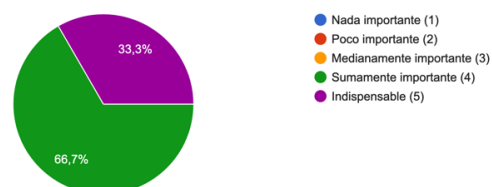
2. ¿Para un marco de referencia de seguridad de IoT que tan importante es que este apegada a la estrategia del negocio?

Figura B.2 Estrategia apegada al negocio



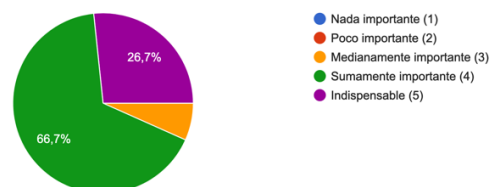
3. ¿Para un marco de referencia de seguridad de IoT que tan importante es una gestión de activos de la información?

Figura B.3 Gestión de activos de información



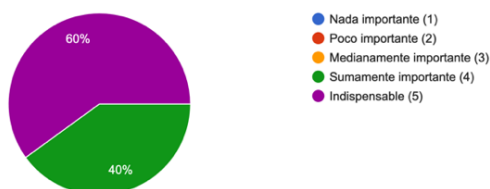
4. ¿Para un marco de referencia de seguridad de IoT que tan importante es contar con un glosario de términos y definiciones de seguridad de información?

Figura 9.4 Glosario de términos y definiciones



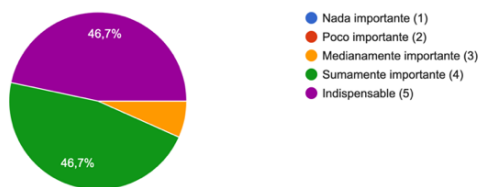
5. ¿Para un marco de referencia de seguridad de IoT que tan importante es establecer y formalizar políticas y procedimientos de seguridad de datos?

Figura B.5 *Formalizar políticas y procedimientos de seguridad de datos*



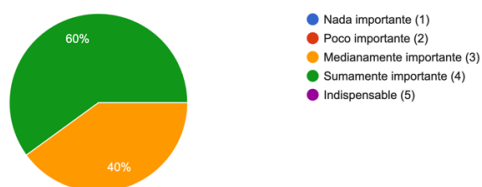
6. ¿Para un marco de referencia de seguridad de IoT que tan importante es comunicar las políticas de seguridad de información?

Figura B.6 *Comunicar políticas de seguridad*



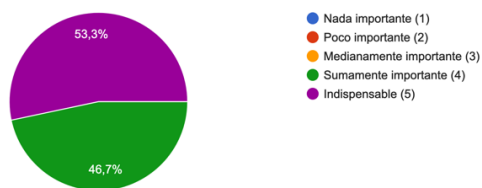
7. ¿Para un marco de referencia de seguridad de IoT que tan importante es una guía oral, aparte de la política principal?

Figura B.7 *Guía oral, aparte de la política principal*



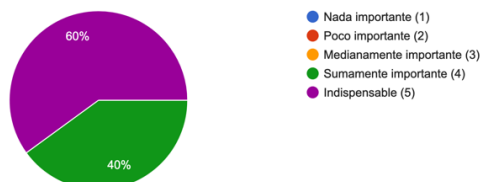
8. ¿Para un marco de referencia de seguridad de IoT que tan importante es tener establecido un procedimiento en casos emergentes?

Figura B.8 *Procedimientos en casos emergentes*



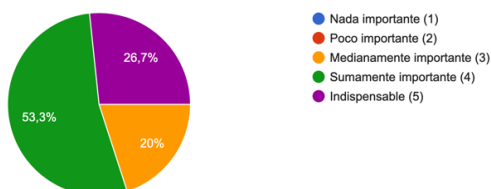
9. ¿Para un marco de referencia de seguridad de IoT que tan importante es la implementación de controles de seguridad en la operación, como la autenticación, el control de acceso, encriptación de datos, entre otros?

