UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES INFORMÁTICOS

Tema:

PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO – ECUADOR

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

ÁREA: Sector Financiero – Gestión Empresarial

LÍNEA DE INVESTIGACIÓN: Seguridad informática

AUTOR: Christian Paul Quispe García

TUTOR: Ing. Elsa Pilar Urrutia Urrutia, Mg.

Ambato – Ecuador

septiembre – 2021

APROBACIÓN DEL TUTOR

En calidad de tutora del Trabajo de Titulación con el tema: PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO – ECUADOR, desarrollado bajo la modalidad Proyecto de Investigación por el señor Christian Paul Quispe García, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, septiembre 2021

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.

TUTORA

AUTORÍA

El presente Proyecto de Investigación titulado: PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO – ECUADOR es absolutamente original, auténtico y personal. En tal virtud, el contenido, a efectos legales y académicos que se despenden del mismo, son de exclusiva responsabilidad del autor.

Ambato, septiembre 2021

Christian Paul Quispe García

CC: 1803475811

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Christian Paul Quispe García, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO – ECUADOR, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, septiembre 2021

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.

PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
RUBEN EDUARDO NOGALES PORTERO

Ing. Rubén Eduardo Nogales Portero

PROFESOR CALIFICADOR

Firmado electrónicamente por:
OSCAR FERNANDO IBARRA TORRES

Ing. Oscar Fernando Ibarra Torres

PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, septiembre 2021

Christian Paul Quispe García

C.C. 1803475811

AUTOR

DEDICATORIA

A mi padre que con sacrificio, valentía, humildad me ha apoyado incondicionalmente y me ha enseñado el valor incalculable de luchar día a día ante cualquier adversidad.

A mi madre que me ha demostrado que nada es imposible y que todos los sueños se pueden hacer realidad con esfuerzo, dedicación, perseverancia y sencillez.

A mis hermanos que me han enseñado que el valor de la hermandad no tiene precio, que la alegría y esperanza van de la mano para enfrentar cualquier fracaso, que la honradez, respeto, dignidad no se compran y que cada problema debe ser resuelto con positivismo sin bajar los brazos.

A aquellos que ya no están dejando un legado de sabiduría, conocimientos y lecciones ayudándome a mejorar como ser humano.

AGRADECIMIENTO

A Dios y la Virgen Santísima que me han brindado la oportunidad de alcanzar este logro académico y me han bendecido con la sabiduría e inteligencia necesaria para poder demostrar mis conocimientos y así afrontar cualquier desafío de la vida.

A mi tutora, por su compromiso, enseñanza, dedicación por formar y mostrar mis capacidades escondidas día a día.

Pero, especialmente agradezco a mis padres por haber confiado en mí, demostrándome su apoyo incondicional día a día y enseñándome que la mayor riqueza que uno puede tener es la educación, valores, respeto a uno mismo y a los demás.

LO ÚNICO IMPOSIBLE ES AQUELLO QUE NO INTENTAS.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

Actualmente, la evolución tecnológica genera riesgos como incidentes informáticos, pérdida de funcionalidad en herramientas tecnológicas, ciberataques, robo o hackeos de la información y fraudes. Es por ello que, este trabajo determina un procedimiento de gestión para ciberseguridad según el análisis de las herramientas de monitoreo de red. En ese sentido, se establece las fases para la gestión de riesgos de ciberseguridad en base al caso de estudio. Con este fin, se revisaron documentos en español e inglés indizados en bases de datos como: Journal of Cyber Security Technology, Science Direct, Scopus, Springer, Espacios y ProQuest. Seguidamente, el análisis de la literatura permitió sustentar el objeto de estudio y consolidar los resultados en base a la herramientas de monitoreo y análisis de red según el enfoque básico de la Metodología Magerit. En conclusión, la investigación refleja la importancia de un procedimiento de gestión para ciberseguridad en la infraestructura tecnológica del sector financiero con la finalidad de salvaguardar las funciones como disponibilidad, autenticidad, integridad y confidencialidad.

Palabras clave: Procedimiento de gestión, ciberseguridad, infraestructura tecnológica, herramientas, sector financiero.

ABSTRACT

Currently, technological evolution generates risks such as computer incidents, loss of functionality in technological tools, cyberattacks, theft or hacking of information and fraud. That is why, this work determines a management procedure for cybersecurity according to the analysis of network monitoring tools. In this sense, the phases for the management of cybersecurity risks are established based on the case study. To this end, documents in Spanish and English indexed in databases such as: Journal of Cyber Security Technology, Science Direct, Scopus, Springer, Espacios and ProQuest were reviewed. Next, the analysis of the literature allowed to support the object of study and consolidate the results based on the monitoring and network analysis tools according to the basic approach of the Magerit Methodology. In conclusion, the research reflects the importance of a management procedure for cybersecurity in the technological infrastructure of the financial sector in order to safeguard functions such as availability, authenticity, integrity and confidentiality.

Keywords: Management procedure, cybersecurity, technological infrastructure, tools, financial sector.

INTRODUCCIÓN

En la actualidad, la evolución tecnológica ha permitido el desarrollo económico-social de una empresa, entidad u organización. Sin embargo, estas se exponen a riesgos como incidentes informáticos, ciberataques, robo o hackeos de la información, fraudes, entre otros debido a la falta de procedimientos de gestión de ciberseguridad. Es así que, se evidencia que el sector financiero no cuenta con un continuo seguimiento a procesos de seguridad informática, lo cual puede generar pérdida de funcionalidad en herramientas tecnológicas.

Es por ello, que la investigación tiene como objetivo determinar un procedimiento de gestión para ciberseguridad según el análisis de las herramientas de monitoreo de red. Por tanto, el presente estudio denominado "PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO - ECUADOR" se desarrolló en los siguientes capítulos:

- Capítulo I.- Marco Teórico, detalla los antecedentes investigativos, la contextualización del problema, la fundamentación teórica y los objetivos que guiarán el desarrollo del proyecto.
- Capítulo II.- Metodología, señala los materiales y métodos (modalidad, recolección de la información, y procesamiento y análisis de datos) a emplear durante la investigación.
- Capítulo III.- Resultados y Discusión, describe el análisis y discusión de los resultados, donde se identifica en tiempo real la actividad maliciosa a través de herramientas de monitoreo y análisis de red, y plantea las etapas o fases del procedimiento de gestión para la ciberseguridad según el sector.
- Capitulo IV.- Conclusiones y Recomendaciones, determina las respectivas conclusiones del estudio al estar finalizado y las recomendaciones para futuras investigaciones o proyectos similares que se relacionen con el tema.

CAPITULO I.-

MARCO TEÓRICO

1.1 Tema de Investigación

Procedimiento de gestión para ciberseguridad en la infraestructura tecnológica del sector financiero segmento 1 regulado por la Superintendencia de Economía Popular y Solidaria (SEPS) en el cantón Ambato - Ecuador.

1.2 Antecedentes Investigativos

Mediante una búsqueda bibliográfica en las bases de datos Journal of Cyber Security Technology, Science Direct, Scopus, Springer y Espacios, se presenta los antecedentes investigativos que aportan al proyecto de investigación propuesto. A continuación el detalle (Tabla 1.1):

Tabla 1.1: Búsqueda bibliográfica de antecedentes investigativos

Fuente: Elaboración propia

Tipo de investigación	Artículo Científico Libro			**Autores**	[1, 2, 3, 4, 5, 6, 7, 8]
Tema	**Aporte**				**Acerca de**
	Teórico	Práctico	Empírico	Analítico	
Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica.	x		x		Ciberseguridad (origen, prevención y evolución).
Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas.	x	x			Seguridad cibernética y métodos de evaluación del riesgo.

The role of cyber-security in information technology education.	x			x	Ciberseguridad en un contexto de educación de TI bajo el marco "Preparar, defender y actuar".
The financial technology (fintech) and cybersecurity.	x			x	Ciberseguridad en la tecnología financiera.
Educación en ciberseguridad. Planificación del futuro mediante el desarrollo de la fuerza laboral.		x			Un plan de acción (metas, involucrados y esquema) educativo sobre ciberseguridad.
Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe.	x				Ciberseguridad a nivel mundial.
Cyber security and IT infrastructure protection.	x	x			Seguridad cibernética e infraestructura tecnológica.
Cyber security issues of telecommunication infrastructure.	x	x			Seguridad cibernética para la protección de infraestructura.
Observación	Las investigaciones de los autores permitieron analizar y sintetizar información que contiene el objeto de estudio,				

por ejemplo: evolución de la ciberseguridad, metodología Magerit, ciberseguridad a nivel mundial, entre otros.

1.2.1 Contextualización del problema

El sector financiero del Ecuador está comprendido por: el Banco Central del Ecuador (BCE), las instituciones financieras públicas y privadas, y las demás entidades controladas por la Superintendencia de Bancos (SB) y la Superintendencia de Economía Popular y Solidaria (SEPS), que son los organismos encargados de velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su vigilancia y, en general, controlar que cumplan las normas que rigen su funcionamiento, las actividades financieras que brindan; a través de la supervisión preventiva, permanente, extra situ y visitas de inspección in situ que permitan determinar la situación económica y financiera de las instituciones, evaluar el control y calidad de la gestión de riesgo, y verificar la veracidad de la información que generan. Es por ello que, se destaca el Art.3 de las SEPS, correspondiente al Glosario de Términos, el cual menciona la Seguridad de la Información, como los mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella; y la Tecnología de la información, como el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros [9, 10, 11].

En ese sentido, las entidades financieras son parte del Sector Financiero Popular y Solidario y el Sistema Financiero Nacional conforme a lo establecido en el Art. 163 de la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del sector financiero popular y solidario, y el Art. 1 de la Ley General de Instituciones del Sistema Financiero, siendo reguladas por la SEPS y SB. En el cantón de Ambato existen 141 entidades financieras, de las cuales 14 son de carácter privado, de un total de 911 entidades a nivel nacional, según datos recogidos de [12, 13]. Estas entidades, son las encargadas de desarrollar sus propias metodologías y procedimientos de administración de riesgo operativo, lo cual implica que deben elaborar un manual de riesgo operativo de acuerdo a su estructura, tamaño y

complejidad de sus operaciones, el que contendrá al menos, lo siguiente: 1) Las políticas, procesos y procedimientos para la administración del riesgo operativo; 2) Los roles y responsabilidades de quienes participan en la administración del riesgo operativo; 3) Las metodologías y procedimientos para identificar, medir (cuantificar), priorizar, controlar, mitigar, monitorear y comunicar los riesgos operativos y su nivel de aceptación; 4) Los procedimientos para priorizar y gestionar los eventos de riesgo, entre otros [1]. Para su ejecución es determinante la transferencia e innovación tecnológica (herramientas financieras) mediante la utilización de las Tecnologías de la Información y la Comunicación (TIC) fundamentales dentro del sector financiero ecuatoriano.

Las herramientas financieras hoy en día son el complemento y soporte financiero ya que brindan ventajas en cuanto la disponibilidad y accesibilidad inmediata a la información mediante la utilización del software libre vía web [14]. Además, sirven de soporte financiero mediante la transacción digital debido a que el 75,9% de las entidades financieras usan herramientas de manera exclusiva para la atención financiera [15]. Ahora la realidad es distinta, se considera que la mayoría de los socios usan medios digitales para llevar a cabo las actividades bancarias; en base a esta necesidad, las entidades han tenido que implementar y fortalecer las herramientas que permiten automatizar los servicios. Sin embargo, esto ha incrementado la posibilidad de los ataques informáticos y violaciones de seguridad en las herramientas digitales financieras [16, 17].

Es así que, la problemática que se evidencia, es que la infraestructura tecnológica del sector financiero del cantón Ambato-Ecuador no cuenta con un continuo seguimiento a procesos de seguridad de las herramientas financieras, tales como: correo electrónico, página web y billetera electrónica; lo cual ocasiona riesgos de ciberseguridad en las mismas. Adicionalmente se identifica que no realizan un análisis de cada una de estas herramientas que a futuro pueden causar incidentes informáticos que afectan interna (personal) y externamente (socios) el entorno financiero. Finalmente, el objeto de estudio determinará un procedimiento de gestión para ciberseguridad, que ha criterio de [1] debe ser considerado y abordado con conciencia y visión estratégica.

1.2.2 Fundamentación teórica

1.2.2.1 Procedimiento de gestión

1.2.2.1.1 Concepto de procedimiento

De acuerdo con [18], un procedimiento es una secuencia de pasos o acciones que definen cómo los estándares, políticas, guías y prácticas serán implementados en una determinada situación. Para la [19], un procedimiento es una acción que conlleva una serie de pasos que permiten realizar una tarea o lograr un objetivo. Por tanto, en base a las investigaciones de los autores anteriormente mencionados los procedimientos pueden ser: obligatorios y recomendados. El segundo, representa eficaces prácticas, que son aconsejables, pero no requeridas. De esta manera, si en un procedimiento no se utiliza el término recomendado se asumirá como obligatorio. Mientras que, [20] lo conceptualiza como una serie de etapas o fases que permiten la mejora continua de actividades, funciones, herramientas y áreas para alcanzar una meta.

1.2.2.1.2 Definición de procedimiento de gestión

En base a la investigación de [21], un procedimiento de gestión es un conjunto de fases que permiten controlar los componentes de una infraestructura de manera segura y eficiente. A criterio de, [22] es un proceso específico para delinear las etapas que puede seguir una entidad para la seguridad de un sistema. Según [23], es un método o sistema ordenado para lograr un objetivo. Abundando al respecto, este tipo de procedimiento son pasos a ejecutar con la finalidad de realizar una tarea determinada, considerándose las políticas de seguridad de la entidad, organización, empresa e institución [24].

