UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

"MODELOS DE SEGURIDAD, ACCIONES Y PROTOCOLOS PARA LA PREVENCIÓN DE VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LAS TECNOLOGÍAS IOT Y API RESTFUL"

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: BRYAN ANDRES CASTRO MACIAS

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Bryan Andres Castro Macías con documento de identificación N° 0925738015 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 26 de febrero del año 2022

Atentamente,

Bryan Andres Castro Macías
0925738015

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Bryan Andres Castro Macías con documento de identificación No. 0925738015, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Modelos de seguridad, acciones y protocolos para la prevención de vulnerabilidades de la seguridad de la información mediante las tecnologías IOT y API RESTful", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 26 de febrero del año 2022

Atentamente,

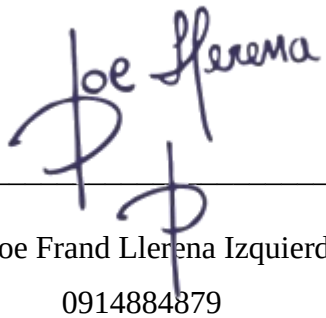
Bryan Andres Castro Macías
0925738015

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: MODELOS DE SEGURIDAD, ACCIONES Y PROTOCOLOS PARA LA PREVENCIÓN DE VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LAS TECNOLOGÍAS IOT Y API RESTFUL, realizado por Bryan Castro Macías con documento de identificación N° 0925738015, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 26 de febrero del año 2022

Atentamente,



Joe Frand Llerena Izquierdo, Msc.
0914884879

DEDICATORIA

Dedico este trabajo principalmente a mi madre la Sra. Angela Macías que se esforzó mucho por darnos las mejores enseñanzas, llenarnos de valores éticos y morales aun estando sola desde que éramos unos niños, ya que ya no se encuentra con nosotros desde hace muchos años mi difunto padre el Sr. Silvio Castro (+), mi madre siempre nos dijo que su mayor orgullo son sus hijos y que unos de sus mayores sueños es ver graduados a sus 3 hijos y yo soy el ultimo que falta, así que esto va por ti mi hermosa y amada madre.

También se lo dedico a mis dos hermanos Sr. Tito Castro y Sr. Steven Castro, que siempre me apoyaron en todo lo que pudieron, una gran y reconocida dedicatoria a mi hermano Tito Castro que varias veces me apoyo económicamente para darme unos pequeños lujos, como la mayoría de los jóvenes que creo yo deseamos, pero no podía dármelos ya que la mayoría de mi salario la invertía en mis estudios.

Dedicado también para todas las personas que han creído en mi diciéndome que soy una persona muy inteligente y que nunca deje de luchar, ya que todo lo que quiero lo puedo conseguir.

Bryan Andres Castro Macías

AGRADECIMIENTO

Agradezco a Dios por haberme dado la vida y salud para estar donde estoy en estos momentos ya que es gracias a su voluntad que todos estamos donde estamos, gracias a mi madre por haberme y tenerme tanta paciencia ya que tengo un carácter a veces muy fuerte, gracias a mis hermanos que los amo con todo el corazón y sé que siempre puedo contar con ellos.

También agradezco a la Universidad Politécnica Salesiana por siempre creer en sus estudiantes y siempre llenarnos de valores y amor por el prójimo y, por último, pero no menos importante a todos los docentes de la universidad que siempre tuvieron la amabilidad y carisma en enseñarnos de la mejor manera posible y sobre todo a mi tutor y gran profesor Joe Llerena Izquierdo.

RESUMEN

La vulnerabilidad de la seguridad de la información, debido al auge de dispositivos IoT en la actualidad y el nexo que tiene con la red, se convierte en el objetivo perfecto para cometer delitos informáticos. El desarrollo tecnológico evoluciona y con ello, propósitos delincuenciales siguen siendo un problema de forma general debido al aumento de ataques informáticos generados. Para una institución y debiendo garantizar el cumplimiento de confidencialidad, integridad y disponibilidad de toda la información en las actividades operacionales y comerciales, se ven comprometida a impulsar seguridades aplicadas a los servicios que rodean la IoT (Internet de las cosas) y API RESTful. Con el soporte de consultas de fuentes bibliográficas se busca identificar esquemas de las problemáticas presentadas en la seguridad de la información, analizando y clasificando de forma metodológica y sistemática la información precisa de enfocar la prevención y corrección de vulnerabilidades para mantener la confidencialidad, integridad y disponibilidad de los datos. De un total de 1700 artículos en primera línea, de acuerdo con los filtros aplicados sobre el tema propuesto, se definen 65 artículos de alta relevancia. Se tiene como resultado la importancia de aplicar políticas de seguridad en nuevas tecnologías usando la guía de buenas prácticas de las normas ISO. Se concluye que este trabajo aporta con aspectos definidos sobre la seguridad de la información en distintas fases de un ambiente tecnológico, permitiendo analizar modelos de esquematización para proteger la información de las organizaciones ante el uso de tecnologías con servicios IoT y API RESTful. Se concluye que las vulnerabilidades se van a mantener en el tiempo, y aún más con el uso de nuevas tecnologías, pero siempre será necesario la implementación de protocolos que permitan generar confianza en los usuarios y de esta manera no estar expuestos a amenazas.

Palabras claves: Seguridad, IoT, tecnologías emergentes, API RESTful.

ABSTRACT

The vulnerability of information security, due to the rise of IoT devices today and the nexus it has with the network, becomes the perfect target for committing cybercrime. Technological development evolves and with it, criminal purposes continue to be a general problem due to the increase of computer attacks generated. For an institution and having to ensure compliance with confidentiality, integrity, and availability of all information in operational and commercial activities, they are committed to promote security applied to services surrounding the IoT (Internet of Things) and RESTful APIs. With the support of consultations of bibliographic sources, we seek to identify outlines of the problems presented in information security, analyzing, and classifying in a methodological and systematic way the precise information to focus on the prevention and correction of vulnerabilities to maintain the confidentiality, integrity and availability of data. From a total of 1700 articles in first line, according to the filters applied on the proposed topic, 65 articles of high relevance are defined. The result is the importance of applying security policies in new technologies using the good practices guide of the ISO standards. It is concluded that this work contributes with defined aspects on information security in different phases of a technological environment, allowing to analyze schematization models to protect the information of the organizations before the use of technologies with IoT services and RESTful APIs. It is concluded that vulnerabilities will be maintained over time, and even more with the use of new technologies, but it will always be necessary to implement protocols to generate confidence in users and thus not be exposed to threats.