Figura B.9 *Implementación de controles de seguridad*



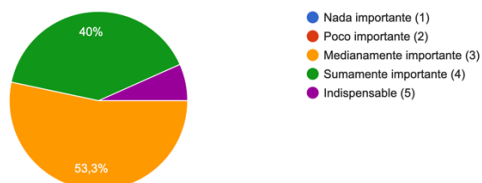
10. ¿Para un marco de referencia de seguridad de IoT que tan importante es identificar amenazas a través de investigación de escritorio con los especialistas?

Figura B.10 *Investigación de escritorio*



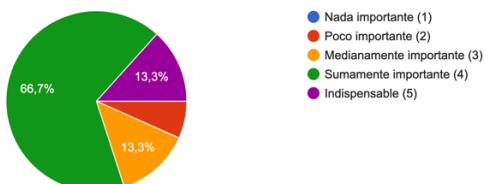
11. ¿Para un marco de referencia de seguridad de IoT que tan importante es identificar amenazas a través de un cuestionario de los especialistas?

Figura B.11 *Cuestionario de especialistas*



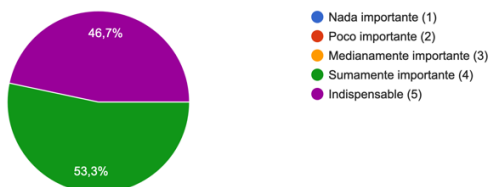
12. ¿Para un marco de referencia de seguridad de IoT que tan importante es identificar amenazas a través de colaboración abierta con los usuarios finales?

Figura B.12 *Colaboración abierta con los usuarios finales*



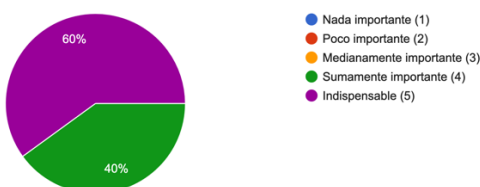
13. ¿Para un marco de referencia de seguridad de IoT que tan importante es identificar los riesgos de seguridad de información?

Figura B.13 *Importancia de riesgos de seguridad de información*



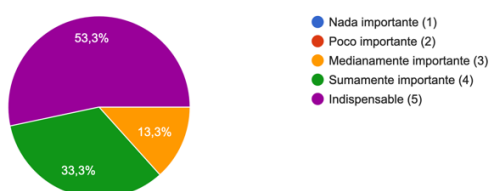
14. ¿Para un marco de referencia de seguridad de IoT que tan importante es mitigar o aceptar los riesgos de información detectados?

Figura B.14 *Mitigar o aceptar riesgos*



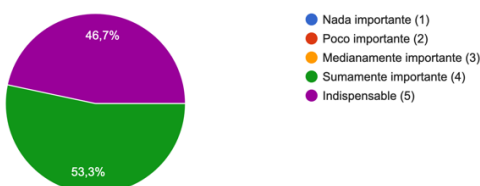
15. ¿Para un marco de referencia de seguridad de IoT que tan importante es implementar un sistema de detección de intrusos en la infraestructura de IoT?

Figura B.15 *Sistemas de detección de intrusos en IoT*



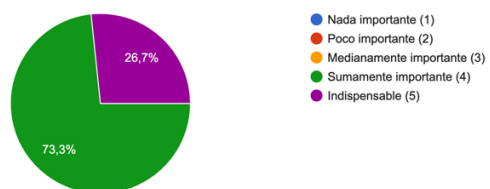
16. ¿Para un marco de referencia de seguridad de IoT que tan importante es contar con gestión de incidencias de seguridad de información?

Figura B.16 *Gestión de incidencias de seguridad de información*



17. ¿Para un marco de referencia de seguridad de IoT que tan importante es formalizar y comunicar un plan de comunicación en una incidencia de seguridad?