1.2.2.1.3 Aspectos relacionados con un procedimiento de gestión

Para [24, 25] los aspectos relacionados con un procedimiento de gestión pueden ser:

- Acatamiento de las regulaciones legales que rigen las actividades o funciones de cada sector o tipo de entidad o institución.
- Control del acceso a los servidores y a la información archivada por un sistema informático.
- Identificación y análisis de los incidentes (internos o externos), e informe de solución a cada uno de ellos.
- Implementación y seguimiento a las etapas o fases del procedimiento propio de cada institución.

De acuerdo al estudio realizado por [19, 21] concuerdan que los aspectos relacionados con este tipo de procedimiento se basan en normas generales, tales como:

- Identificar los requerimientos de seguridad de las herramientas o aplicaciones.
- Establecer reglas coherentes sobre el control de acceso y la clasificación de la información de los diversos sistemas y redes.
- Cumplir la legislación (obligaciones y derechos) con respecto a la protección del acceso a la información y servicios.
- Definir controles informáticos considerándose los estándares, normas y marcos legales.
- Informar que la política de seguridad conforme al procedimiento establecido son de aplicación obligatoria para todos los colaboradores de la organización, entidad e institución.

En el estudio de [22] manifiesta que los aspectos relacionados con un procedimiento de gestión especifican las responsabilidades, roles y acciones necesarias para recolectar, analizar, documentar y optimizar la respuesta ante un incidente (externo o interno) de seguridad de la infraestructura tecnológica o información.

1.2.2.1.4 Objetivos, funciones, etapas y entorno a considerar en este tipo de procedimiento

Las investigaciones de [24, 27] destacan los objetivos, funciones, etapas y entorno en un procedimiento de gestión. El detalle a continuación (Tabla 1.2):

Tabla 1.2: Procedimiento de gestión
Fuente: Elaboración propia

Procedimiento de gestión	
Objetivos	• Salvaguardar la confidencialidad de la información y privacidad de los clientes o usuarios. • Cumplir con el marco legal sobre protección de datos. • Minimizar la cantidad de incidentes (internos o externos). • Prevenir interrupciones del servicio a causa de ataques o virus informáticos. • Optimizar la calidad del servicio.

Funciones	Confidencialidad.- se refiere a la capacidad de asegurar que los datos están disponibles solo para aquellas personas autorizadas. Disponibilidad.- se basa en la garantía que tanto la información como el sistema están disponibles para el cliente en todo momento. Integridad.- se refiere a la capacidad de garantizar que la información no ha sido modificada desde la creación sin autorización. No repudio.- se basa en la participación de las partes (emisor y receptor) en una comunicación. Es por ello, que distingue dos tipos de repudio: • En origen.- hace referencia a que la persona que emite el mensaje no puede negar que es el emisor del mismo, puesto que el receptor tendrá pruebas del envió. • En destino.- es lo contrario, ya que el receptor no puede negar que recibió la información (mensaje) debido a que el emisor tiene pruebas de la recepción del mismo.
Etapas	• Análisis de la implementación de medidas básicas de seguridad. • Adaptación a los requisitos de la normativa y de las exigencias del cliente. • Gestión integral de la seguridad cibernética o de la información. • Certificación de la gestión de la seguridad cibernética.
Entorno	Es indispensable examinar el entorno, es decir analizar: • Personas (clientes, usuarios o clientes). • Tecnología (herramientas, aplicaciones, plataformas, otros). • Legislación, normativa o marco legal. • Estructura organizacional u organizativa.

De acuerdo, a la investigación de [26] en un procedimiento de gestión se distinguen las siguientes etapas (Figura 1.1):

Figura 1.1: Etapas procedimiento de gestión

Fuente: [26]

1.2.2.1.5 Importancia de este procedimiento

De acuerdo con, [28, 29] un procedimiento de gestión es importante para: 1) Detectar riesgos, 2) Comprender las consecuencias de los incidentes, 3) Determinar prioridades para el tratamiento de riesgos, 4) Monitorizar y controlar la efectividad del tratamiento, 5) Concienciar y educar a los colaboradores y a la dirección sobre los riesgos y la forma de mitigarlos, entre otros. Mientras que, [26, 30] demuestra la importancia de un procedimiento de gestión a través del impacto de incidentes (Figura 1.2).

Rango impacto / Descripción		Descripción	Pérdidas financieras	Pérdida del activo(s)	Reputación e imagen	Disminución de rendimiento
5	Catastrófico	> 6 % del presupuesto	Total	Mayor que un mes	Alta y muy extendida	> 50 % de variación en los indicadores
4	Desastroso	6% del Presupuesto	Muy gran impacto	De una semana a un mes	Media y muy extendida	25-50 % variación en los indicadores
3	Serio	2% del presupuesto	Gran impacto	De un día a una semana	Media y poco extendida	10-25% variación en los indicadores
2	Menor	1% del presupuesto	Impacto menor	½ día o 1 día	Baja y muy extendida	5-10 % variación enl os indicadores
1	Insignificante	< 0,5 % del presupuesto	Casi sin impacto	Menor de ½ día	Baja y poco extendida	Hasta 5% variación en los indicadores

Figura 1.2: Impacto de incidentes

Fuente: [26, 30]

La Figura 1.2 muestra que el rango del impacto de incidentes va desde insignificante hasta catastrófico. En ese sentido, si en una entidad el incidente es catastrófico, este podría generar un presupuesto mayor al estimado, pérdidas financieras totales, pérdida de los activos en meses, reputación e imagen muy extendida sobre riesgos o incidentes y disminución de rendimiento en más del 50%. Cabe destacar, que los parámetros anteriormente mencionados dependerán del rango del impacto de incidentes.

1.2.2.1.6 Acciones inmersas en un procedimiento de gestión

Según [31, 32], las acciones en un procedimiento de gestión pueden ser: 1) Establecer controles de seguridad, 2) Contratar servicios o instalar herramientas de monitoreo, 3) Considerar métodos de detección temprana, 4) Implantar un plan de contingencia y continuidad, 5) Fomentar la capacitación para tratar incidentes en la infraestructura tecnológica, otros.

Asimismo, [26, 33] concuerdan que las acciones inmersas en este procedimiento deben: impedir el riesgo (eliminándose esa actividad), minimizar el riesgo (a través de medidas o controles), transportar el riesgo (mediante la contratación de un seguro) o aceptar el riesgo (es decir, monitorizarlo para controlar que no se incremente).

1.2.2.1.7 Tipos de procedimiento de gestión

En base a [34] un procedimiento de gestión puede llevarse a cabo mediante el proceso cíclico denominado planificar, hacer, verificar y actuar (PHVA). A continuación, el detalle:

- Planificar.- etapa referente al desempeño de acciones, tales como: 1) Identificar, analizar y evaluar los riegos, 2) Valorar alternativas de tratamiento de riesgos, 3) Considerar una política de seguridad, 4) Determinar el alcance del procedimiento en términos de entidad, localización, tecnologías y activos, entre otros.
- Hacer.- etapa donde se debe tomar decisiones como: 1) Determinar un plan de tratamiento de riesgos, 2) Implementar controles a través de herramientas de monitoreo, 3) Establecer un sistema de métricas de eficiencia y eficacia de los controles, 4) Definir un método de solución ante los incidentes de seguridad, otros.

- Verificar.- etapa que abarca las actividades para la monitorización, entre ellas: 1) Analizar la efectividad del sistema, 2) Renovar los planes de seguridad, 3) Revisar las métricas de riesgo (residual y aceptable), 4) Ejecutar auditorías internas del sistema de seguridad, entre otros.
- Actuar.- etapa indispensable para que los resultados sean favorables, por ello destaca acciones como: 1) Implementar mejoras en el sistema de seguridad, 2) Presentar un informe detallado y preciso del progreso, 3) Velar que las medidas implementadas alcancen los objetivos planteados.

Por otro lado, [35] menciona que un procedimiento de gestión debe ser la parte integral del proceso de negocio de una entidad. Es así que, ilustra el siguiente procedimiento de gestión del riesgo (Figura 1.3):

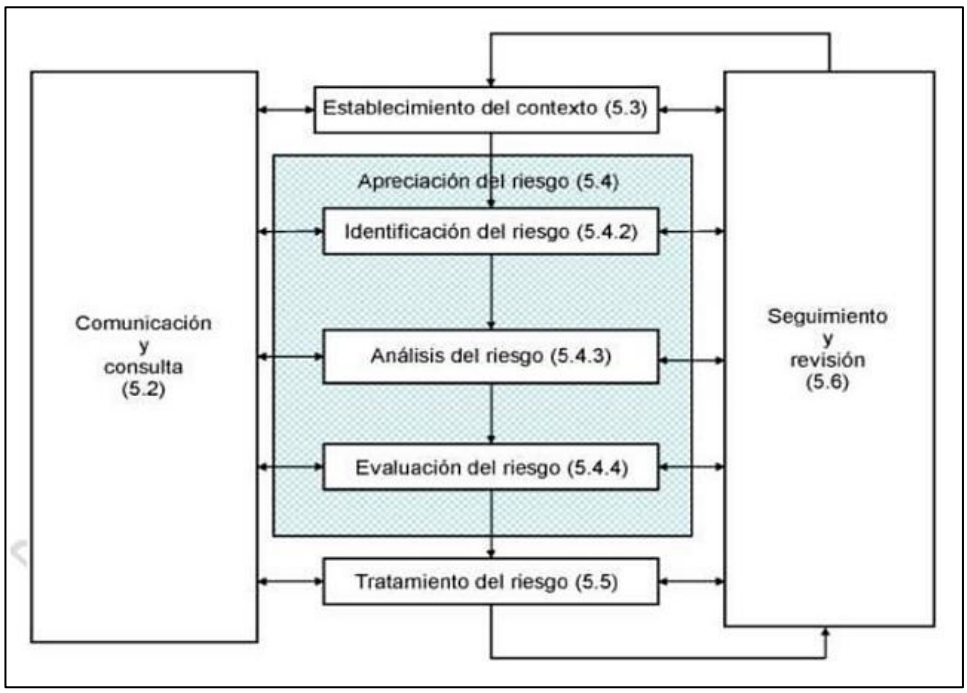


Figura 1.3: Tipo de procedimiento de gestión

Fuente: [35]

De esta manera, la Figura 1.3 abarca siete componentes, los cuales se refieren a: 1) Establecimiento del contexto (determina la responsabilidad, objetivo y visión que tiene la organización respecto al alcance de riesgos de seguridad de la información), 2) Identificación (evalúa la causa y efecto de los incidentes), 3) Análisis (establece el impacto del riesgo), 4) Evaluación (determina qué riesgo es prioridad), 5) Tratamiento del riesgo (ejecuta criterios como: salir, compartir, mitigar o aceptar el riesgo), 6)

Comunicación y consulta (enfocada en la interacción de las partes involucradas en las etapas o fases del proceso), 7) Seguimiento y revisión (orientada a revisar los nuevos riegos o cambios legales).

Ahora bien, la investigación de [36] propone un procedimiento de gestión de riesgos de ciberseguridad dentro de los Institutos Tecnológicos Superiores (ITS). El detalle a continuación (Figura 1.4):

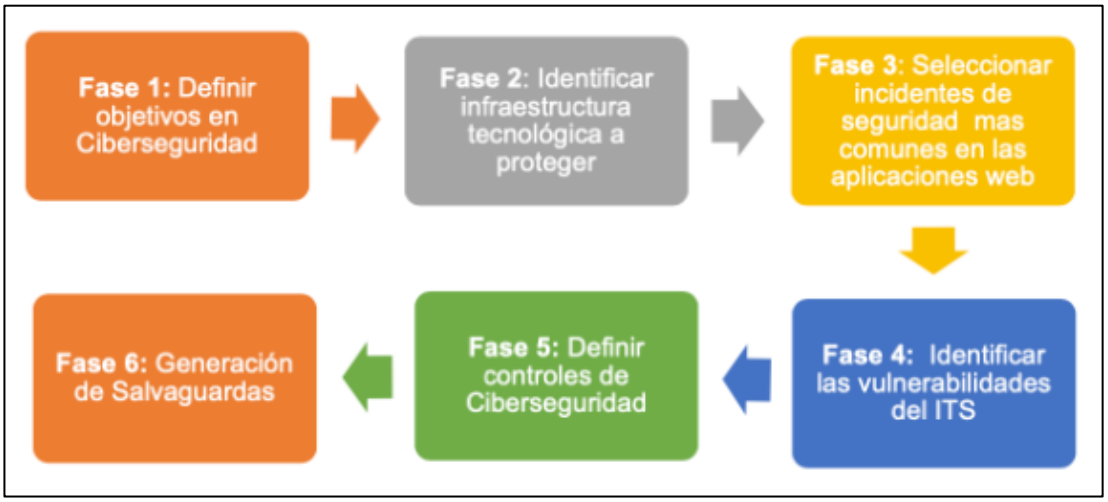


Figura 1.4: Fases del procedimiento de gestión

Fuente: [36]

En este caso, la Figura 1.4 describe las fases del procedimiento de gestión que tratan de: 1) Definir objetivos, con la finalidad de reducir riesgos en las aplicaciones; 2) Identificación infraestructura, como plataformas web, servidores, redes y aplicaciones; 3) Selección de incidentes, de acuerdo al área de afectación; 4) Identificación de vulnerabilidades, mediante el reconocimiento, exploración, enumeración e informes; 5) Definición de controles, a través de las normas ISO con la finalidad de establecer soluciones de seguridad; 6) Salvaguardas, conforme al área de afectación.