Key words: Security, IoT, emerging technologies, API RESTful.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

La adaptación de tecnologías emergentes modernas son descritas como el internet de las cosas (IoT), manteniendo un constante cambio en las plataformas digitales de las organizaciones, con el objetivo de innovar, agilizar y ofrecer una alta gama de oportunidades de mejoras en las operaciones de las instituciones (Griffy-Brown et al., 2019)(Ayala Carabajo & Llerena Izquierdo, 2016)(Salazar Acosta, 2018), lo cual a su vez ha generado grandes e importantes riesgos en la seguridad de los datos (Llerena Izquierdo et al., 2009), por lo tanto, las organizaciones necesitan comprender y tomar acciones entorno al riesgo que se incurre en la implementación de estas tecnologías emergentes.

Los modelos esquemáticos de seguridad adaptados en la web y sus servicios interconectados ofrecen actualmente un marco referencial para los requisitos en la seguridad de la información basados en el planteamiento de diseño, procedimientos, métodos, protocolos y técnicas con el fin de obtener información segura y confiable (Hina et al., 2015)(Ayala Carabajo & Llerena Izquierdo, 2017).

Ante esta situación el manejo y control de procesos lógicos, sistemáticos y de infraestructura, ayudará a optimizar el riesgo que existe con la vulnerabilidad de la información mediante la aplicación de estrategias para reducir o eliminar riesgos vulnerables de los datos (Llerena Izquierdo et al., 2018).

Enfocamos la parte de seguridad de los datos dentro de una organización la garantía que se cumpla con la integridad de la información, su confidencialidad y disponibilidad en actividades operacionales y comerciales de la organización, por lo tanto, es importante establecer políticas y controles con el objetivo de salvaguardar la información (Melendrez-Caicedo & Llerena-Izquierdo, 2022)(Hina & Dominic, 2016)(Ayala Carabajo & Llerena Izquierdo, 2014)(de la Nube Toral Sarmiento et al., 2018)(Llerena-Izquierdo & Ayala-Carabajo, 2021).

Las tecnologías IOT y API RESTful buscan simplificar la estructura de servicios y equipos interconectados en red de la empresa a través de sus interfaces de software creados (Garg & Dave, 2019)(Llerena Izquierdo, 2020).

El objetivo de este trabajo consiste en centrar medidas de prevención bajo el concepto de investigación científica, ante el uso cada vez más en auge de las tecnologías emergentes, explorando durante los últimos 7 años (2015) hasta la actualidad en plataformas digitales de

modelos y protocolos que se enfocan en la prevención y corrección de vulnerabilidades de aspectos de seguridad.

2. REVISIÓN DE LITERATURA

Los filtros aplicados en la búsqueda de bases de datos científicas pueden variar de acuerdo con su fecha y año de publicación actual, con el fin de implantar nuevos resultados representativos sobre servicios IOT y Api RESTful representada en la tabla 1.

Tabla 1. Cadenas de búsqueda en bases indexadas.

Base de datos indexadas	Búsqueda aplicada	Resultados
PROQUEST	(MODEL SECURITY IOT AND API RESTFUL)	51
IEEEXPLORE	("All Metadata":Model of security of information JSON) AND ("All Metadata":IOT) OR ("All Metadata":RESTFUL)	37
SPRINGER	(IOT AND API RESTFUL)	10
WEB OF SCIENCE	((ALL= (JSON WEB)) AND ALL=(IOT)) OR ALL=(API RESTFUL)	65

La seguridad de la información dentro de las instituciones debe garantizar que se cumpla la CIA (Confidencialidad, Integridad y Disponibilidad) de la información en las actividades operacionales y comerciales de la organización, por lo tanto, es importante establecer políticas y controles con el objetivo de salvaguardar la información (Montalvo & Morán, 2012)(Sánchez Guzmán, 2021).

la identificación de las diferentes amenazas a las que se encuentran expuesta la información ante el uso de las tecnologías emergentes y la identificación de las acciones serán los imperativos de la investigación (Coello Ochoa, 2021)(Ponce Larreategui, 2021)(Holguín Mendoza, 2021)(Vera Navas, 2021), así como los modelos o protocolos que se enfocan en la prevención y corrección de vulnerabilidades para garantizar la seguridad de la información (Guaigua Bucheli, 2021)(Morán Maldonado, 2021) (Llerena Izquierdo & Vélez Chilán, 2011)(López & Parra, 2015)(Chévez Morán, 2021)(Escalante Quimis, 2021)(Guaranda Lara, 2021)(Narváez Picón, 2021).

2.1. Modelos de conectividad aplicados a entornos IoT y API RESTfull

En la actualidad las entidades gubernamentales en su meta por generar más servicios, ingresos y oportunidades de negocio van de la mano con los avances tecnológicos como IoT, lo que a su vez permite la aparición de nuevas vulnerabilidades que deben ser gestionadas de manera eficiente (Amato et al., 2020)(Llerena Izquierdo, 2014)(Rosero Tejada, 2021)(Moncayo Ronquillo, 2021).