Figura B.17 *Formalizar y comunicar plan de comunicación*



10 ANEXO C

Tabla C.1 Vulnerabilidades de CVE ® (CVE - Search Results, 2022

Name	Description
CVE-2021-34431	In Eclipse Mosquitto version 1.6 to 2.0.10, if an authenticated client that had connected with MQTT v5 sent a crafted CONNECT message to the broker a memory leak would occur, which could be used to provide a DoS attack against the broker.
CVE-2021-33176	VerneMQ MQTT Broker versions prior to 1.12.0 are vulnerable to a denial of service attack as a result of excessive memory consumption due to the handling of untrusted inputs. These inputs cause the message broker to consume large amounts of memory, resulting in the application being terminated by the operating system.
CVE-2021-28166	In Eclipse Mosquitto version 2.0.0 to 2.0.9, if an authenticated client that had connected with MQTT v5 sent a crafted CONNACK message to the broker, a NULL pointer dereference would occur.
CVE-2021-0229	An uncontrolled resource consumption vulnerability in Message Queue Telemetry Transport (MQTT) server of Juniper Networks Junos OS allows an attacker to cause MQTT server to crash and restart leading to a Denial of Service (DoS) by sending a stream of specific packets. A Juniper Extension Toolkit (JET) application designed with a listening port uses the Message Queue Telemetry Transport (MQTT) protocol to connect to a mosquitto broker that is running on Junos OS to subscribe for events. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: 16.1R1 and later versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1.
CVE-2020-6882	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other devices by sending specific topics. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13>
CVE-2020-6881	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of abnormal messages. A remote attacker could connect to the MQTT server and send an MQTT exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13>
CVE-2020-5935	On BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) versions 15.1.0-15.1.0.5, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when handling MQTT traffic through a BIG-IP virtual server associated with an MQTT profile and an iRule performing manipulations on that traffic, TMM may produce a core file.
CVE-2020-27220	The Eclipse Hono AMQP and MQTT protocol adapters do not check whether an authenticated gateway device is authorized to receive command & control messages when it has subscribed only to commands for a specific device. The missing check involves verifying that the command target device is configured giving permission for the gateway device to act on its behalf. This means an authenticated device of a certain tenant, notably also a non-gateway device acting like a gateway, may receive command & control messages targeted at a different device of the same tenant without corresponding permissions getting checked.
CVE-2020-16168	Origin Validation Error in temi Robox OS prior to 120, temi Android app up to 1.3.7931 allows remote attackers to access the REST API and MQTT broker used by the temi and send it custom data/requests via unspecified vectors.
CVE-2020-13932	In Apache ActiveMQ Artemis 2.5.0 to 2.13.0, a specially crafted MQTT packet which has an XSS payload as client-id or topic name can exploit this vulnerability. The XSS payload is being injected into the admin console's browser. The XSS payload is triggered in the diagram plugin; queue node and the info section.
CVE-2020-13849	The MQTT protocol 3.1.1 requires a server to set a timeout value of 1.5 times the Keep-Alive value specified by a client, which allows remote attackers to cause a denial of service (loss of the ability to establish new connections), as demonstrated by SlowITe.
CVE-2020-13821	An issue was discovered in HiveMQ Broker Control Center 4.3.2. A crafted clientid parameter in an MQTT packet (sent to the Broker) is reflected in the client section of the management console. The attacker's JavaScript is loaded in a browser, which can lead to theft of the session and cookie of the administrator's account of the Broker.
CVE-2020-10071	The Zephyr MQTT parsing code performs insufficient checking of the length field on publish messages, allowing a buffer overflow and potentially remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.
CVE-2020-10070	In the Zephyr Project MQTT code, improper bounds checking can result in memory corruption and possibly remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.
CVE-2020-10062	An off-by-one error in the Zephyr project MQTT packet length decoder can result in memory corruption and possible remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.
CVE-2019-9749	An issue was discovered in the MQTT input plugin in Fluent Bit through 1.0.4. When this plugin acts as an MQTT broker (server), it mishandles incoming network messages. After processing a crafted packet, the plugin's mqtt_packet_drop function (in /plugins/in_mqtt/mqtt_prot.c) executes the memmove() function with a negative size parameter. That leads to a crash of the whole Fluent Bit server via a SIGSEGV signal.