1.2.2.1.8 Principales aportes teóricos sobre este procedimiento

En base al aporte investigativo de [22, 26, 37, 38, 39] se detalla los procedimientos de gestión utilizados a nivel mundial. A continuación, el detalle:

Tabla 1.3: Aportes teóricos sobre procedimientos de gestión

Fuente: Elaboración propia

País	Entidad	Tipo			Etapas o fases	Normas ISO			Sector
		I	CC	CI		27001	27000	N	

ES	Incibe		x	Tres			x	Comercial
COL	MINTIC	x		Cinco	x			Tecnológico
COL	CNO		x	Cuatro		x		Electricidad
CHI	SENDA	x		Cinco			x	Social
EC	BCE	x		Cinco			x	Financiero

De esta manera, la Tabla 1.3 detalla los procedimientos de gestión, mismos que corresponden a países como España (ES), Colombia (COL), Chile (CHI) y Ecuador (ECU); seguido de la entidad; el tipo de procedimiento como: Incidentes (I), Critica Cibernética (CC) y Ciberincidentes (CI); las etapas o fases, tales como: objetivos, gestión, proceso, roles, alcance, otros; relación con las Normas ISO, en este caso ISO-27001 y 27000, y Ninguna (N); y finalmente el sector en el que se ha utilizado o implementado para brindar una solución a los riesgos y vulnerabilidades en la infraestructura y sistema de seguridad.

1.2.2.2 Ciberseguridad

1.2.2.2.1 Concepto

El término ciberseguridad también conocido como seguridad informática, seguridad tecnológica, seguridad de la información o seguridad digital ha modernizado el sistema de seguridad de las entidades debido a que ocupa el tratamiento de la información por medio de las computadoras y la integridad del sistema informático [35, 40].

Por tanto, en base a la investigaciones de [41, 44], la ciberseguridad es el conjunto de políticas, herramientas, salvaguardas de seguridad, seguros y tecnologías que pueden utilizarse para proteger la información interna y externamente de una organización. Mientras que, [1, 42, 45] manifiestan que es un proceso que involucra prevención, detección y reacción o respuesta, el cual debe abarcar un elemento de aprendizaje para la mejora continua del propio proceso. Para [43], es un conjunto de diversos programas o herramientas que protegen y proporcionan lineamientos, normas y mejores prácticas para gestionar el riesgo.

1.2.2.2.2 Evolución

La evolución de la ciberseguridad a través del conjunto de políticas, herramientas, directrices, procesos de gestión de seguridad, conceptos de seguridad, métodos de

gestión de riesgos, acciones, prácticas idóneas, seguros y tecnologías ha permitido proteger a los usuarios el ciberentorno y los activos organizacionales [1]. Por otra parte, [42] menciona que la evolución de las TIC en los últimos años ha acelerado el proceso de globalización dando importancia a la ciberseguridad (seguridad en el ciberespacio), considerada actualmente de interés común, puesto a que percibe como mecanismos esenciales el salvaguardar los sistemas informáticos o tecnológicos y primordialmente prevenir los incidentes informáticos o conflagraciones cibernéticas. En ese sentido, a continuación, se detalla la evolución de la ciberseguridad (Tabla 1.4):

Tabla 1.4: Evolución de la ciberseguridad

Fuente: [1, 46, 47, 48]

Año	Suceso
1986	En Estados Unidos se fundó la Computer Fraud and Abuse Act. como reparación a la primera ley federal de fraude informático, para abordar el hacking.
1900s	La industria antivirus respondió con productos como Norton Antivirus, Kaspersky y McAfee que detectaban amenazas en los archivos de un sistema.
1995	Secure Sockets Layer (SSL) se creó para cifrar las comunicaciones entre una computadora y un servidor remoto.
2001	Se aprobó y firmó el Convenio de Budapes, enfatiza la importancia de crear mecanismos de cooperación internacional contra la cibercriminalidad.
2003	En Estados Unidos en el departamento de Seguridad Nacional establece la División Nacional de Seguridad Cibernética, el primer grupo de trabajo oficial dedicado a la seguridad cibernética.
2012	ISO 27032 de Ciberseguridad se publicó para garantizar y velar la seguridad de la información durante los intercambios, para evitar hackeos, sabotajes o alteraciones que puedan ponerla en riesgo.
2014	El Consorcio de Internet Industrial, se centra en la creación de estándares que promueven la interoperabilidad abierta y el desarrollo de arquitecturas comunes.

	Big Data Analytics creado para detectar un sistema infectado y aportar una solución en tiempo real de forma rápida.
2016	SIEM (*Security Information and Event Management* - Gestión de Información y Eventos de Seguridad) sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad.
2019	CSF (Cybersecurity Framework - Marco de ciberseguridad) concebido bajo las premisas de identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica, proporcionando un enfoque flexible y repetible, que permite la priorización de actividades y apunta a obtener un buen rendimiento de la infraestructura, manteniéndose rentable para la empresa, entidad u organización.
2020	Con el teletrabajo, el uso compartido de la información en la nube y el IoT los riegos amplían su alcance, el riesgo ahora está en casa.

1.2.2.2.3 Clasificación y fases

Con respecto, a la clasificación de ciberseguridad, los autores [40] señalan que puede ser activa y pasiva en base a los elementos utilizados en la infraestructura o sistema informático.

- Activa.- medida que se emplea para detectar las amenazas (vulnerabilidades y riesgos), y en caso de la detención desarrollar los mecanismos adecuados para evitar problemas. Entre los ejemplos, de ciberseguridad activa se encuentra el uso de antivirus, *firewall* o cortafuegos (dispositivo de seguridad de red que controla el tráfico que llega o sale de la red), contraseñas o claves de acceso, otros.
- Pasiva.- medida que se utiliza cuando una vez que se produce el fallo o ataque en la seguridad de los sistemas, genere un impacto menor y active mecanismos de recuperación del mismo. Entre los ejemplos, de ciberseguridad pasiva se encuentra las copias de la información o datos del sistema.

Por consiguiente, [40, 49, 50] concuerdan que para mitigar los riesgos es necesario considerar tres fases, tales como:

- Prevención.- medida que permite actuar de manera oportuna e informar lo que puede suceder al sistema.
- Localización.- medida que ayuda a localizar donde radica el problema a través de dos aspectos: 1) Gestión de vulnerabilidades y 2) Monitorización continua del sistema.
- Reacción.- medida que permite brindar una respuesta técnica mediante tres pasos: 1) Actualización del antivirus, 2) Análisis del sistema y cambios de contraseñas, 3) Limpieza a profundidad del sistema para eliminar todo tipo de peligro. Por otra parte, en el caso de robo de datos es indispensable informar a los usuarios afectados y notificar lo ocurrido como una situación de delito informático.

1.2.2.2.4 Tipos de ataques

La investigación de [40], menciona que un ataque inicia desde un ordenador a otro con la finalidad de comprometer la confidencialidad, integridad o disponibilidad de la información almacenada en el sistema. Es por ello, que en base al aporte del autor mencionado se detalla los siguientes tipos de ataques:

- Ransomware.- software malicioso que compromete el sistema, al secuestrar la información y exigir el pago como rescate o liberación del equipo para evitar daños colaterales.
- Escaneo de puertos abiertos.- proceso que analiza los puertos de un ordenador conectado a la red con el propósito de verificar cuales están abiertos, cerrados o disponen de un protocolo de seguridad y en base aquello conocer la composición de la arquitectura, agujeros de seguridad y sistema operativo de la computadora para luego ser explotado por el atacante.
- *Pishing*.- envío de correos falsos que solicitan información respecto a trámites bancarios supliendo la identidad de la institución.
- Robo de *cookies*.- proceso donde el usuario o cliente accede a un enlace y este automáticamente busca las diversas cookies almacenadas en la memoria del ordenador para posteriormente enviar al atacante.

- DoS.- *Denial of Service* traducido como la denegación del servicio, es decir, proceso que inhabilita el uso de una aplicación, sistema u ordenador al alterar o bloquear el funcionamiento.
- Inyección SQL.- ciberataque oculto donde un *hacker* inserta código propio en un sitio o página web con el propósito de transgredir las medidas de seguridad y acceder a la información protegida del sitio y los usuarios.
- *Man-In-The-Middle*.- ciberataque que intercepta la comunicación entre dos partes por medio del uso de una entidad externa o software.
- *Cross-site request*.- falsificación de solicitudes en sitios cruzados que llevan al usuario a realizar un *exploit* malicioso, mediante comandos no autorizados que son transmitidos por el propio usuario que el sitio confía.
- Redes *Wireless*.- acceso a datos sensibles transmitidos mediante la conexión WiFi, los cuales pueden ser manipulados por el atacante.

Ahora bien, [51, 52, 53] manifiestan que en los ataques se distinguen ciberataques y amenazas, entre los más destacados están los siguientes (Tabla 1.5):

Tabla 1.5: Tipos de ataques
Fuente: Elaboración propia a partir de [51]

Ataques		**Nombre / Concepto**	**Funciones afectadas**			
C	A		D	A	I	C
x		Ciberdelito.- delito informático que vulnera los derechos de las personas o terceros.	x	x	x	X
x		Ciberterrorismo.- actividad terrorista realizada en el ciberespacio que puede causar terror a la población.	x		x	
x		Ciberespionaje.- robo de datos o información a organizaciones para acceder a las medidas de seguridad, propiedad intelectual, base de datos de clientes o usuarios, desarrollo tecnológico, otros.	x	x	x	X
x		Ciberguerra.- conflicto bélico que considera el ciberespacio como escenario transcendental.	x		x	

x		Advanced Persistent Threat (APT).- aquellos grupos o individuos que tienen la efectividad, persistencia y capacidad para comprometer la seguridad informática de cualquier empresa u organización.	x		x	
x		Ciberhacktivismo.- individuos o grupos que por alguna ideología intentan debilitar la estructura del oponente.	x	x	x	X
	x	Botnet.- red de sistemas o equipos informáticos que se encuentran bajo el control de un atacante o malware (software malicioso).	x			
	x	*Exploit kits*.- paquetes de software utilizados para automatizar delitos informáticos.	x	x	x	
	x	Gusanos/Troyanos.- programas maliciosos que se duplican y redistribuyen a través de riesgos en los sistemas.		x	x	X
	x	Falsos antivirus.- como *scareware* que busca infectar los ordenadores mediante falsas alertas de seguridad.		x	x	X
	x	Spam.- exceso de correos electrónicos para saturar los buzones del usuario con mensajes no solicitados.		x	x	X
	x	Dirigidos.- ataque que se centra en una empresa o entidad durante un largo periodo de tiempo.	x		x	X
	x	Envenenamiento de Motor de Búsqueda.- se refiere cuando un usuario busca un artículo y está siendo desviado a un contenido malicioso.		x	x	

La Tabla 1.5 describe los tipos de ataques, entre ellos Ciberataques (C) y Amenazas (A), seguido de nombre y concepto, y funciones afectadas como: Disponibilidad (D), Autenticidad (A), Integridad (I) y Confidencialidad (C).

1.2.2.2.5 Importancia de la ciberseguridad

Para [1], la importancia de la ciberseguridad radica en la preservación de los medios humanos, tecnológicos, financieros e informativos adquiridos por las entidades para lograr los objetivos; y en la reducción de las amenazas, limitando las averías resultantes o daños, lográndose reanudar las operaciones tras un incidente informático, en un plazo de tiempo razonable y a un coste admisible. A criterio de [54], esto se recalca como un factor de inversión y una necesidad de fomento de capacitación y formación de los responsables de la seguridad informática.

1.2.2.2.6 Ventajas y desventajas

En base a los aportes de [55, 56, 57, 58, 59], las ventajas que brinda la ciberseguridad son: 1) Mejora de los procesos operativos, 2) Generación de confianza en los clientes, socios y proveedores, 3) Ahorro de gastos imprevistos, 4) Mejora de la imagen corporativa, 5) Capacidad de recuperación, 6) Monitoreo sin límites, entre otros. Mientras que, [43] menciona las desventajas, tales como: 1) Poca compatibilidad con los distintos dispositivos, 2) Saturación de la red por aplicaciones o herramientas pesadas, 3) Necesidad en todo momento de internet, 4) Funcionamiento deficiente del hardware de cifrado digital, entre otros.

1.2.2.2.7 Normas para la ciberseguridad

De acuerdo con, [40, 60] las normas para la ciberseguridad de información que pueden emplearse son:

- Norma ISO 27032.- puesto que permite desarrollar los lineamientos para salvaguardar los activos de la información que están en el ciberespacio.
- Norma ISO/IEC 27032.- ya que garantiza la seguridad en los intercambios de datos o información en la red, al enfrentar el cibercrimen con una cooperación fiable y segura.
- Norma ISO/IEC 27032:2012.- debido a que fortalece el estado de la seguridad cibernética a través de parámetros técnicos y estratégicos relevantes para esta actividad relacionado con la seguridad de internet, información, aplicaciones y red.

1.2.2.2.8 Pasos básicos para establecer la ciberseguridad en una entidad

Las investigaciones de [61, 62, 63] concuerdan en los siguientes pasos básicos para establecer la ciberseguridad en una entidad, organización e institución:

- Analizar la legislación, normativa o marco legal acorde al sector de la entidad.
- Determinar los beneficios y obtener el respaldo de la alta gerencia.
- Definir los objetivos (general y específico) para la ciberseguridad.
- Establecer las directrices o lineamientos para la adecuada implementación de la ciberseguridad.
- Organizar la implementación a través de las respectivas acciones, roles y responsabilidades.
- Evaluar y mitigar los riesgos.
- Establecer las medidas de protección.
- Incentivar la formación, capacitación y concientización sobre ciberseguridad.

1.2.2.2.9 Aportes de prevención en ciberseguridad

Los autores [1], resaltan los aportes de prevención en ciberseguridad. Es por ello, que se presenta el siguiente detalle (Tabla 1.6):

Tabla 1.6: Aportes de prevención en ciberseguridad

Fuente: Elaboración propia

Tipo de ataque	Afectados	Factor relevante	Aporte de prevención
Malware	Equipos	Virus troyano	Disponer de un antivirus a través de IDS, IPS o *firewalls* (dispositivos de seguridad).
Pishing	Usuarios y Entidades	Técnica dirigida al usuario final de una entidad.	Comprobar la barra de navegación mediante el certificado digital https:// y el candado cerrado que refleje el navegador.