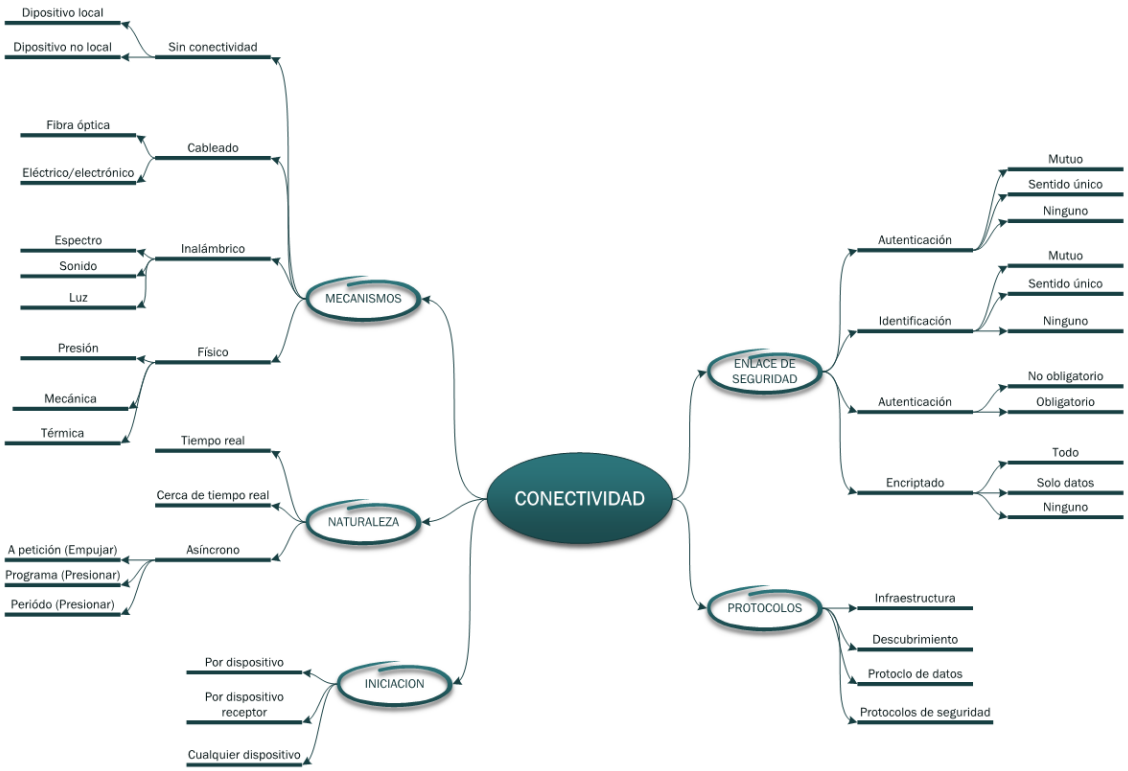


Figura.1. Conectividad en un entorno de IoT

Los eventos o problemas van creciendo con la admisión de nuevas arquitecturas como el Internet de las cosas (IoT), así como los datos recolectados en IoT son muy sensibles y privados para los usuarios (ver Fig. 1). Los problemas de privacidad y seguridad de la información, como por ejemplo en el sector de la salud, son críticos para la privacidad del ciudadano, por tal motivo, no deben ser accedidos por usuarios o entidades no autorizadas (Aguirre Sánchez, 2021). La arquitectura IoT recopila o produce datos a través de los sensores y actuadores. Los dispositivos pueden estar conectados directamente a Internet, a una red local cableada o de forma inalámbrica, WiFi o rango de Radio Frecuencia (RF) (Boyes et al., 2018)(Pazmiño Sánchez, 2021).

La norma ISO/IEC 30141, brinda un vocabulario y arquitectura de referencia IoT (ISO / IEC JTC, 2018)(Rodríguez Pesantes, 2021)(Terán Terranova, 2021), para el modelado de aplicativos y su desarrollo. La finalidad es obtener altos estándares de seguridad que permitan además desarrollar sistemas fiables y, mantener la integridad y la confidencialidad de la información a la hora de enfrentar un ciberataque (Miranda Jiménez, 2021)(Ponce Larreategui, 2021)(Muñoz Campuzano, 2021)(Vera Navas, 2021)(Orozco Bonilla, 2021).

De acuerdo con la ISO citada anteriormente, los componentes de un sistema IoT, corresponden a seis dominios, los cuales son, dominio de usuario, dominio de operaciones y gestión, dominio del servicio de la aplicación, dominio de recursos e intercambio, dominio de detección y control, dominio de la entidad física. Una parte de la visión de IoT se basa en la instrucción de que los avances establecidos en microelectrónica, las tecnologías de la información y las comunicaciones presenciadas durante la última época (ver Tabla 2) perdurarán en un futuro con una sociedad hiperconectada (Fraile et al., 2021)(Alladi et al., 2021)(Xenofontos et al., 2021). Sectores como la salud y el servicio al cliente de las diferentes organizaciones públicas ya están usando las aplicaciones de IoT. De igual forma, las universidades y las escuelas están incorporando este tipo de sistemas (Yadav et al., 2018) acogiendo las consideraciones técnicas para precautelar la ciberseguridad de IoT (Prehofer, 2015).

Tabla 2. Limitaciones y riesgos con el uso de IoT.

Consideraciones	Limitantes IoT	Riesgos IoT
Ciclo de Vida	Vida útil de los dispositivos varía, algunos dispositivos (como los sensores simples) son de corta duración, mientras que otros pueden durar décadas.	Con el tiempo los dispositivos no se pueden actualizar. Los mecanismos de seguridad integrados pueden resultar vulnerables o en desuso, como las antiguas suites de cifrado.
Bajos Costos	Valor percibido por el consumidor de un dispositivo depende en gran medida del costo de compra e implementación del dispositivo. Los impulsores del mercado a menudo requieren que las empresas produzcan dispositivos a un costo muy bajo.	Para satisfacer las presiones de precios, los dispositivos pueden tener una potencia de procesamiento baja y un espacio de hardware restringido, lo que ofrece un soporte limitado para los mecanismos de seguridad.
Consumo de energía	Los dispositivos de IoT requieren una batería de larga duración, sin	El hardware de bajo consumo puede carecer de capacidades adicionales

acceso a una fuente de alimentación permanente.	como la de admitir cifrado o mecanismos de seguridad.

Las API nos permiten exponer el dispositivo conectado a los usuarios en una manera segura (Salagean & Zinca, 2020)(Chen, Huang, et al., 2020)(Park & Nam, 2020)(Chen, Huo, et al., 2020). La mayor parte de implementaciones de IoT actuales utilizan arquitectura REST sobre conectividad basada en HTTP desde el cliente al servidor. Las API RESTful son utilizadas ampliamente en la web actual. La transferencia de datos por lo general se realiza mediante JSON o XML a través de HTTP. Es un buen modelo para los sistemas heterogéneos. El sistema RESTful brinda seguridad en diferentes esquemas (ver Fig. 2).

Figura 2. Esquemas de seguridad en RESTful

Esquema de seguridad Cliente-Servidor. En este esquema el modelo de ejecución distribuida hacia usuarios finales (cliente-servidor), permite solicitar acceso transparente a las aplicaciones tecnológicas de datos u servicios enviados desde un servidor remoto.

Esquema de seguridad Sin estado. En este esquema se obtiene una respuesta a los diferentes procesos de solicitud recibidas de los agentes de red tecnológicos sin mantener sesiones abiertas.

Esquema de seguridad Cacheable. En este esquema el rendimiento de la capa de almacenamiento de datos transitorios soporta varios niveles evitando repetir conexiones simultaneas de aplicaciones distribuidas (cliente-servidor) permitiendo la recuperación de un mismo recurso.

Esquema de seguridad mediante Interfaz uniforme. En este esquema se utiliza el modelo de normas para la interacción del desarrollo de interfaz de diseño para los servicios API RESTful

en tecnologías emergentes, aplicados hacia los usuarios finales (cliente-servidor) mostrando que los recursos de los servicios REST tenga una única dirección, "URI".

Esquema de seguridad mediante Sistema de capas. En este esquema el modelo aplicado en el desarrollo de las aplicaciones es de suma importancia caracterizarla por capas para su implementación y validez de los datos mejorando la seguridad, escalabilidad y el rendimiento.

2.2. Protocolos usados para reforzar la seguridad de los sistemas de información

A continuación, revisamos diferentes esquemas de protocolos más comunes aplicando en distintos modelos de seguridad de sistemas de información basados en el uso de tecnologías emergentes.