CVE-2019-5635	A cleartext transmission of sensitive information vulnerability is present in Hickory Smart Ethernet Bridge from Belwith Products, LLC. Captured data reveals that the Hickory Smart Ethernet Bridge device communicates over the network to an MQTT broker without using encryption. This exposed the default username and password used to authenticate to the MQTT broker. This issue affects Hickory Smart Ethernet Bridge, model number H077646. The firmware does not appear to contain versioning information.
CVE-2019-5432	A specifically malformed MQTT Subscribe packet crashes MQTT Brokers using the mqtt-packet module versions < 3.5.1, 4.0.0 - 4.1.3, 5.0.0 - 5.6.1, 6.0.0 - 6.1.2 for decoding.
CVE-2019-19307	An integer overflow in parse_mqtt in mongoose.c in Cesanta Mongoose 6.16 allows an attacker to achieve remote DoS (infinite loop), or possibly cause an out-of-bounds write, by sending a crafted MQTT protocol packet.
CVE-2019-17389	In RIOT 2019.07, the MQTT-SN implementation (asymcute) mishandles errors occurring during a read operation on a UDP socket. The receive loop ends. This allows an attacker (via a large packet) to prevent a RIOT MQTT-SN client from working until the device is restarted.
CVE-2019-17210	A denial-of-service issue was discovered in the MQTT library in Arm Mbed OS 2017-11-02. The function readMQTTLenString() is called by the function MQTTDeserialize_publish() to get the length and content of the MQTT topic name. In the function readMQTTLenString(), mqttstring->lenstring.len is a part of user input, which can be manipulated. An attacker can simply change it to a larger value to invalidate the if statement so that the statements inside the if statement are skipped, letting the value of mqttstring->lenstring.data default to zero. Later, cur is accessed, which points to mqttstring->lenstring.data. On an Arm Cortex-M chip, the value at address 0x0 is actually the initialization value for the MSP register. It is highly dependent on the actual firmware. Therefore, the behavior of the program is unpredictable from this time on.
CVE-2019-16754	RIOT 2019.07 contains a NULL pointer dereference in the MQTT-SN implementation (asymcute), potentially allowing an attacker to crash a network node running RIOT. This requires spoofing an MQTT server response. To do so, the attacker needs to know the MQTT MsgID of a pending MQTT protocol message and the ephemeral port used by RIOT's MQTT implementation. Additionally, the server IP address is required for spoofing the packet.
CVE-2019-13120	Amazon FreeRTOS up to and including v1.4.8 lacks length checking in prvProcessReceivedPublish, resulting in untargetable leakage of arbitrary memory contents on a device to an attacker. If an attacker has the authorization to send a malformed MQTT publish packet to an Amazon IoT Thing, which interacts with an associated vulnerable MQTT message in the application, specific circumstances could trigger this vulnerability.
CVE-2019-12951	An issue was discovered in Mongoose before 6.15. The parse_mqtt() function in mg_mqtt.c has a critical heap-based buffer overflow.
CVE-2019-12496	An issue was discovered in Hybrid Group Gobot before 1.13.0. The mqtt subsystem skips verification of root CA certificates by default.