Dispositivos a Internet de las cosas (IoT)	Dispositivos	IoT conectados en la actualidad, más de 25 mil millones.	Considerar factores como autentificación robusta, descarga segura, control de acceso físico y actualización de software.
Ransomware	Equipos	Atacante solicita un rescate económico.	Contar con un proceso de respaldo continuo de los datos o información.
Denegación de servicio (DoS)	Equipos	Intenta colapsar los equipos o servicios.	Disponer de sistemas de detección y prevención de intrusiones (IDS e IPS).
Suplantación de identidad (*spoofing attack* y *Sybil*)	Sistemas	Amenaza grave para los sistemas de verificación automática.	Implementar sistemas con rasgos biométricos, como por ejemplo el reconocimiento facial.
Redes LAN inalámbricas	Equipos	70% de sistemas disponen de una red inalámbrica en las infraestructuras.	Adoptar estándares de cifrado avanzado, por ejemplo 802.1x, TKIP (Protocolo de integridad de clave temporal).

1.2.2.2.10 Principales desafíos de ciberseguridad

Para [64], los principales desafíos se centran en la experiencia (lecciones útiles) de los países más avanzados en seguridad cibernética. El detalle a continuación:

- Estonia.- fue el primero en crear una estrategia nacional de ciberseguridad que garantice la prestación de servicios seguros al combatir la ciberdelincuencia y mejorar la capacidad de defensa nacional. En el año 2009, fundó el Consejo de Seguridad Cibernética y el Mapeo de infraestructuras críticas con la finalidad de apoyar la colaboración entre organismos y controlar la ejecución de la estrategia. Actualmente, es el líder en gobernanza y autentificación electrónica o digital a nivel mundial.

- Israel.- destaco mundialmente al reconocer la importancia de salvaguardar los sistemas informáticos críticos mediante la creación del Proyecto de Gobierno Electrónico (Tehila) para mejorar la interacción *online* entre estado y sociedad. Es así que, en 2015 determinó una Autoridad Nacional de Defensa Cibernética con el objetivo de proteger frente a ataques cibernéticos a las entidades públicas y privadas de su entorno. De esta forma, al menos un tercio de las exportaciones están relacionadas con las TIC, lo cual lo convierte en un país que fomenta la cultura digital.
- República de Corea.- anunció un Plan Maestro Nacional de Ciberseguridad con el propósito de responder los ataques cibernéticos. Además, busca incrementar la concientización acerca de la ciberseguridad, identificar alertas de riesgos y compartir adecuadas o mejores prácticas. Por tanto, es uno de los países que promueve la formación de expertos en el área de seguridad cibernética.
- Estados Unidos.- sobresale por el complejo conjunto de políticas, instituciones y normas para gestionar los desafíos de la seguridad cibernética. De esta forma, a través de la Comisión Federal de Comercio (FTC) proporciona a las entidades informes sobre la seguridad de la información. En definitiva, ha sido uno de los países que enfatizó la creación de requisitos de seguridad de datos para el sector financiero mediante la Ley Gramm-Leach-Bliley (GLBA).

1.2.2.2.11 Ciberseguridad en el sector financiero a nivel mundial

A criterio de [65], el reporte de la Organización de Estados Americanos (OEA) sobre ciberseguridad en el sector bancario en América Latina y el Caribe, demuestra que el 85% de las entidades financieras han logrado una seguridad fiable mediante equipos de detección y prevención de intrusiones (IDS e IPS), sin embargo aún no desarrollan directrices en tecnologías como Machine Learning, Inteligencia Artificial y Big Data, la cuales son fundamentales para combatir los nuevos ataques. Por consiguiente, con respecto a la concientización de seguridad cibernética, un 80% conoce sobre incidentes de seguridad, pero únicamente un 20% afirma ser víctima de *pishing* y denegación de servicio (DoS). De modo accesorio, entre un 50% y 68% los marcos referenciales o metodológicos utilizados con frecuencia por este sector son las Normas ISO 27001 y *Control Objectives for Information and Related Technologies* - Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas (COBIT), seguido de

lineamientos como *Payment Card Industry Data Security Standard* - Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS). Ahora bien, en cuanto a usuarios el 53% realiza transferencias bancarias a través de la banca móvil y el 47% acude físicamente a la entidad. De ahí que, el 63% de socios revisan las transacciones y saldos mediante teléfonos inteligentes, respaldados por certificaciones de seguridad digital. En definitiva, el reporte detalla los países con más ciberataques de América Latina de tipo *pishing*, *scareware*, *malware*, denegación de servicio (DoS) y *ransomware*. A continuación, el detalle (Figura 1.5):

País	Porcentaje de Ataques
Colombia	28%
Perú	17%
México	15%
Brasil	11%
Argentina	9%
Chile	1.33%
Ecuador	1.33%
Venezuela	1.33%
Resto de América Latina	6%

Figura 1.5: Países con más ciberataques de América Latina

Fuente: [65]

Seguidamente, la autora [66] detalla que el 73% de las empresas del sector financiero utilizan equipos de red vulnerable, tal es el caso de Estados Unidos (EEUU) y México como los países con mayor ataque cibernético bancario. Por añadidura, Android es una de las plataformas que recibe ataques del 99,78% del *malware* móvil. Finalmente, este estudio concuerda con el reporte anteriormente detallado, al mencionar que Ecuador se encuentra en el puesto siete que más ciberataques sufre anualmente encabezados por *hackers* desde Francia, Italia, Alemania, Rusia, Corea, China, Argentina, Sudáfrica y EEUU.

1.2.2.3 Infraestructura Tecnológica

1.2.2.3.1 Concepto

El avance de las TIC ha ocasionado que las entidades estén cada vez más actualizados y a la vanguardia. Por tanto, una infraestructura tecnológica o plataforma son los sistemas (equipos de almacenamiento, ordenadores, equipos de red, otros) junto con la forma de gestión (procesos, herramientas, programas, mediciones de rendimiento, entre otros) [67, 70]. Según [68], es el conjunto de software y hardware que permite realizar una actividad. Mientras que, [69, 71] señala que es el conjunto de elementos que hacen posible el funcionamiento de la actividad tecnológica de una entidad, empresa u organización.

1.2.2.3.2 Importancia

En efecto, la importancia de una infraestructura tecnológica es estratégica debido a que potenciará o limitará el desarrollo de una organización, entidad o empresa [72, 73]. A criterio de, [1, 74, 75] esto radica en los beneficios de este tipo de infraestructura, tales como: 1) Alojar una mayor cantidad de datos, 2) Mejor la capacidad de respuesta, 3) Disminuir los riesgos de fallas, 4) Elevar la competitividad empresarial, otros.

1.2.2.3.3 Responsabilidades en la infraestructura tecnológica

La investigación de [76] describe las responsabilidades (Tecnología de la Información -TI y usuarios) en la infraestructura tecnológica (software y hardware). El detalle a continuación (Tabla 1.7):

Tabla 1.7: Responsabilidades en la infraestructura tecnológica

Fuente: Elaboración propia

Infraestructura tecnológica	Entorno	Responsabilidades
Software	Área TI	• Elaborar un inventario de programas instalados en la empresa, entidad o institución. • Vigilar que los programas estén instalados bajo licencia. • Preservar el almacenamiento y custodia de los programas informáticos.

		• Definir discos de red para fragmentar el acceso a los datos y mejorar la organización. • Determinar configuraciones automatizadas para que los usuarios archiven la información en la red, y con ello proporcionar las respectivas copias de seguridad (*backup*). • Restringir el ingreso a los equipos fuera de jornada, a los usuarios que no dispongan de una autorización previa del superior de la entidad.
	Usuario	• Evitar la instalación de programas que no tienen relación con la entidad. • Prevenir que en el disco de red no se archive datos ajenos a la actividad de la institución. • Evitar la desinstalación de antivirus del equipo. • Comunicar al área TI los problemas de virus en el equipo informático. • Notificar al área TI el informe del inmediato superior sobre la autorización para laborar fuera de horario de trabajo.
Hardware	Área TI	• Custodiar todos los activos informáticos de la entidad. • Asignar los equipos a los usuarios, conforme con los requisitos de área. • Verificar que un mismo activo informático no sea asignado a más de un usuario. • Establecer un control de los equipos asignados al personal que realiza tareas fuera de la entidad.
	Usuario	• Salvaguardar los equipos informáticos (USB, monitores, teclados, parlantes, impresoras, PC´s, otros) asignados por la entidad. • Comunicar vía telefónica o digital los problemas presentados con los equipos informáticos.

1.2.2.3.4 Infraestructura tecnológica del sector financiero

En base a las investigaciones de [77, 79, 83, 84] la infraestructura tecnológica del sector financiero puede basarse en herramientas digitales como:

- Correo electrónico.- denominado e-mail o mail (correo), es un medio o herramienta que permite la instantaneidad de comunicación (envió-recepción de mensajes) entre uno o más usuarios en una red de datos (Red de Información). Por tanto, [78] destaca las características relevantes del e-mail, tales como: digital (datos en tiempo real), informático (entrega y recepción electrónica), asíncrono (comunicación bidireccional), electrónico (uso de medios digitales de gestión) y ubicuo (acceso en diversos lugares). Asimismo, ventajas como: 1) Rapidez y eficiencia, 2) Reducción de costos, 3) Simplificación de procesos dentro y fuera de la entidad, entre otras.
- Página o sitio web.- es una información o documento electrónico que abarca elementos multimedia (video, imágenes, texto, otros) y enlaces de hipertexto a través de la *World Wide Web* (WWW o Web). Para [80], un sitio web tiene la finalidad de: 1) Atraer nuevos socios, 2) Mejorar el servicio, 3) Promover la comunicación entre empresa-cliente, 4) Desarrollar mercados, otros. Según, el estudio de [81] esto fue creado por científicos interesados en trabajar en equipo, superándose las incompatibilidades entre diversos ordenadores y sistemas operativos.
- Billetera electrónica.- conocida como billetera móvil o billetera digital, es una aplicación web, móvil u omnicanal que permite a los usuarios almacenar datos para distintas formas de pago y programas seguros con la finalidad de enviar y recibir dinero de persona a persona (*peer to peer – P2P*), pagar facturas, realizar compras *online*, transferencias bancarias, otros; puesto que la identidad del usuario está protegida mediante cifrado, tokenización, *Know Your Customer* - Conoce a tu cliente (eKYC o KYC) y adicionales métodos de autorización y autenticación (biometría, *One-Time Password* – Contraseña de un solo uso (OTP), clave o PIN, entre otros). Por tanto, [82] menciona que las transacciones pueden realizarse en distintas direcciones, por ejemplo: persona a negocio (P2B), empresa a empresa (B2B), empresa a persona (B2P), gobierno a persona (G2P), gobierno a empresa (G2B), entre otros. De esta forma, refleja

la importancia de este tipo de herramienta digital a nivel general en un mundo tan cambiante.

Ahora bien, el autor [65] manifiesta los instrumentos, sistemas y asistentes utilizados con frecuencia en la infraestructura tecnológica del sector financiero. A continuación, el detalle:

- Chatbots Transaccionales.- es un asistente de servicio al cliente apoyado en la Inteligencia Artificial (IA) que permite realizar transacciones a través del movimiento de la información de un sistema a otro [85].
- Consultas IVR.- es un sistema transaccional (*Interactive Voice Respond* - Respuesta de Voz Interactiva) que permite ejecutar consultas a las cuentas de los socios de manera indirecta [86].
- Botones de pago.- es un sistema de pago *online* integrado a la aplicación móvil o sitio web para que las empresas o individuos cobren por sus bienes o servicios de forma virtual [87].
- Tarjetas de débito - crédito.- es un instrumento financiero que permite operar (consultar saldos, consultar cupos, depósitos, pago de servicios, otros) con una entidad bancaria mediante cajeros automáticos o datafast (dispositivo de cobro) [88].

1.2.2.3.5 Ventajas de la infraestructura tecnológica en el sector financiero

A criterio de, [89] las ventajas de una adecuada infraestructura tecnológica en el sector financiero pueden ser: 1) Fomentar activos rentables, 2) Automatizar y simplificar los procesos transaccionales, 3) Elevar la competitividad empresarial, 4) Reducir costes, 5) Optimizar el servicio al cliente, entre otras.

1.2.2.4 Sector financiero segmento 1 regulado por la SEPS

1.2.2.4.1 Norma de Control para la Administración del Riesgo

De acuerdo con, la Norma de Control para la Administración del Riesgo Operativo y Riesgo Legal en las Entidades del Sector Financiero bajo el control de la SEPS, el Art. 3.- Glosario de términos, define lo siguiente:

"Procedimiento, es el método específico y estandarizado para llevar a cabo una actividad o proceso" [9].

Riesgo operativo, es la probabilidad de que se produzcan pérdidas para la entidad, debido a fallas o insuficiencias originadas en proceso, personas, tecnología de información y eventos externos. El riesgo operativo no incluye los originados por el entorno político, económico y social, los riesgos sistémico, estratégico y de reputación [9].

"Seguridad de la información, son los mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella" [9].

"Tecnología de la información, es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros" [9].

1.2.2.4.2 Segmentación SEPS

De acuerdo con, la Norma para la Segmentación de las Entidades del Sector Financiero bajo el control de la SEPS, el Art.1, menciona que las entidades del sector financiero acorde al tipo y saldo de sus activos se ubicarán en los siguientes segmentos (Figura 1.6):

Segmento	***Activos (USD)***
1	*Mayor a 80'000.000,00*
2	*Mayor a 20'000.000,00 hasta 80'000.000,00*
3	*Mayor a 5'000.000,00 hasta 20'000.000,00*
4	*Mayor a 1'000.000,00 hasta 5'000.000,00*
5	*Hasta 1'000.000,00*
	Cajas de Ahorro, bancos comunales y cajas comunales

Figura 1.6: Segmentación sector financiero

Fuente: [90]

Por consiguiente, el Art. 2, detalla que "Las entidades de los segmentos 3, 4 y 5 definidas en el artículo anterior se segmentarán adicionalmente al vínculo con sus territorios. Se entenderá que las entidades referidas tienen vínculo territorial cuando coloquen al menos el 50% de los recursos en los territorios donde estos fueron captados" [90].