Seguridad Message Queing Telemetry Transport. Protocolo de comunicación enfocado en el funcionamiento TCP/IP, cuya conectividad es de tipo Machine-to-Machine (M2M) (Prehofer, 2015). Las distintas medidas de seguridad que adopta MQTT es la protección de las comunicaciones tales como: Transporte SSL/TLS y la autenticación por medio de un certificado o por un usuario y contraseña (Garg & Dave, 2019). Por Transporte SSL/TLS la capacidad que tienen en los terminales Iot es limitada generando cargas de procesos importante (Salagean & Zinca, 2020). Para la parte de autentificación de usuario y contraseña se considera importante porque envía archivos de texto plano generando brecha de seguridad. Mediante la transferencia de datos MQTT podemos transferir datos a una velocidad de 20 a 25 veces. Tomamos como ejemplo la autenticación en Cloud IoT atraves de los puentes MQTT o HTTP realizando autenticación de corta duración con la conexión de dispositivos que tiene como seguridad token web JSON (JWT) (Salagean & Zinca, 2020).

Seguridad JSON Web Token Basados en el estándar (RFC 7519) para los desarrollos en JSON Web Token (JWT) genera seguridad a las comunicaciones IoT, definiéndolos de modo compacto y autónomo para la transmisión de información mediante un objeto JSON. La información procesada es verificada y firmada digitalmente dando confiabilidad en los archivos de texto procesados. Utilizan algoritmo HMAC para claves públicas o privadas con el uso de JWT.

Características principales de tipos de token y sus casos de uso:

- ID token: Emitido por un gestor de identidades. Permite ejecutar aplicaciones distribuida hacia usuarios finales (cliente-servidor) de manera fiable y segura sin la gestión de sus credenciales.

- Data token: Trabaja de manera fácil en la transmisión de peticiones HTTP ejecutados por la seguridad JWT en el intercambio de datos

- Access token: El tipo de modelo empleado por un servidor de autorización por petición de usuarios finales (cliente-servidor), permite el acceso a un recurso protegido a través de un token usando método autenticación y verificación de datos.

Usamos JWT que permita el intercambio de datos de forma segura, se puede dar en los escenarios: Sesión entre cliente y servidor, autenticación federada, autorización de acceso. Los datos de IoT se deben proteger tanto en reposo como en la trasmisión y, pueden garantizar así la integridad de los datos. Las soluciones de seguridad IoT en APIs se implementan para detectar intrusiones no deseadas y prevenir ataques maliciosos en la comunicación (Freed & Borenstein, 1996a).

Seguridad Advanced Message Queuing Protocol. Sus siglas conocidas como AMQP protocolo de comunicación del nivel 7 (modelo OSI) ejecuta aplicaciones distribuidas de tipo publicación y suscripción. Dado que su modelo es robusto en el soporte de transacciones mejorando la seguridad, escalabilidad y el rendimiento de los datos de forma cifrada utilizando autenticación mediante llaves de tipo SASL o TLS generando compatibilidad en los protocolos HTTP y HTPPS de datos transitorios soportando varios niveles evitando repetir conexiones simultaneas de aplicaciones distribuidas (cliente-servidor) permitiendo la recuperación de un mismo recurso (Moran, 2018)(Freed & Borenstein, 1996b)(Cerf, 1969).

Seguridad Data Distribution Service. El servicio DDS concebida para sistemas de tiempo real generando una buena solución para aplicaciones informáticas distribuidas como el intercambio de datos tales como archivos físicos, lógicos, pantalla, impresora. Ofreciendo seguridad a través de los protocolos TLS, DTSL (Rescorla, 2000)(Jones, 2015).

Seguridad Hypertext Transfer Protocol. Ofrece transmisión independiente de información en grandes cantidades a través de peticiones de datos y recursos mediante el esquema API REST apoyado por el estándar HTTP (Lu, 2020)(Garg & Dave, 2019). Asegurando que la información

transmitida sea con protocolos criptográfico SSL/TLS en HTTP, cualquier método aplicado en las respuestas de intercambio de información en un dispositivo IoT lo realice con conexión a un solo cliente HTTP, lo que hace factible utilizar su propia Api de manera muy sencilla en formato soportado de tipo JSON (Yergeau, 2003)(Jones, 2015)(Sáez, 2019).

3. MATERIALES Y MÉTODOS

Utilizamos el proceso de metodología descriptiva para elaborar un mapeo sistemático, cuyos resultados fueron de conclusiones generales de información investigativa existentes a partir de premisas particulares sobre el funcionamiento de aspectos de seguridad, en tecnologías emergentes de servicios IOT y API RESTful, ejecutando técnicas de revisión bibliográfica aplicadas a trabajos relacionados sobre seguridad de la información.

3.1. Fases de investigación

A partir de modelos de esquemas particulares sobre el funcionamiento de aspectos de seguridad, en los dispositivos con servicios IOT y API RESTful (Hina et al., 2015)(Prehofer, 2015), se realiza la revisión de literatura para la clasificación de trabajados relacionados explorados sobre información de vulnerabilidades en las plataformas digitales. Se establecen cinco fases: (I) Definir el objetivo a investigar, (II) Delimitar preguntas de investigación, (III) Desarrollar planteamiento de método de búsqueda bibliográficas de diferentes esquemas de seguridad, (IV) Fase de criterios de selección referenciadas, (V) Procesamiento y Análisis de Ambientes Virtuales.

FASE I. Definir el objetivo a Investigar. Las tecnologías IOT y API RESTFUL buscan simplificar la estructura de servicios de dispositivos interconectados en red desde los procesos de comunicación industriales u domésticos a través de sus interfaces de software creados mediante el sistema RESTful. El objetivo de la presente investigación consiste en la identificación de las diferentes amenazas a las que se encuentran expuesta la información ante el uso de las tecnologías emergentes al consumir el cliente el servicio del api desarrollado; así como la identificación de las acciones, modelos o protocolos que se enfocan en la prevención y corrección de vulnerabilidades para garantizar la seguridad de la información.

FASE II. Delimitar preguntas de Investigación. Es importante definir preguntas de investigación que permitan la creación de esquemas de seguridad para sistemas heterogéneos, las preguntas que guiaron la presente investigación se presentan a continuación: (ver Tabla 3).

Tabla 3. Delimitación de Preguntas de investigación

Preguntas	Búsqueda de información
¿Cuál ha sido el valor numérico de gran importancia de búsqueda científica e investigativa en aspectos de seguridad relacionados con vulnerabilidades en tecnologías emergentes utilizando servicios IoT y API RESTful desde el año 2015?	Cantidad de cadenas de búsquedas por años
¿Cuál es el porcentaje aplicado en aspecto de seguridad sobre vulnerabilidad de información basados en servicios IoT y API RESTful desde el año 2015?	Tendencias de aplicación por años
¿Qué tipo de referencias aplican los modelos de seguridad y protocolos con respecto al sistema RESTful?	Características de las publicaciones

FASE III. Desarrollar el planteamiento para el de método de búsqueda bibliográficas de diferentes esquemas de seguridad. Con la información recopilada de la búsqueda en los repositorios indexados de aprendizaje se ha llevado a cabo una revisión en distintas fases de proceso como la búsqueda inicial, con PROQUEST(MODEL SECURITY IOT AND API RESTFUL), IEEEXPLORE("All Metadata":Model of security of information JSON) AND ("All Metadata":IOT) OR ("All Metadata":RESTFUL); SPRINGER (IOT AND API RESTFUL); WEB OF SCIENCE((ALL=(JSON WEB)) AND ALL=(IOT)) OR ALL=(API RESTFUL), aplicando después en la fase siguiente una revisión de búsqueda de literatura relevante con estas palabras claves. La búsqueda planteada para la primera fase toma como punto de partida el año 2015 y presenta datos relacionados con tecnologías de servicios interconectados referentes servicios IOT, API RESTFUL, posteriormente se realiza la combinación de términos booleanos AND, OR en la búsqueda con las bases de datos PROQUEST, IEEEXPLORE, SPRINGER, WEB OF SCIENCE.