CVE-2019-11779	In Eclipse Mosquitto 1.5.0 to 1.6.5 inclusive, if a malicious MQTT client sends a SUBSCRIBE packet containing a topic that consists of approximately 65400 or more '/' characters, i.e. the topic hierarchy separator, then a stack overflow will occur.
CVE-2019-11778	If an MQTT v5 client connects to Eclipse Mosquitto versions 1.6.0 to 1.6.4 inclusive, sets a last will and testament, sets a will delay interval, sets a session expiry interval, and the will delay interval is set longer than the session expiry interval, then a use after free error occurs, which has the potential to cause a crash in some situations.
CVE-2019-11777	In the Eclipse Paho Java client library version 1.2.0, when connecting to an MQTT server using TLS and setting a host name verifier, the result of that verification is not checked. This could allow one MQTT server to impersonate another and provide the client library with incorrect information.
CVE-2019-10244	In Eclipse Kura versions up to 4.0.0, the Web UI package and component services, the Artemis simple Mqtt component and the emulator position service (not part of the device distribution) could potentially be target of XXE attack due to an improper factory and parser initialisation.
CVE-2019-0222	In Apache ActiveMQ 5.0.0 - 5.15.8, unmarshalling corrupt MQTT frame can lead to broker Out of Memory exception making it unresponsive.
CVE-2018-8531	A remote code execution vulnerability exists in the way that Azure IoT Hub Device Client SDK using MQTT protocol accesses objects in memory, aka "Azure IoT Device Client SDK Memory Corruption Vulnerability." This affects Hub Device Client SDK, Azure IoT Edge.
CVE-2018-5879	Improper length check while processing an MQTT message can lead to heap overflow in snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 835, SDA660, SDM630, SDM660
CVE-2018-19587	In Cesanta Mongoose 6.13, a SIGSEGV exists in the mongoose.c mg_mqtt_add_session() function.
CVE-2018-19417	An issue was discovered in the MQTT server in Contiki-NG before 4.2. The function parse_publish_vhdr() that parses MQTT PUBLISH messages with a variable length header uses memcpy to input data into a fixed size buffer. The allocated buffer can fit only MQTT_MAX_TOPIC_LENGTH (default 64) bytes, and a length check is missing. This could lead to Remote Code Execution via a stack-smashing attack (overwriting the function return address). Contiki-NG does not separate the MQTT server from other servers and the OS modules, so access to all memory regions is possible.
CVE-2018-18765	An exploitable arbitrary memory read vulnerability exists in the MQTT packet-parsing functionality of Cesanta Mongoose 6.13. It is a heap-based buffer over-read in mg_mqtt_next_subscribe_topic. A specially crafted MQTT SUBSCRIBE packet can cause an arbitrary out-of-bounds memory read potentially resulting in information disclosure and denial of service. An attacker needs to send a specially crafted MQTT packet over the network to trigger this vulnerability.
CVE-2018-18764	An exploitable arbitrary memory read vulnerability exists in the MQTT packet-parsing functionality of Cesanta Mongoose 6.13. It is a heap-based buffer over-read in a parse_mqtt_getul6 call. A specially crafted MQTT SUBSCRIBE packet can cause an arbitrary out-of-bounds memory read potentially resulting in information disclosure and denial of service. An attacker needs to send a specially crafted MQTT packet over the network to trigger this vulnerability.