Asimismo, el Art. 447 del Código Orgánico Monetario y Financiero indica que "Las cooperativas se ubicarán en los segmentos que la Junta determine" [9] [90], en base al Art.1 de la norma anteriormente mencionada.

1.2.2.4.3 Sector financiero

El sector financiero es parte del Sector Financiero Popular y Solidario (SFPS), y el Sistema Financiero Nacional (SFN) conforme a lo establecido en el Art. 163 de la Norma de Control para la Administración del Riesgo Operativo y Riesgo Legal en las Entidades del Sector Financiero Popular y Solidario, y el Art. 1 de la Ley General de Instituciones del Sistema Financiero [9]. Por tanto, el Cap.1 de la Ley de Instituciones Financieras, detalla que el sector financiero "Es la columna vertebral de la economía del país, la base fundamental para la realización de todas las transacciones económicas, tanto a nivel nacional como internacional y el creador del dinero regulando todas las transacciones personales, empresariales y del Estado". De esta manera, según el Art. 12, "Las entidades del sector financiero ecuatoriano, previa autorización de la Superintendencia, podrán participar en el capital de instituciones financieras del exterior, constituidas o por constituirse, y abrir oficina fuera del país, con sujeción a los procedimientos determinados en la Ley y a las normas que expida la Superintendencia" [91].

En base a [92, 93, 94], las funciones del sector financiero en el Ecuador son: 1) Receptar depósitos, 2) Emitir retiros, 3) Brindar préstamos, 4) Emitir tarjetas de pago, 5) Realizar inversiones y transacciones de divisas, 6) Emitir cuentas con obligaciones, 7) Realizar transferencias de cobros, 8) Negociar títulos valores y descontar letras documentarias sobre el exterior o hacer adelantos sobre ellas, 9) Efectuar por cuenta propia o de terceros operaciones con divisas, contratar reportos y arbitrajes sobre éstas y emitir o negociar cheques de viajeros, 10) Comprar o vender minerales preciosos

acuñados o en barra, 11) Garantizar la colocación de acciones y obligaciones, entre otros, lo cual ha generado un crecimiento sostenido a nivel económico-social

1.3 Objetivos

1.3.1 Objetivo General

Determinar un procedimiento de gestión para ciberseguridad según el análisis de las herramientas de monitoreo de red.

1.3.2 Objetivos Específicos

- Elaborar el marco conceptual sobre ciberseguridad en la infraestructura tecnológica del sector financiero segmento 1 regulado por la SEPS.
- Identificar en tiempo real la actividad maliciosa a través de herramientas de monitoreo y análisis de red.
- Establecer las fases para la gestión de riesgos de ciberseguridad caso de estudio: Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda.

CAPITULO II.-

METODOLOGÍA

2.1 Materiales

2.1.1 Humanos

- Docente Tutor de la Universidad Técnica de Ambato.
- Investigador.
- Asistente TI sector financiero (cooperativa).

2.1.2 Espaciales

- Libros, revistas, artículos y estudios especializados.
- Acceso a Internet.
- Repositorio virtual de la Universidad Técnica de Ambato.

2.1.3 Otros

- Acceso a Internet.
- Servidores.
- Herramientas financieras (correo, página web y billetera electrónica).
- Computadora.
- Dispositivo de almacenamiento (USB).

2.1.4 Económicos

Tabla 2.1: Materiales económicos (presupuesto)

Fuente: Elaboración propia

Nº	DETALLE	UNIDAD	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
1	Servicio de Internet	Pago mensual	2	$ 25,00	$ 50,00
2	Herramientas financieras	c/u	3	$300,00	$ 900,00
3	Servidores	c/u	1	$ 1.800,00	$ 1.800,00

4	Computadora	c/u	1	$ 750,00	$ 750,00
5	Almacenamiento	c/u	1	$ 18,00	$ 18,00
		Subtotal			$ 3.518,00
		Imprevistos (10%):			$ 351,80
		Total:			$ 3.869,00

La Tabla 1.8 detalla el presupuesto (materiales económicos) para el presente proyecto de investigación, mismo que será financiado en su totalidad por el investigador.

2.2 Métodos

2.2.1 Modalidad de la Investigación

El proyecto de investigación se basará en las siguientes modalidades:

Investigación bibliográfica: debido a que el estudio se sustenta en elementos teóricos de libros, artículos científicos, revistas y estudios especializados en idioma inglés y español indizados en las bases de datos Journal of Cyber Security Technology, Science Direct, Scopus, Springer, Espacios y ProQuest; a través del método análisis-síntesis que permite llegar a las conclusiones.

Investigación explicativa: debido a que los resultados obtenidos permiten establecer un procedimiento de gestión para la ciberseguridad en la infraestructura tecnológica del sector financiero, considerándose las investigaciones de [34, 35, 36, 97, 98], las cuales detallan etapas, componentes o fases, mismas que se analiza y sintetizan en el objeto de estudio.

2.2.2 Recolección de Información

Para esta etapa se considera un enfoque básico basado en la Metodología MAGERIT V3.0 mencionada en el estudio de [95], la cual permite identificar en tiempo real la actividad maliciosa (situación actual de riesgos) a través de herramientas de monitoreo y análisis de red [96], caso de estudio: Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda. (CCCA) (Anexo 1). De esta manera, se llevará a cabo el último objetivo de la investigación con la finalidad de proteger los sistemas en su integridad, disponibilidad y confiabilidad.

2.2.3 Procesamiento y Análisis de Datos

En este caso, los datos (resultados) serán procesados y analizados mediante las herramientas de monitoreo y análisis de red que actualmente son utilizadas en el caso de estudio y en investigaciones o estudios relacionados con el tema. Por tanto, a continuación se define las herramientas acorde al sector financiero (Tabla 2.2):

Tabla 2.2: Herramientas de monitoreo y análisis de red

Fuente: Elaboración propia

Herramienta Monitoreo	**Relación con herramientas financieras**			**Tipo de herramientas financieras**			**Autor**	**Descripción**
	Alta	Media	Baja	Página Web	Correo	Billetera Electrónica		
LibreNMS		x		x	x		[99]	Es un sistema de monitoreo de red basado en *Simple Network Management Protocol* - Protocolo Simple de Administración de Red (SNMP) que genera alertas sobre problemas vía *Internet Relay Chat* - Charla Interactiva de Internet (IRC), Slack (aplicación de mensajería), email y otros servicios.
NetCrunch		x			x		[100]	O AdRem NetCrunch, es un software creado por la compañía AdRem Software, Inc. que permite monitorear la red multiplataforma sin agentes y gestionar los sistemas como: *switches*, *routers*, servidores, entre otros.
OpManager		x		x			[101]	Es un software de monitoreo de red integral que da seguimiento a los recursos críticos de TI,

						tales como: firewalls, servidores, controladores de dominio, enlaces WAN, *routers*, *switches*, otros.
OpenNMS		x			x	[102]	Es un producto de *Open Source* (código abierto) que crea soluciones de monitoreo de red, realiza tareas de administración de redes y controla el tráfico generado por la red para manipularlo de una forma sencilla, cómoda y eficaz.
PRTG	x		x	x	x	[103]	O PRTG Network Monitor, es un software de monitoreo de red que permite vigilar y clasificar las actividades, las condiciones de un sistema, y recopilar en tiempo real estadísticas o datos de diversos *hosts* (equipos) como enrutadores, conmutadores, servidores, aplicaciones, dispositivos, entre otros.
PandoraFMS		x		x		[104]	Es un software de monitoreo de gestión de servidores, comunicaciones y aplicaciones que genera alertas en base a los datos obtenidos y muestra gráficos e informes del entorno.

Wireshark	x		x	x	x	[105]	Conocido anteriormente como Ethereal es un analizador de paquetes de red que permite identificar en tiempo real actividad maliciosa.

CAPITULO III.-

RESULTADOS Y DISCUSIÓN

3.1 Análisis

En base a la tabla anteriormente mencionada (Tabla 2.2), es indispensable destacar que se ha seleccionado dos herramientas de monitoreo y análisis de red (aquellas que tienen una alta relación y abarcan diversos tipos de herramientas financieras, acorde al caso de estudio) para llevar a cabo este capítulo. En ese contexto, a continuación se presenta el análisis de los resultados mediante las herramientas PRTG y Wireshark:

3.1.1 PRTG

Es un software de monitoreo de red que permite vigilar y clasificar las condiciones de un sistema. Por tanto, al realizar el monitoreo de red mediante PRTG se recopiló en primera estancia información de la infraestructura de red TI del caso de estudio, lo cual permitió determinar los recursos, identificar rupturas, prever los servicios y redes. De esta forma, a continuación se detalla los resultados obtenidos (Véase Figuras y Tablas):

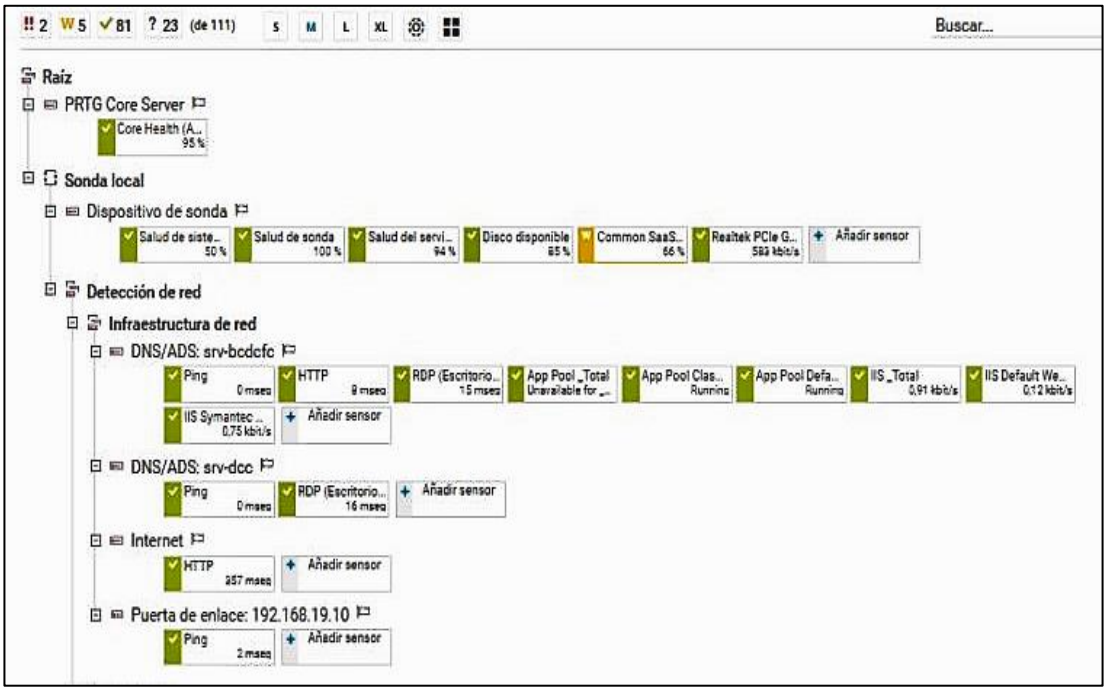


Figura 3.1: Infraestructura de red TI

Fuente: [106]

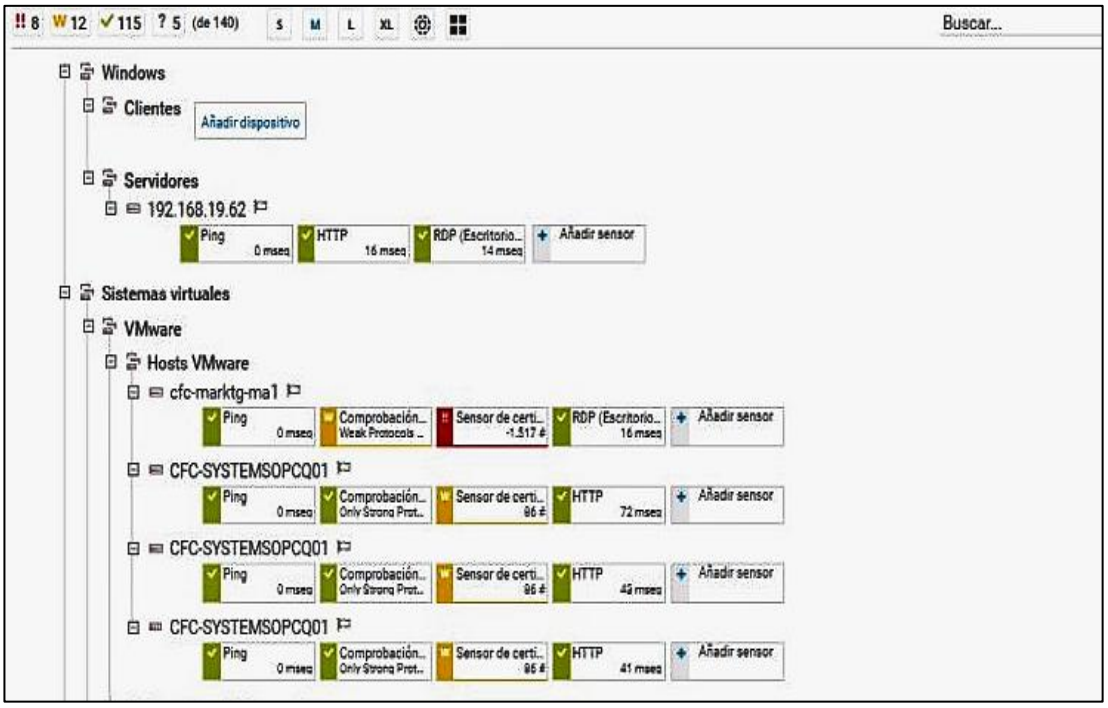


Figura 3.2: Infraestructura de red TI – Servidores y Sistemas virtuales

Fuente: [106]