FASE IV. Fase de criterios de selección referenciadas. Para recopilar información que existen de manera general de estudios pertinentes e importantes se consideran los siguientes criterios de identificación de las diferentes amenazas a las que se encuentran expuesta la información ante el uso de las tecnologías emergentes y la identificación de las acciones, modelos o

protocolos que se enfocan en la prevención y corrección de vulnerabilidades para garantizar la seguridad de la información. Criterios de Inclusión. Se escogen temas de investigación relacionadas con tecnologías emergentes modernas ya sea en artículos, revistas, libros publicados. Así como estudios de identificación de esquemas o modelos que se enfocan en la prevención y corrección de vulnerabilidades manteniendo la confidencialidad, integridad y disponibilidad de la información en las organizaciones. Información obtenida en cualquier idioma. Criterios de Exclusión. Se excluyen estudios relacionados y publicados anteriores al año 2015. Se excluyen esquemas importantes de seguridad acogiendo las consideraciones técnicas que restringen o limitan la ciberseguridad de la IoT.

FASE V. Procesamiento y Análisis de Ambientes Virtuales. Para este sustento se comandará los resultados del tema propuesto a las preguntas planteadas de las fases anteriores. ¿Cuál ha sido el valor numérico de gran importancia de búsqueda científica e investigativa en aspectos de seguridad aporto con conocimiento de vulnerabilidad en tecnologías emergentes utilizando, servicios IoT y API RESTful desde el año 2015? Se observa (ver Tabla 4) que en diversas fuentes y de una manera independiente el estudio realizado de los puntos relacionado da un total de 56 trabajos propuestos por año en las diferentes bases de datos virtuales de PROQUEST con un valor de 17, en el IEEExplore, obtuvimos 23 trabajos, en el SPRINGER 7 y 9 trabajos en WEB OF SCIENCE.

Tabla 4. Número de trabajos virtuales por año

AÑO	PROQUEST	IEEExplore	SPRINGER	WEB OF SCIENCE	TOTAL
2015	1	2	0	0	3
2016	2	3	0	0	5
2017	2	2	0	1	5
2018	2	5	1	2	10
2019	4	7	2	2	15
2020	3	4	3	2	12
2021	3	0	1	2	6

¿Cuál es el porcentaje aplicado en aspecto de seguridad sobre vulnerabilidad de información en aspectos de seguridad basados servicios IoT y API RESTful desde el año 2015? Se evidencia que el porcentaje de trabajos relevantes es alto en el año 2015, en la base indexada del IEEExplore un 67%, en el 2016 alcanza un 60%, y en el 2017 un 40%, en el 2018 un 50%, en el 2019 un 47%, en el 2020 un 33%, y en el 2021 sin ningún porcentaje; para Proquest en

cambio se presenta, un 33% en el 2015, el 2016 tiene 40%, el 2017 con 40%, el 2018 con 20%, el 2019 con 27%, el 2020 con 25%, el 2021 con 50%; en la base del Web of Science un 0% en el 2015, el 2016 tiene 0%, el 2017 con 20%, el 2018 con 20%, el 2019 con 13%, el 2020 con 17%, el 2021 con el 33%; en la base de Springer un 0% en el 2015, el 2016 tiene 0%, el 2017 con 0%, el 2018 con 10%, el 2019 con 13%, el 2020 con 25%, el 2021 con el 17% de publicaciones válidas para el análisis, (ver Fig.3).

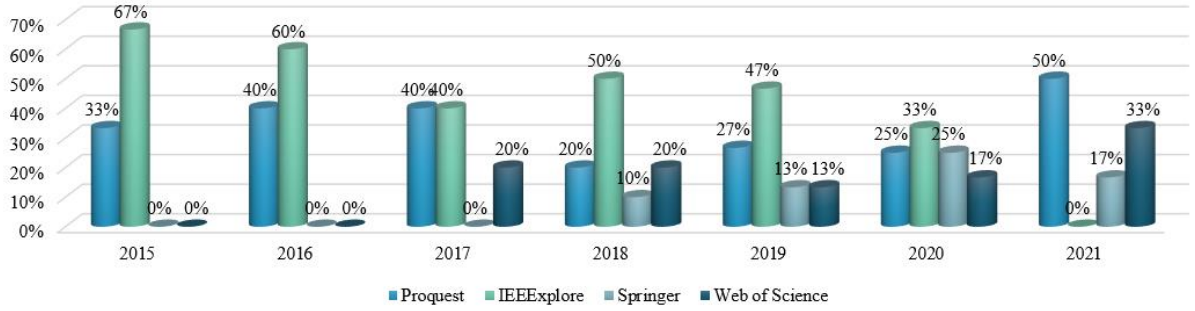


Figura 3. Porcentaje de trabajos relevantes por año

4. RESULTADOS

Para encontrar hallazgos pertinentes al objetivo de la investigación se aplicaron filtros de búsquedas adecuados para considerar trabajos relevantes (revistas científicas, y artículos de congresos), con el fin de elaborar el mapeo sistemático de trabajos relacionados con modelos y protocolos, analizar los resultados e interpretar la clasificación de la información obtenida.

Recopilamos los datos de las búsquedas de los repositorios indexados de aprendizaje se ha llevado a cabo una revisión en distintas fases de proceso como la búsqueda inicial, aplicando después en la fase siguiente una revisión de literatura relevante con un total de 163 resultados. La búsqueda planteada para la primera fase, presentan datos desde el año 2015 relacionados con tecnologías de servicios interconectados referentes a servicios IOT, API RESTful, y se realiza la combinación de términos booleanos AND, OR, obteniendo resultados óptimos para esta fase, además de considerar la selección de artículos valorados de criterios de inclusión y exclusión (ver Fig. 4).