CVE-2018-17614	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Losant Arduino MQTT Client prior to V2.7. User interaction is not required to exploit this vulnerability. The specific flaw exists within the parsing of MQTT PUBLISH packets. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-6436.
CVE-2018-1684	IBM WebSphere MQ 8.0 through 9.1 is vulnerable to a error with MQTT topic string publishing that can cause a denial of service attack. IBM X-Force ID: 145456.
CVE-2018-16528	Amazon Web Services (AWS) FreeRTOS through 1.3.1 allows remote attackers to execute arbitrary code because of mbedTLS context object corruption in prvSetupConnection and GGD_SecureConnect_Connect in AWS TLS connectivity modules.
CVE-2018-15323	On BIG-IP 14.0.0-14.0.0.2 or 13.0.0-13.1.1.1, in certain circumstances, when processing traffic through a Virtual Server with an associated MQTT profile, the TMM process may produce a core file and take the configured HA action.
CVE-2018-11998	While processing a packet decode request in MQTT, Race condition can occur leading to an out-of-bounds access in snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, SD 210/SD 212/SD 205, SD 427, SD 435, SD 450, SD 625, SD 636, SD 835, SDA660, SDM630, SDM660, Snapdragon_High_Med_2016
CVE-2018-11993	Improper check while accessing the local memory stack on MQTT connection request can lead to buffer overflow in snapdragon wear in versions MDM9206, MDM9607
CVE-2017-9868	In Mosquitto through 1.4.12, mosquitto.db (aka the persistence file) is world readable, which allows local users to obtain sensitive MQTT topic information.
CVE-2017-7651	In Eclipse Mosquitto 1.4.14, a user can shutdown the Mosquitto server simply by filling the RAM memory with a lot of connections with large payload. This can be done without authentications if occur in connection phase of MQTT protocol.
CVE-2017-7650	In Mosquitto before 1.4.12, pattern based ACLs can be bypassed by clients that set their username/client id to '#' or '+'. This allows locally or remotely connected clients to access MQTT topics that they do have the rights to. The same issue may be present in third party authentication/access control plugins for Mosquitto.
CVE-2017-7296	An issue was discovered in Contiki Operating System 3.0. A Persistent XSS vulnerability is present in the MQTT/IBM Cloud Config page (aka mqtt.html) of cc26xx-web-demo. The cc26xx-web-demo features a webserver that runs on a constrained device. That particular page allows a user to remotely configure that device's operation by sending HTTP POST requests. The vulnerability consists of improper input sanitisation of the text fields on the MQTT/IBM Cloud config page, allowing for JavaScript code injection.
CVE-2017-2895	An exploitable arbitrary memory read vulnerability exists in the MQTT packet parsing functionality of Cesanta Mongoose 6.8. A specially crafted MQTT SUBSCRIBE packet can cause an arbitrary out-of-bounds memory read potentially resulting in information disclosure and denial of service. An attacker needs to send a specially crafted MQTT packet over the network to trigger this vulnerability.
CVE-2017-2894	An exploitable stack buffer overflow vulnerability exists in the MQTT packet parsing functionality of Cesanta Mongoose 6.8. A specially crafted MQTT SUBSCRIBE packet can cause a stack buffer overflow resulting in remote code execution. An attacker needs to send a specially crafted MQTT packet over the network to trigger this vulnerability.
CVE-2017-2893	An exploitable NULL pointer dereference vulnerability exists in the MQTT packet parsing functionality of Cesanta Mongoose 6.8. An MQTT SUBSCRIBE packet can cause a NULL pointer dereference leading to server crash and denial of service. An attacker needs to send a specially crafted MQTT packet over the network to trigger this vulnerability.
CVE-2017-2892	An exploitable arbitrary memory read vulnerability exists in the MQTT packet parsing functionality of Cesanta Mongoose 6.8. A specially crafted MQTT packet can cause an arbitrary out-of-bounds memory read and write potentially resulting in information disclosure, denial of service and remote code execution. An attacker needs to send a specially crafted MQTT packet over the network to trigger this vulnerability.
CVE-2016-9877	An issue was discovered in Pivotal RabbitMQ 3.x before 3.5.8 and 3.6.x before 3.6.6 and RabbitMQ for PCF 1.5.x before 1.5.20, 1.6.x before 1.6.12, and 1.7.x before 1.7.7. MQTT (MQ Telemetry Transport) connection authentication with a username/password pair succeeds if an existing username is provided but the password is omitted from the connection request. Connections that use TLS with a client-provided certificate are not affected.
CVE-2016-10523	MQTT before 3.4.6 and 4.0.x before 4.0.5 allows specifically crafted MQTT packets to crash the application, making a DoS attack feasible with very little bandwidth.
CVE-2014-6116	The Telemetry Component in WebSphere MQ 8.0.0.1 before p000-001-L140910 allows remote attackers to bypass authentication by setting the JAASConfig property in an MQTT client configuration.
CVE-2014-0923	IBM MessageSight 1.x before 1.1.0.0-IBM-IMA-IT01015 allows remote attackers to cause a denial of service (daemon restart) via crafted MQ Telemetry Transport (MQTT) authentication data.
CVE-2014-0922	IBM MessageSight 1.x before 1.1.0.0-IBM-IMA-IT01015 allows remote attackers to cause a denial of service (resource consumption) via WebSockets MQ Telemetry Transport (MQTT) data.