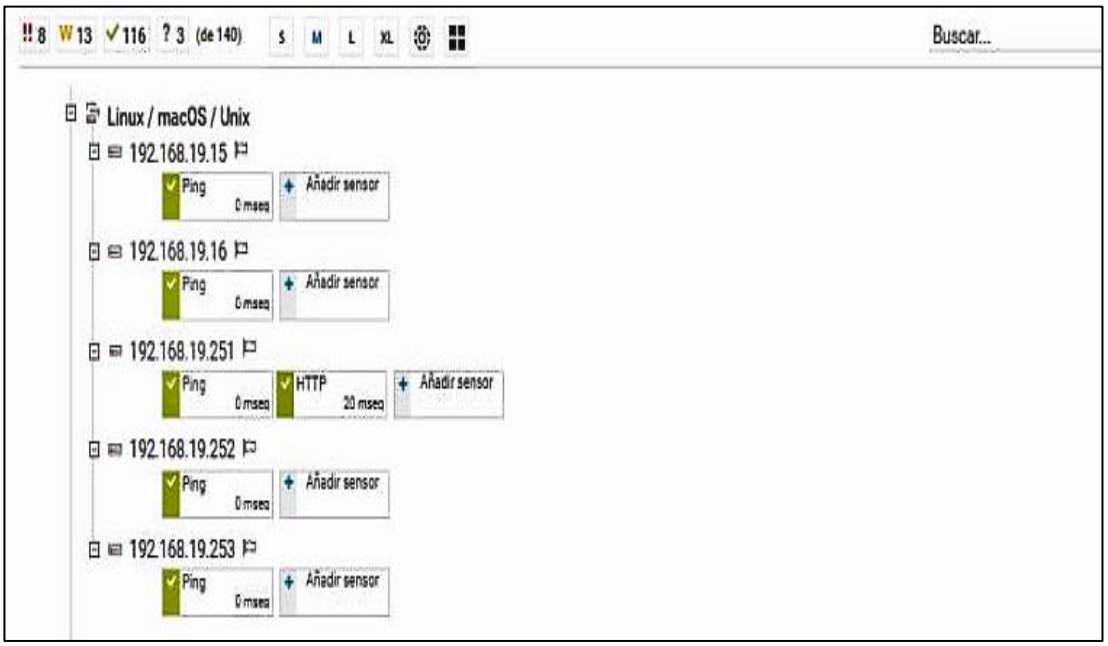


Figura 3.3: Infraestructura de red TI – Sistemas operativos Linux/Mac Os/ Unix

Fuente: [106]

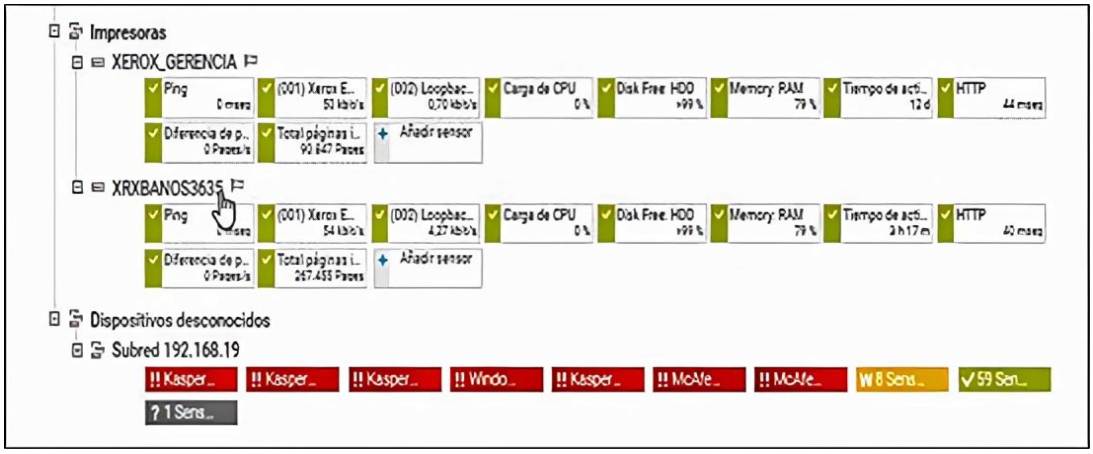


Figura 3.4: Infraestructura de red TI – Impresoras y dispositivos desconocidos

Fuente: [106]

De acuerdo con las figuras, la herramienta PRTG muestra la infraestructura de red por grupos de dispositivos que se agregan automática o manualmente en base al dominio del caso de estudio **coaccca.local** (por seguridad empresarial se evita la visualización del dominio). A continuación, el detalle (Tabla 3.1):

Tabla 3.1: Explicación Infraestructura de red TI del caso de estudio

Fuente: Elaboración propia

Explicación	**Dispositivos**		
	Grupo	**Subgrupo**	**Descripción**
Figura 3.1	Raíz	PRTG Core Server	Dispositivo servidor central de PRTG.
	Sonda local	Dispositivo de sonda	Dispositivo que almacena la información.
	Detección de red	Infraestructura de Red: - DNS/ADS srv-bcdcfc - DNS/ADS srv-dcc - Internet - Puerta de Enlace	Dispositivos que conforman o pertenecen a la red.
Figura 3.2	Windows	Clientes Servidores	Dispositivos que participan

			directamente en la red.
	Sistemas Virtuales	VMware: - Hosts VMware - Servidores VMware vCenter	Dispositivos basados en virtualización.
Figura 3.3	Sistemas operativos	Linux/macOS/Unix	Dispositivos que trabajan con estos sistemas operativos multitarea.
Figura 3.4	Impresoras	XEROX	Dispositivos que están conectados a través de una IP estática.
	Dispositivos desconocidos	Subred 192.168.19	Programas que se encuentran instalados en dispositivos dentro del rango 192.168.19 como antivirus Kaspersky y McAfee.

Seguidamente, en base a la infraestructura de red, la herramienta genera un reporte de alertas o métricas inusuales que se observan en el sistema o correo electrónico, lo cual permite estar alerta ante cualquier inconveniente. Según el análisis del caso de estudio la Figura 3.5 detalla lo siguiente (Tabla 3.2):

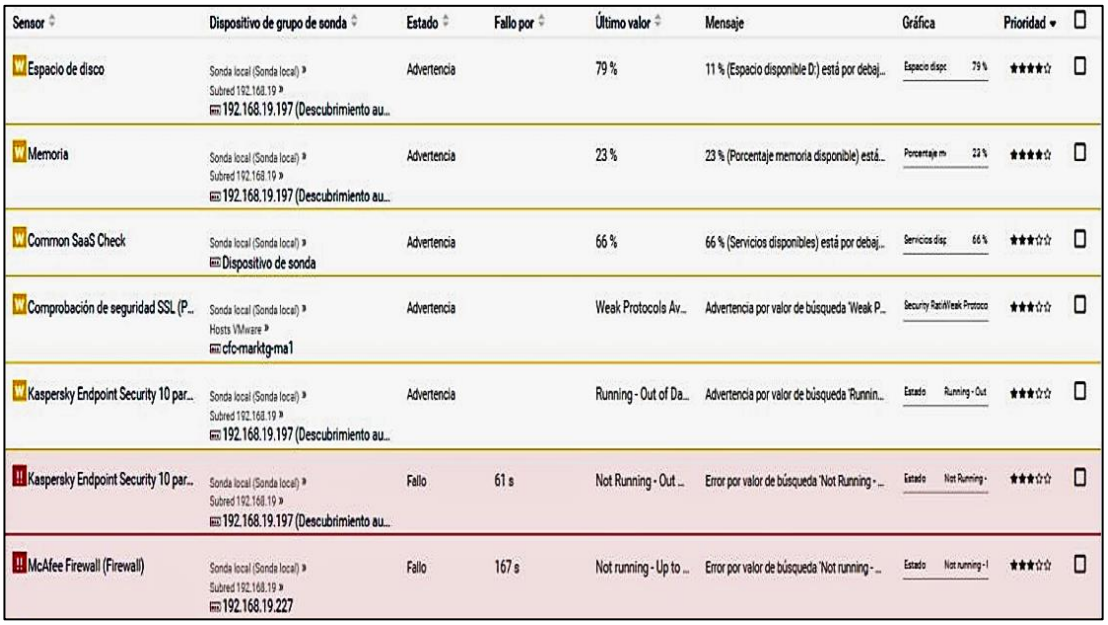


Figura 3.5: Sensores de alerta o advertencia en espacio de disco, memoria, comprobación de seguridad SSL y antivirus

Fuente: [106]

Tabla 3.2: Explicación Sensores de alerta o advertencia del caso de estudio

Fuente: Elaboración propia

Explicación	**Alertas**		
	Tipo	**Identificación por color**	**Descripción**
Figura 3.5	Media		Refleja un estado de advertencia en el: - Dispositivo de la subred 192.168.19 que tiene el 11% de espacio de disco D: - Dispositivo de la subred 192.168.19 que tiene un 23% de memoria disponible. - Dispositivo de la subred 192.168.19 que indica una conexión de sitio web no asegurada mediante un

			Certificado *Secure Sockets Layer* - Capa de Sockets Seguros (SSL).
	Alta		Refleja un estado de fallo en los: - Dispositivos de la subred 192.168.19 donde los antivirus Kaspersky 10 y McAfee están caducados, convirtiéndose en una advertencia crítica.

Al mismo tiempo, la Figura 3.6 refleja advertencias, el detalle a continuación (Tabla 3.3):

Figura 3.6: Sensores de alerta o advertencia en AntiSpyware

Fuente: [106]

Tabla 3.3: Explicación Sensores de advertencia del caso de estudio

Fuente: Elaboración propia

Explicación	**Alertas**	
	Tipo	**Identificación por color**	**Descripción**

Figura 3.6	Media		Refleja un estado de advertencia en el: - Dispositivo de la subred 192.168.19 que presenta una deshabilitación de Windows Defender.

Por último, la herramienta PRTG dispone de sensores, uno de ellos el Sensor Ping que refleja una petición de eco del *Internet Control Message Protocol* - Protocolo de Mensaje de Control de Internet (ICMP) desde el sistema de sonda al dispositivo central para monitorear la disponibilidad. A continuación, el detalle (Figura 3.7):

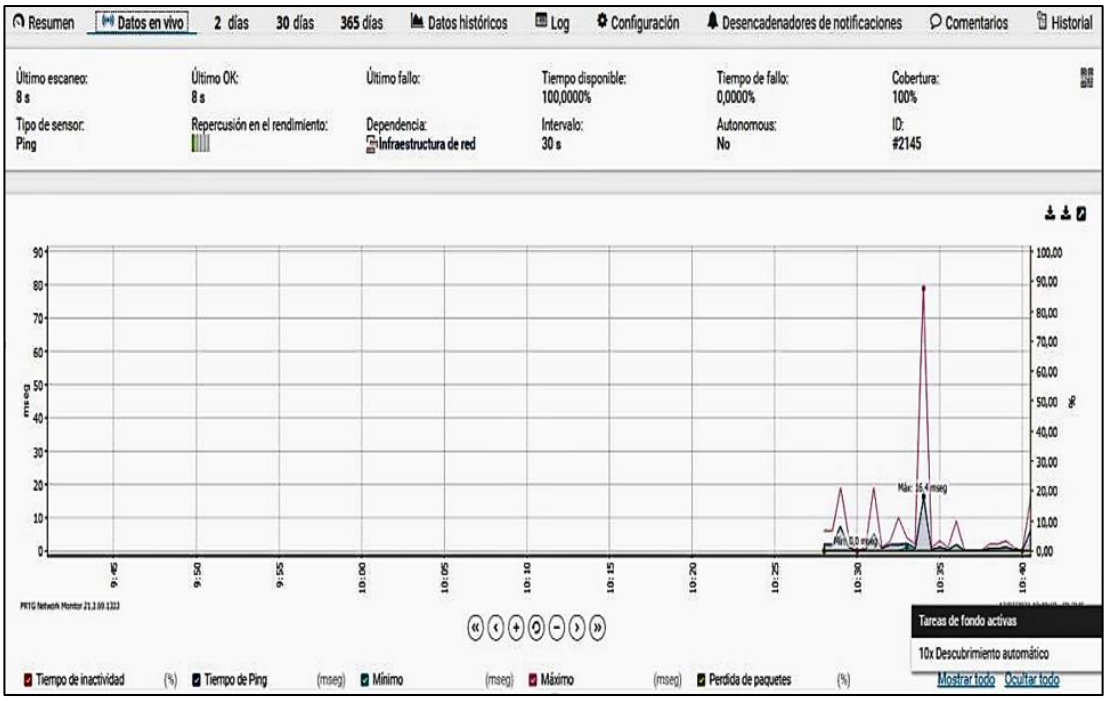


Figura 3.7: Sensor Ping herramienta PRTG

Fuente: [106]

Como se observa, la Figura 3.7 refleja el Tiempo de inactividad, el Tiempo de Ping y la Pérdida de paquetes calculados en milisegundos (mseg), lo cual demuestra que el tiempo de disponibilidad del dispositivo del caso de estudio (CCCA) varía entre los 6 y 16,4 milisegundos, sin pérdida de paquetes.