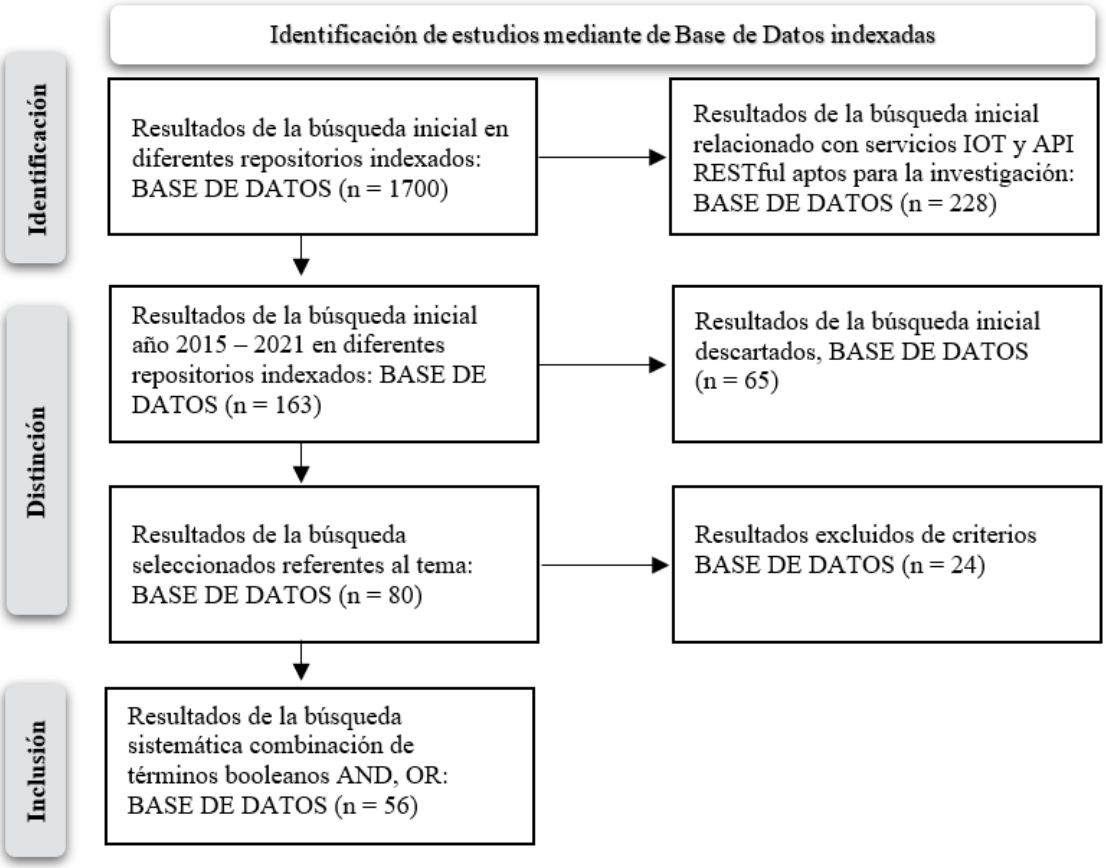


Figura 4. Flujo de datos PRISMA del proceso de recolección de datos

Obtuvimos en los resultados a través de la selección de criterios generales, aplicando filtros de búsqueda más específicos sobre el tema propuesto y que cumplan con la selección de información virtual de títulos, palabras claves, autores e idiomas disponibles, basados en 4 bibliotecas virtuales, como se observa en el diagrama PRISMA utilizado (ver Fig. 4) (Alvarado-Salazar & Llerena-Izquierdo, 2022). Se contabilizaron un total de 1700 documentos científicos obtenidos disponibles en las diferentes bases de datos donde constan aquellos artículos, revistas y conferencias referenciadas de mejores prácticas y seguridades a aplicarse en las tecnologías emergentes. Con la masificación y el gran flujo de datos de IoT y API RESTful, aplicando términos booleanos surge la importancia de aplicar políticas de seguridad en estas nuevas tecnologías usando la guía de buenas prácticas de las normas ISO arrojando resultados finales de un total de 56 documentos. Para la siguiente búsqueda se aplicaron filtros de investigación de las actividades desarrolladas que, para este estudio, se obtiene un total de 163 referencias de ambientes virtuales, se escogen finalmente, 51 trabajos de PROQUEST, 37 trabajos de IEEExplore, 10 trabajos de SPRINGER, y 65 trabajos de WEB OF SCIENCE.

4.1. Resultado de la selección de protocolos.

En la tabla 5, se presenta con un mínimo de referencias de modelos de protocolos en temas relacionados e importantes, 5 trabajos de PROQUEST, 7 trabajos de IEEExplore, 2 trabajos de SPRINGER y 3 trabajos de WEB OF SCIENCE, identificados por año, de acuerdo con el estudio seleccionado que dan soporte al tema propuesto.

Tabla 5. Referencias de trabajos importantes por año en las bases de datos indexadas

AÑO	PROQUEST	IEEExplore	SPRINGER	WEB OF SCIENCE
2015	JSON Web Algorithms (JWA)	Models at REST or modelling RESTful interfaces for the Internet of Things		
2016		Information security policies: Investigation of compliance in universities		
2017		Security Trust Zone in 5G networks		
2018	IoT: Challenges and Issues in Indian Perspective	The industrial internet of things (IoT): An analysis framework	ISO/IEC 30141:2018 Internet of Things (IoT) - Reference Architecture	

2019	NIST Cybersecurity for IoT Program - NIST	Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware		Emerging technologies and risk: How do we optimize enterprise risk when deploying emerging technologies?
2020	IoT Applications based on MQTT Protocol.	The use of MQTT in M2M and IoT systems: A survey. Measurement and Analysis of Network Data Based on MQTT Protocol.	Security Architecture and Protocols for Secure MQTT-SN.	Measurement and Analysis of Network Data Based on MQTT Protocol.
2021	Measurement and Analysis of Network Data Based on MQTT Protocol.	Measurement and Analysis of Network Data Based on MQTT Protocol.		Empowered Intrusion Detection Architecture for the Internet of Vehicles

4.2. Resultados obtenidos a través de la revisión sistemática de protocolos de seguridad para la prevención de vulnerabilidades.

Presentamos en la tabla 6, características principales de algunos de estos protocolos expuestos en las diferentes búsquedas de información en los repositorios indexados de PROQUEST, IEEExplore, SPRINGER, WEB OF SCIENCE. Se evidencia la confianza que brindan los protocolos SSL, TLS y DTLS aplicados de forma individual o en conjunto para los modelos existentes (Sáez, 2019).