3.1.2 Wireshark

Es un analizador de paquetes de red que permite identificar en tiempo real actividad maliciosa. De esta forma, la herramienta Wireshark permitió capturar paquetes a través de protocolos de red sin o con filtro con el propósito de presentar un reporte exacto de la actividad maliciosa según caso de estudio. El detalle a continuación (Véase Figuras y Tablas):

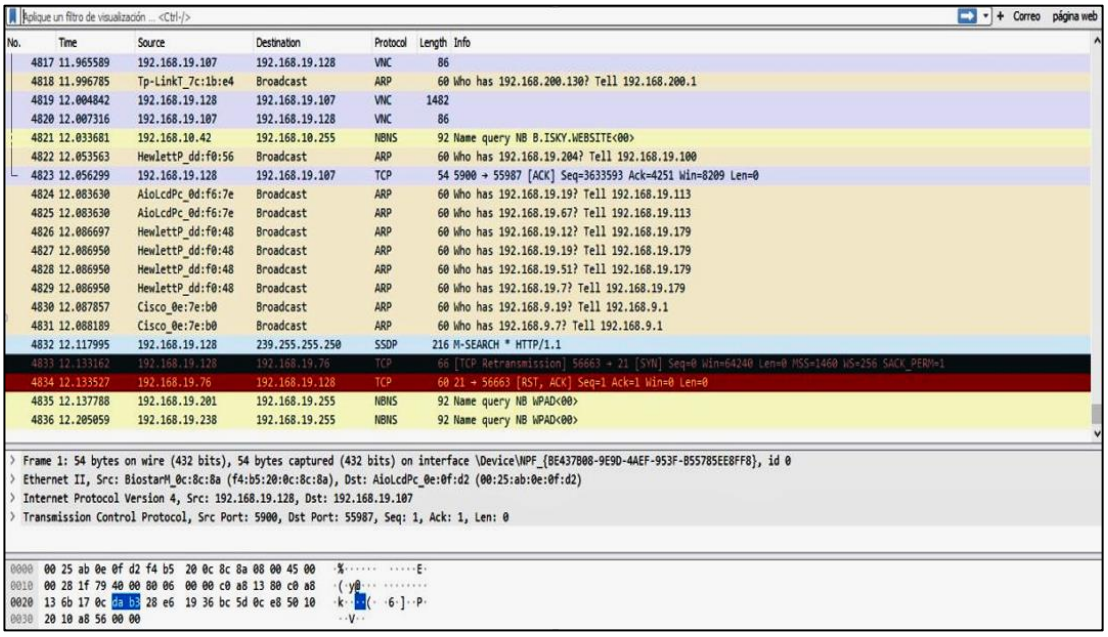


Figura 3.8: Paquete sin filtro a través de protocolos de red según caso de estudio

Fuente: [107]

Tabla 3.4: Explicación Paquete sin filtro

Fuente: Elaboración propia

Explicación	Figura 3.8
	Estructura
Sección 1	Define el tipo de filtro para visualizar el paquete.
Sección 2	Refleja los paquetes capturados en tiempo real.
Sección 3	Separa por capas las cabeceras de los paquetes.
Sección 4	Muestra en estado puro los paquetes en formato hexadecimal.
Columna	**Descripción**
Número (Nº)	Número de paquete que se despliega en la lista.

Tiempo (*Time*)	Calculo en segundos de la captura del paquete.
Origen (*Source*)	Dirección IP y MAC donde surgió el paquete.
Destino (*Destination*)	Dirección a la que se envía el paquete.
Protocolo (*Protocol*)	Tipo de protocolo de red al que hace referencia el paquete (TCP, UDP, SNMP, ARP, entre otros).
Longitud (*Length*)	Longitud en bytes del paquete.
Información - *Information* (Info)	Detalle del paquete.

De acuerdo, con la Figura 3.8 se presenta las Reglas por Default (coloreado) de la herramienta Wireshark (Figura 3.9):

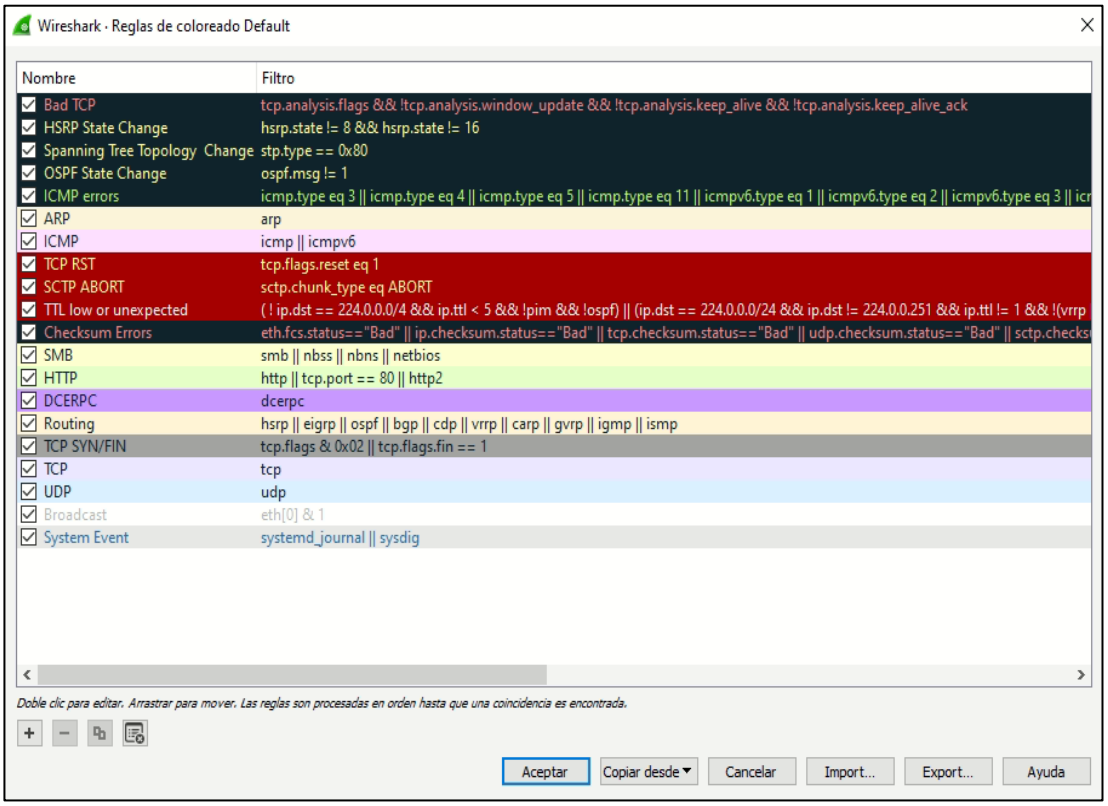


Figura 3.9: Wireshark – Reglas por Default (coloreado)

Fuente: [107]

En base aquello, a continuación se detalla los paquetes capturados sin filtro a través de protocolos de red según el caso de estudio (Tabla 3.5):

Tabla 3.5: Explicación Paquetes sin filtro

Fuente: Elaboración propia

Paquetes sin filtro	
Protocolo	**Información**
ARP	El host con la dirección IP 192.168.19 envía datos pero no conoce la dirección MAC, por lo que envía una solicitud de Protocolo de Resolución de Direcciones (ARP) para averiguar esa información, es decir que 60 es el número de bytes que comprenden este paquete ARP. Dado que 60 es menor que el número mínimo de bytes para una trama de Ethernet, por ende significa que está capturando en la misma máquina que envió la solicitud ARP.
SSDP	Determina el tráfico normal de los dispositivos habilitados para el Protocolo de Comunicación Universal Plug and Play (UPnP) en la Lan a través del protocolo de Descubrimiento de Servicio Simple (SSDP).
VNC	Establece conexiones remotas a interfaces gráficas de usuario.
TCP	El cliente envía una solicitud al servidor el cual responde con datos, pero el cliente no recibe la respuesta por lo que vuelve a retransmitir la solicitud. Determina una conexión al servidor, pero este no acepta una conexión entrante. El cliente inicia la conexión con el Protocolo de Control de Transmisión (TCP) en el primer paquete, enviando un bit de control (SYN), donde el servidor devuelve un paquete marcado Reset (RST, ACK, esto quiere decir que el servidor no tiene la aplicación escuchando en el puerto 56663 o puede haber otro dispositivo que está filtrando el tráfico y reacciona con Restablecer a las conexiones en el puerto 56663.
NBNS	Solicita a través del Protocolo de Autodescubrimiento de Proxy Web (WPAD) a un navegador encontrar un proxy local.

Ahora bien, Wireshark permitió analizar el correo electrónico que se visualiza como una herramienta financiera vulnerable a pasquines o ataques maliciosos a través del

filtro **frame contains "dominio"**, el cual captura los paquetes que se encuentran en el dominio mediante el protocolo de red Syslog. El detalle a continuación (Figura 3.10 y Tabla 3.6):

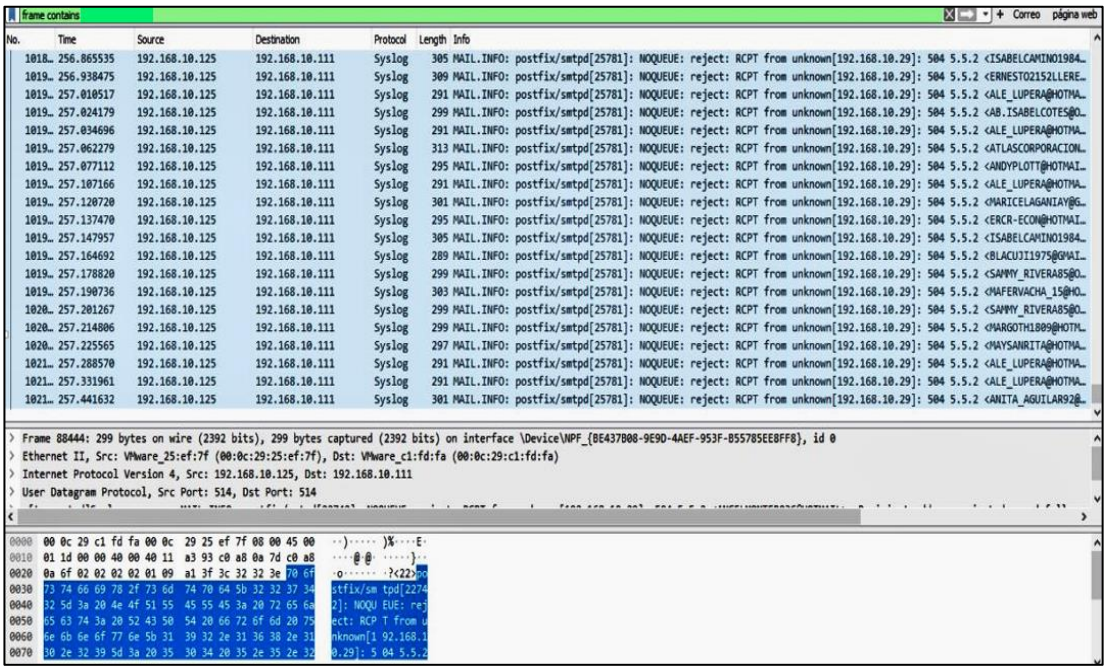


Figura 3.10: Paquete de correo electrónico con filtro según caso de estudio

Fuente: [107]

Tabla 3.6: Explicación Paquete de correo electrónico con filtro

Fuente: Elaboración propia

Explicación	Protocolo	Información
Figura 3.10	Syslog	Muestra todos los correos capturados con origen y destino al dominio del caso de estudio, incluyéndose los usuarios y contraseñas.

Por consiguiente, se presenta el tráfico TCP y UDP por el puerto 80 (Figura 3.11 y Tabla 3.7):

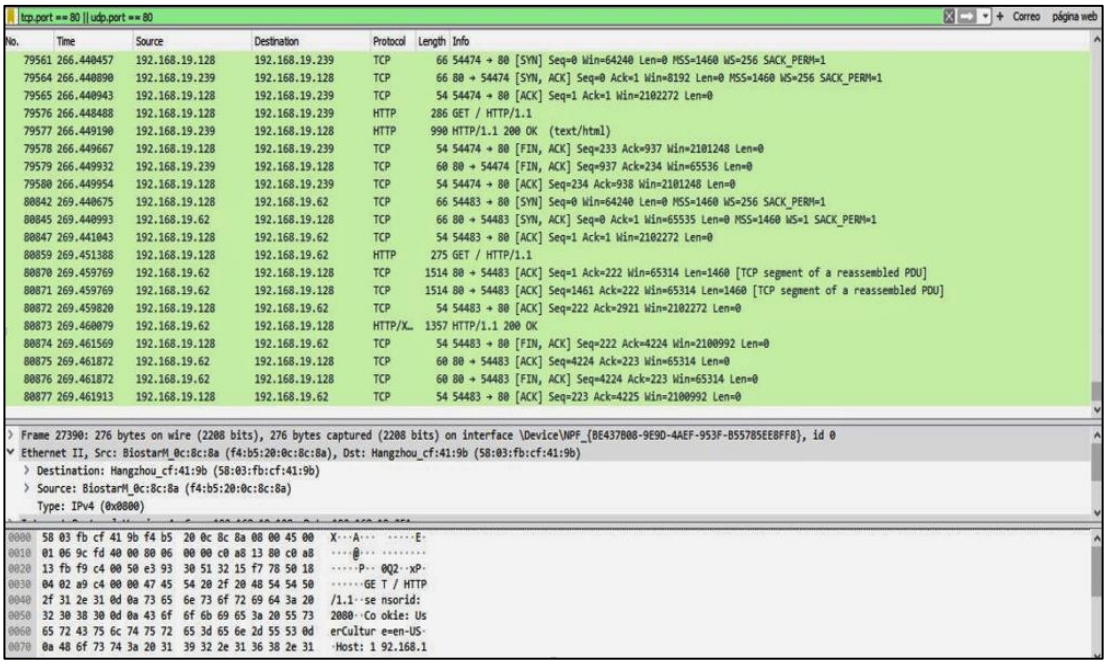


Figura 3.11: Tráfico TCP y UDP por el puerto 80

Fuente: [107]

Tabla 3.7: Explicación Tráfico TCP y UDP

Fuente: Elaboración propia

Explicación	Protocolo	Información
Figura 3.11	TCP	Identifica todo el tráfico de origen y destino, y captura el tráfico mediante el Protocolo de Datagramas de Usuario (UPD) por el puerto 80.