Tabla 6. Modelo comparativo de Protocolos

PROTOCOLOS	MODELO	TRANSPORTE	SEGURIDAD	ESQUEMA DE SEGURIDAD
Seguridad MQTT (Advanced Message Queuing Protocol)	Publicación/Suscripción	TCP/IP	SSL/TLS	Cliente-Servidor
Seguridad JWT (JSON Web Token)	Petición/Respuesta	TCP/IP	TLS	Interfaz uniforme
Seguridad AMQP (Advanced Message Queuing Protocol)	Intercambio de mensajes	TCP/IP	TLS	Cliente-Servidor
Seguridad DDS (Data Distribution Service)	Publicación/Suscripción	TCP/IP	TLS/DTLS	Cacheable
Seguridad HTTP (REST/JSON)	Petición/Respuesta	TCP/IP	SSL/TLS	Cliente-Servidor

(Hypertext
Transfer Protocol)

5. DISCUSIÓN

En este estudio se han desarrollado los aspectos de seguridad en los datos que se definen en fases detalladas sobre medidas de prevención de ataques informáticos. Se determina que estos no garantizan que no exista violación a la información mediante algún ataque, pero sin embargo ayudan a reducir y mitigar las vulnerabilidades existentes. Las vulnerabilidades se van a mantener en el tiempo, y aún más con el uso de nuevas tecnologías, pero siempre será necesario la implementación de protocolos que permitan generar confianza en los usuarios y de esta manera no estar expuestos a amenazas.

Los análisis de seguridad deben ser más divulgados cuando se incluyen nuevas tecnologías con diferentes tipos de servicios protocolarios, seguros y confiables. Con la gran diversidad que existe en la actualidad y con su variedad en sistemas operativos, un análisis más riguroso en las diferentes capas debe ser un desafío en los que están implicados los servicios que ofrecen las organizaciones.

6. CONCLUSIÓN

Con los resultados obtenidos en este tema de investigación propuesto y soportado por cuatro bases de datos indexadas PROQUEST, IEEExplore, SPRINGER y WEB OF SCIENCE, que de un total general de 1700 artículos (desde el 2015), y desglosado por filtros aplicados de búsquedas llegando a 65 artículos relevantes, correspondiente al 3.82% que son objeto de estudio, se determina la sistematización de modelos existentes que permiten dar respuesta a la vulnerabilidad y los riesgos recurrentes que hay sobre la seguridad de la información en las organizaciones.

Se concluye que los aspectos definidos sobre la seguridad de la información en distintas fases de un ambiente tecnológico permiten analizar modelos de esquematización para proteger la información de las organizaciones ante el uso de tecnologías con servicios IoT y API RESTful, siguiendo las normas ISO y protocolos más seguros.

Las políticas de seguridad en IoT se está volviendo cada vez más importante, con el crecimiento en la industria de la tecnología y con más dispositivos conectados a Internet en el ámbito gubernamental. La API puede autenticarse en el servidor y este puede autenticarse para evitar los ataques de the man-in-the-middle. La norma ISO/IEC 30141 da una arquitectura de referencia, para el diseño y desarrollo de aplicaciones con IoT and API RESTful con el fin de reforzar la seguridad y la protección, creando sistemas fiables, cumpliendo con la privacidad y afrontando un ciberataque.

Como trabajo a futuro se planea la creación de un modelo de seguridad aplicado de forma general para las tecnologías emergentes en las organizaciones, con el objetivo de que cumplan lineamientos establecidos basados en la experiencia de trabajos recientes.

REFERENCIAS

Aguirre Sánchez, M. J. (2021). *Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20566

Alladi, T., Kohli, V., Chamola, V., Yu, F. R., & Guizani, M. (2021). Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles. *IEEE Wireless Communications*, *28*(3), 144–149. https://doi.org/10.1109/mwc.001.2000428

Alvarado-Salazar, R., & Llerena-Izquierdo, J. (2022). Revisión de la literatura sobre el uso de Inteligencia Artificial enfocada a la atención de la discapacidad visual. *Revista InGenio*, *5*(1), 10–21. https://doi.org/https://doi.org/10.18779/ingenio.v5i1.472

Amato, F., Casola, V., Cozzolino, G., De Benedictis, A., & Moscato, F. (2020). Exploiting Workflow Languages and Semantics for Validation of Security Policies in IoT Composite Services. *IEEE Internet of Things Journal*, *7*(5), 4655–4665. https://doi.org/10.1109/JIOT.2019.2960316

Ayala Carabajo, R., & Llerena Izquierdo, J. (2014). *Primer Congreso Salesiano de Ciencia, Tecnología e Innovación para la Sociedad. Memoria Académica*. http://dspace.ups.edu.ec/handle/123456789/9506

Ayala Carabajo, R., & Llerena Izquierdo, J. (2016). *Segundo Congreso Salesiano de Ciencia, Tecnología e Innovación para la Sociedad*. https://dspace.ups.edu.ec/handle/123456789/12776

Ayala Carabajo, R., & Llerena Izquierdo, J. (2017). *Tercer Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad*. https://dspace.ups.edu.ec/handle/123456789/14450

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Cerf, V. G. (1969). *ASCII format for network interchange*. https://doi.org/10.17487/rfc0020

Chen, F., Huang, Y., Zhu, J. M., Gao, S., Sui, Z., & Duan, M. J. (2020). Measurement and Analysis of Network Data Based on MQTT Protocol. *International Conference on Communication Technology Proceedings, ICCT*, *2020-Octob*, 92–96. https://doi.org/10.1109/ICCT50939.2020.9295944

Chen, F., Huo, Y., Liu, K., Tang, W., Zhu, J., & Sui, Z. (2020). A study on MQTT node selection. *Proceedings - 2020 16th International Conference on Mobility, Sensing and Networking, MSN 2020*, 622–623. https://doi.org/10.1109/MSN50589.2020.00101

Chévez Morán, M. J. (2021). *Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones*. http://dspace.ups.edu.ec/handle/123456789/20568

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

de la Nube Toral Sarmiento, A., Loaiza Martínez, M. de L., Llerena Izquierdo, J., Ayala Carabajo, R., Torres Toukoumidis, A., Romero-Rodríguez, L. M., Aguaded, I., Vega Ureta, N. T., Fuentes Espinoza, P. G., Peñafiel Caicedo, J. A., & others. (2018). *4to. Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad. Memoria académica*. http://dspace.ups.edu.ec/handle/123456789/16318

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica*. http://dspace.ups.edu.ec/handle/123456789/20576

Fraile, F., Montalvillo, L., Rodriguez, M. A., Navarro, H., & Ortiz, A. (2021). *Multi-tenant Data Management in Collaborative Zero Defect Manufacturing*. 464–468. https://doi.org/10.1109/metroind4.0iot51437.2021.9488534

Freed, N., & Borenstein, N. (1996a). *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. https://doi.org/10.17487/rfc2045

Freed, N., & Borenstein, N. (1996b). *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*. https://doi.org/10.17487/rfc2046

Garg, H., & Dave, M. (2019). Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware. *Proceedings - 2019 4th International Conference on Internet of Things: Smart Innovation and Usages, IoT-SIU 2019*. https://doi.org/10.1109/IoT-SIU.2019.8777334

Griffy-Brown, C., Miller, H., Zhao, V., Lazarikos, D., & Chun, M. (2019). Emerging technologies and risk: How do we optimize enterprise risk when deploying emerging technologies? *2019 IEEE Technology and Engineering Management Conference, TEMSCON 2019*. https://doi.org/10.1109/TEMSCON.2019.8813743

Guaigua Bucheli, C. J. (2021). *Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20319

Guaranda Lara, S. N. (2021). *Modelo de gestión para el alineamiento de estrategias corporativas en pymes mediante las tecnolog{\'\i}as de la información y comunicación*. http://dspace.ups.edu.ec/handle/123456789/20911

Hina, S., & Dominic, D. D. (2016). Information security policies: Investigation of compliance in universities. *2016 3rd International Conference on Computer and Information Sciences, ICCOINS 2016 - Proceedings*, 564–569. https://doi.org/10.1109/ICCOINS.2016.7783277

Hina, S., Dominic, D. D., Prehofer, C., Yadav, E. P., Mittal, E. A., Yadav, H., Garg, H., Dave, M., Amato, F., Casola, V., Cozzolino, G., De Benedictis, A., & Moscato, F. (2015). Models at REST or modelling RESTful interfaces for the Internet of Things. In *IEEE Internet of Things Journal* (Vol. 7, Issue 5, pp. 251–255). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JIOT.2019.2960316

Holguín Mendoza, J. D. (2021). *Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20915

ISO / IEC JTC. (2018). *ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture*. https://www.iso.org/standard/65695.html

Jones, M. (2015). JSON Web Key (JWK). In *Internet Engineering Task Force, IETF* (Request for Comments, Vol. 151, Issue 7517). RFC Editor. https://doi.org/10.17487/RFC7517

Llerena-Izquierdo, J., & Ayala-Carabajo, R. (2021). University Teacher Training During the COVID-19 Emergency: The Role of Online Teaching-Learning Tools. *International Conference on Information Technology & Systems*, 90–99. https://doi.org/10.1007/978-3-030-68418-1_10

Llerena Izquierdo, J. (2014). *Presentación. Primer Congreso Salesiano de Ciencia, Tecnología e Innovación para la Sociedad. Memoria Académica*. https://dspace.ups.edu.ec/handle/123456789/10961

Llerena Izquierdo, J. (2020). *Codifica en Python*. https://pure.ups.edu.ec/es/publications/codifica-en-python

Llerena Izquierdo, J., Naranjo Sánchez, R., Zambrano Santos, M., & Espol. (2018, July 5). *Sistema de*

información geográfico socioeconómico y del medio ambiente. Espol. http://www.dspace.espol.edu.ec/handle/123456789/43942

Llerena Izquierdo, J., Ortiz Rojas, J. G., Mora Saltos, N. S., & Freire, L. (2009, February 20). *Sistema de Gestión de Asistencia Institucional, SIGAI*. https://www.dspace.espol.edu.ec/handle/123456789/767

Llerena Izquierdo, J., & Vélez Chilán, M. (2011). *Determinación de la oferta de calidad de los servicios privados y/o comunitarios reconocidas por el Ministerio de Turismo en la sierra ecuatoriana, Andes*. https://dspace.ups.edu.ec/handle/123456789/1772

López, C., & Parra, A. (2015). *Análisis técnico de los recursos disponibles de la UEFS Santa María Mazzarello de Guayaquil para el diseño e implementación de un escenario de arquitectura*. 143. http://dspace.ups.edu.ec/handle/123456789/10286

Lu, L. (2020). Design and Implementation of an Interactive Information System for University Education under the Cloud Service Model. *2020 IEEE Conference on Telecommunications, Optics and Computer Science, TOCS 2020*, 377–381. https://doi.org/10.1109/TOCS50858.2020.9339620

Melendrez-Caicedo, G., & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos*. http://dspace.ups.edu.ec/handle/123456789/20966

Moncayo Ronquillo, K. C. (2021). *Seguridades de la información bases de datos distribuidas: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21701

Montalvo, A., & Morán, P. (2012). *Propuesta de un Sistema de Gestión del conocimiento para el Departamento de Tecnología de la Información y la incidencia Económica para el Grupo MAVESA.* https://dspace.ups.edu.ec/handle/123456789/3653

Moran, B. (2018). A Firmware Update Architecture for Internet of Things Devices. *Internet Engineering Task Force*, 12. https://doi.org/10.17487/rfc2119

Morán Maldonado, N. M. (2021). *Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20243

Muñoz Campuzano, P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20932

Narváez Picón, E. A. (2021). *Las tecnologías de la información y comunicación orientadas a la calidad del servicio en la gestión empresarial: una revisión sistemática*. https://dspace.ups.edu.ec/handle/123456789/20929

Orozco Bonilla, C. A. (2021). *Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/20933

Park, C. S., & Nam, H. M. (2020). Security Architecture and Protocols for Secure MQTT-SN. *IEEE Access*, *8*, 226422–226436. https://doi.org/10.1109/ACCESS.2020.3045441

Pazmiño Sánchez, C. A. (2021). *Protocolo Lora para análisis de medición con GPS y Arduino en la Industria ganadera del Ecuador: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20340

Ponce Larreategui, J. G. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la*

seguridad informática con enfoque en el código malicioso. http://dspace.ups.edu.ec/handle/123456789/20937

Prehofer, C. (2015). Models at REST or modelling RESTful interfaces for the Internet of Things. *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, 251–255. https://doi.org/10.1109/WF-IoT.2015.7389061

Rescorla, E. (2000). *HTTP Over TLS*. https://doi.org/10.17487/rfc2818

Rodríguez Pesantes, R. P. (2021). *Seguridad en dispositivos IOT en Organizaciones de América Latina*. http://dspace.ups.edu.ec/handle/123456789/20970

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21699

Sáez, I. (2019). IoT: protocolos de comunicación, ataques y recomendaciones | INCIBE-CERT. *IoT: Protocolos de Comunicación, Ataques y Recomendaciones*, 1–7. https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

Salagean, M., & Zinca, D. (2020). IoT Applications based on MQTT Protocol. *2020 14th International Symposium on Electronics and Telecommunications, ISETC 2020 - Conference Proceedings*. https://doi.org/10.1109/ISETC50328.2020.9301055

Salazar Acosta, L. I. (2018). *Implementación de sistema de matriculación y carnetización en la unidad educativa Pablo Picasso.* https://dspace.ups.edu.ec/handle/123456789/16844

Sánchez Guzmán, C. O. (2021). *Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad*. https://dspace.ups.edu.ec/handle/123456789/20321

Terán Terranova, Y. J. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un Mapeo Sistemático*. https://dspace.ups.edu.ec/handle/123456789/20333

Vera Navas, N. A. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales*. http://dspace.ups.edu.ec/handle/123456789/20949

Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., & Choo, K. K. R. (2021). Consumer, Commercial and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3079916

Yadav, E. P., Mittal, E. A., & Yadav, H. (2018). IoT: Challenges and Issues in Indian Perspective. *Proceedings - 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU 2018*. https://doi.org/10.1109/IoT-SIU.2018.8519869

Yergeau, F. (2003). *UTF-8, a transformation format of ISO 10646*. https://doi.org/10.17487/rfc3629