En adelante, uno de los ataques de ciberseguridad clásicos consiste en él envió de correos electrónicos para reemplazar un sitio web, el cual solicita al receptor dar clic en un enlace para posteriormente ingresar información personal, como credenciales o datos bancarios. A continuación, el detalle donde Wireshark con el filtro **tcp contains "https://sitio web/"** captura todos los paquetes alojados en el protocolo http o https (Figura 3.12 y Tabla 3.8):

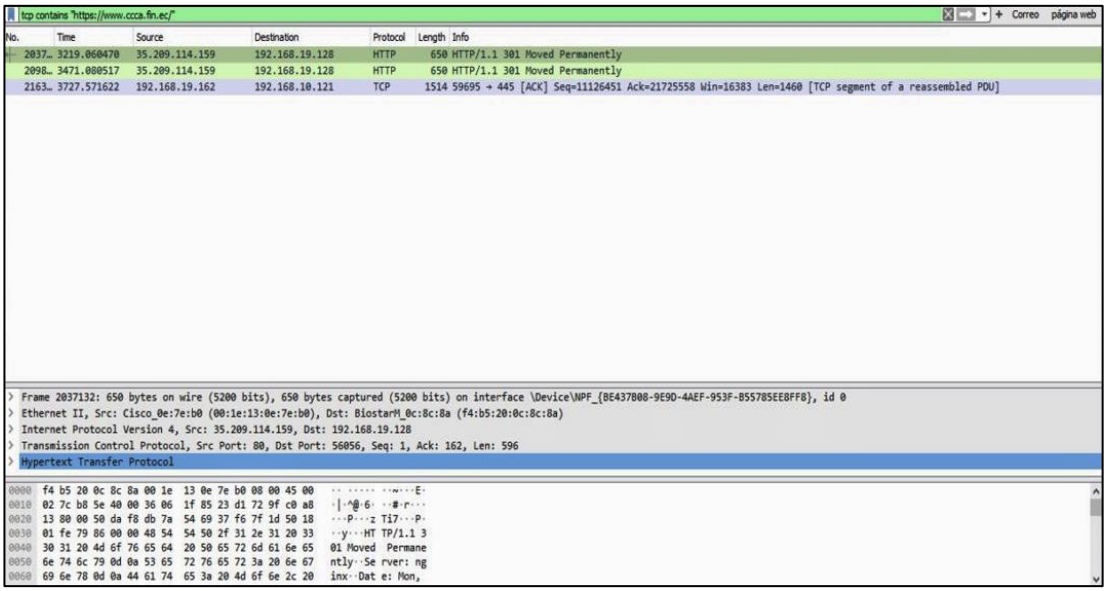


Figura 3.12: Tráfico, origen y destino del sitio web con el protocolo http o https

Fuente: [107]

Tabla 3.8: Explicación Tráfico, origen y destino del sitio web con el protocolo https

Fuente: Elaboración propia

Explicación	Protocolo	Información
Figura 3.12	HTTP	Muestra el tráfico y destino de "http://ccca.fin.ec/". Así como los paquetes que contienen en dicho sitio web.

Seguidamente, Wireshark permite detectar todas las transacciones SIP, registros de clientes, mensajes o llamadas. Por ello, a continuación se detalla el servidor de llamadas mediante teléfonos IP dentro de la Infraestructura de red del caso de estudio (Figura 3.13):

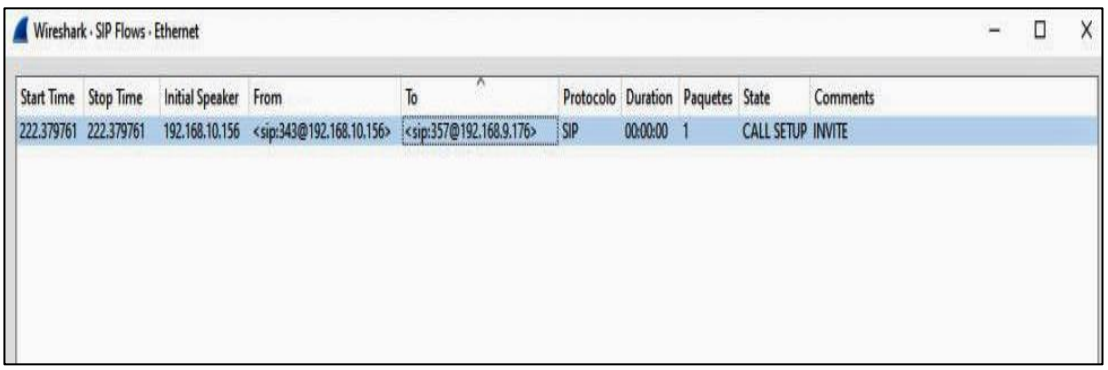


Figura 3.13: Lista de transacciones SIP completas y en curso.

Fuente: [107]

Continuamente, la Figura 3.14 representa un *host* específico donde cada fila son el paquete de tiempo, y los números de los extremos son el número de puerto de cada paquete que puede filtrar todas las conexiones por flujos de Protocolo de Mensajes de Control de Internet (ICMP), flujos ICMPv6, flujos de Monitoreo de Infraestructura (UIM) y flujos TCP.

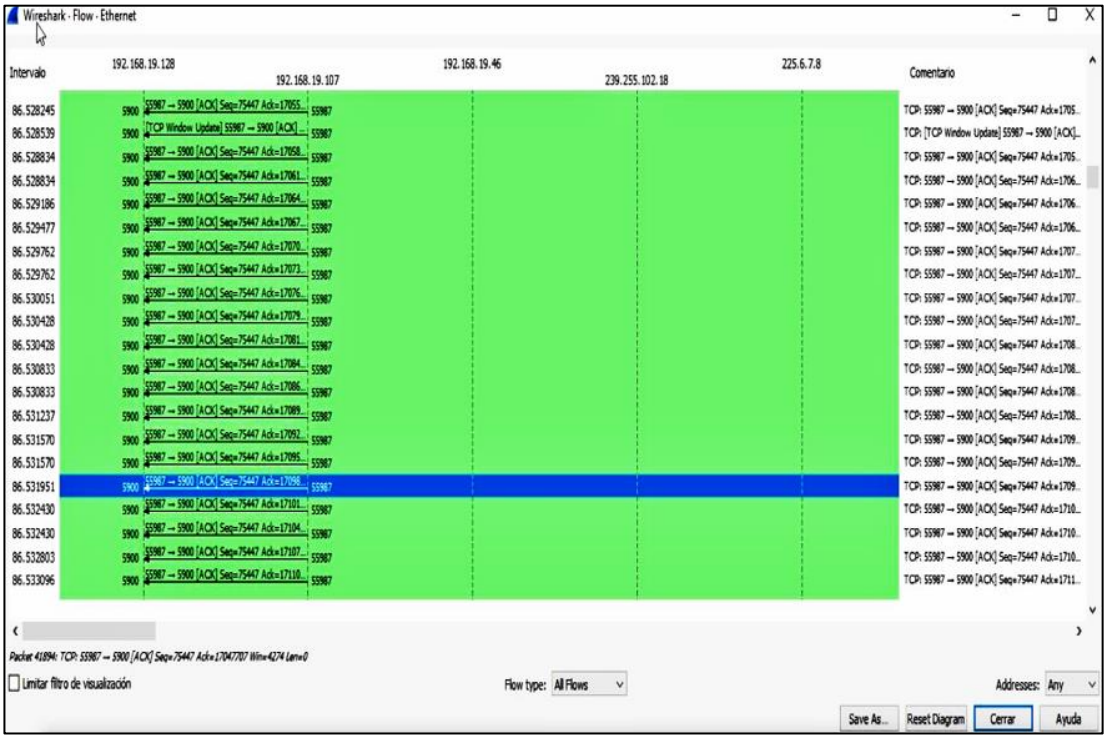


Figura 3.14: Conexiones por flujos ICMP, ICMPv6, UM y TCP

Fuente: [107]

Además de ello, la Figura 3.15 refleja las secuencias de peticiones HTTP que trabajan con encabezados Referer y Location de HTTP para secuenciar las peticiones HTTP como un árbol, lo cual permite verificar cómo una solicitud HTTP dirige a la siguiente.

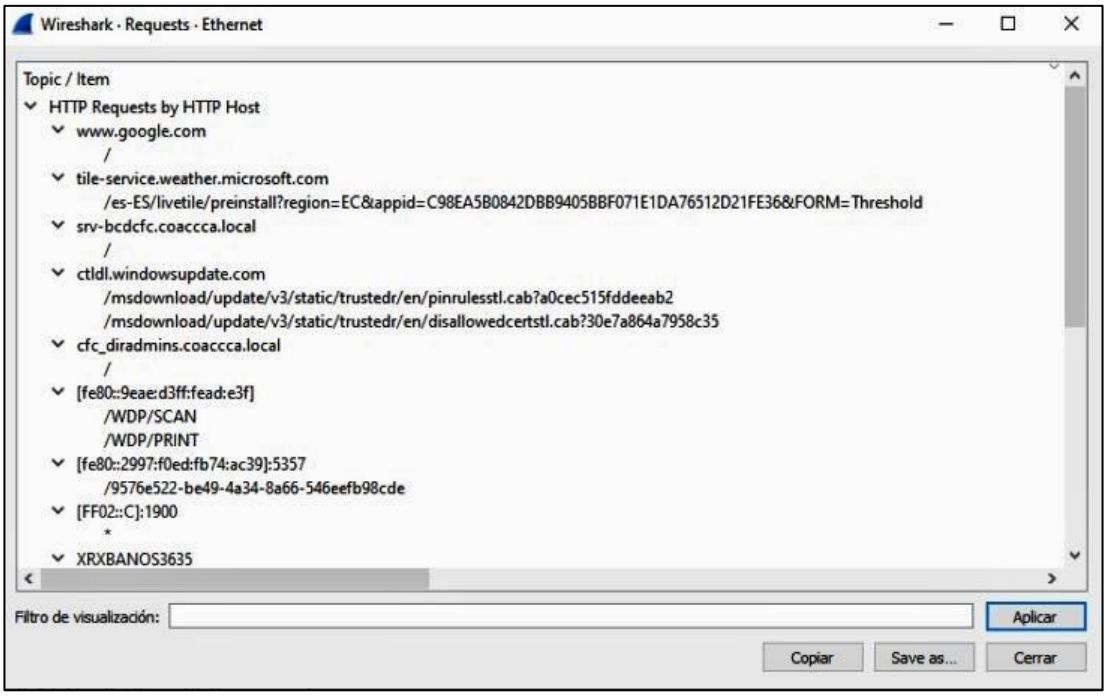


Figura 3.15: Peticiones HTTP que realiza la red

Fuente: [107]

Al mismo tiempo, la Figura 3.16 muestra la lista de direcciones resueltas y los nombres de *host*. Es decir, presenta los nombres de *host* para cada dirección IP en un archivo de captura con un *host* conocido en base a las respuestas del Sistema de Nombres de Dominio (DNS).

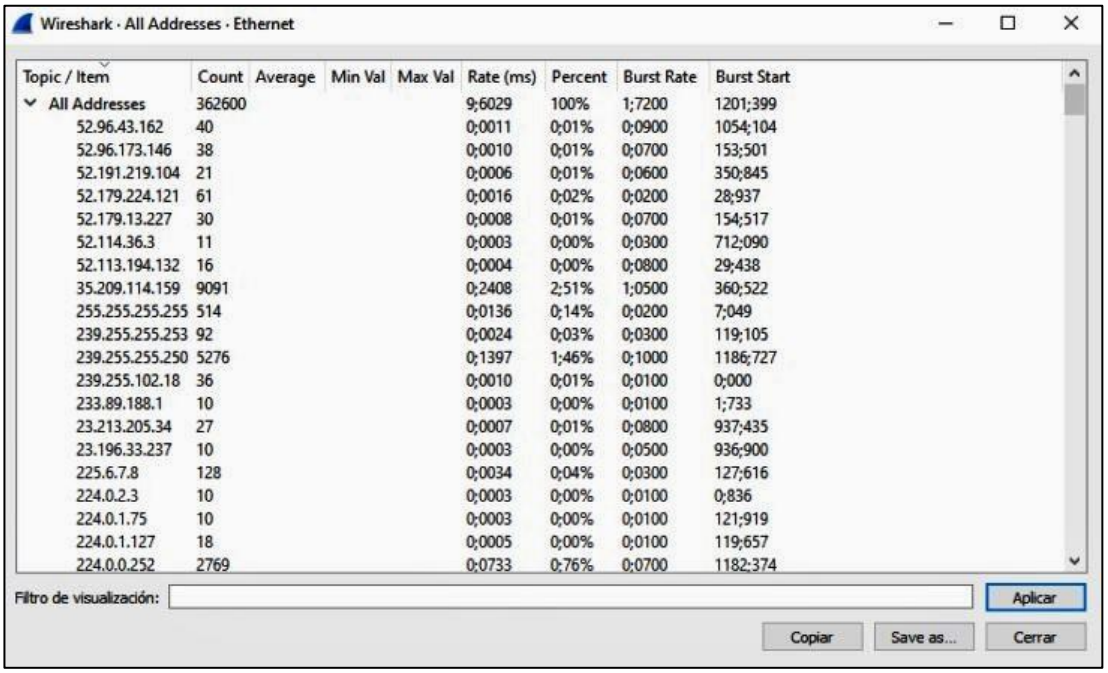


Figura 3.16: Lista de direcciones resueltas y los nombres de *host*

Fuente: [107]

Por consiguiente, la Figura 3.17 refleja los paquetes en base al número de puertos. El detalle a continuación:

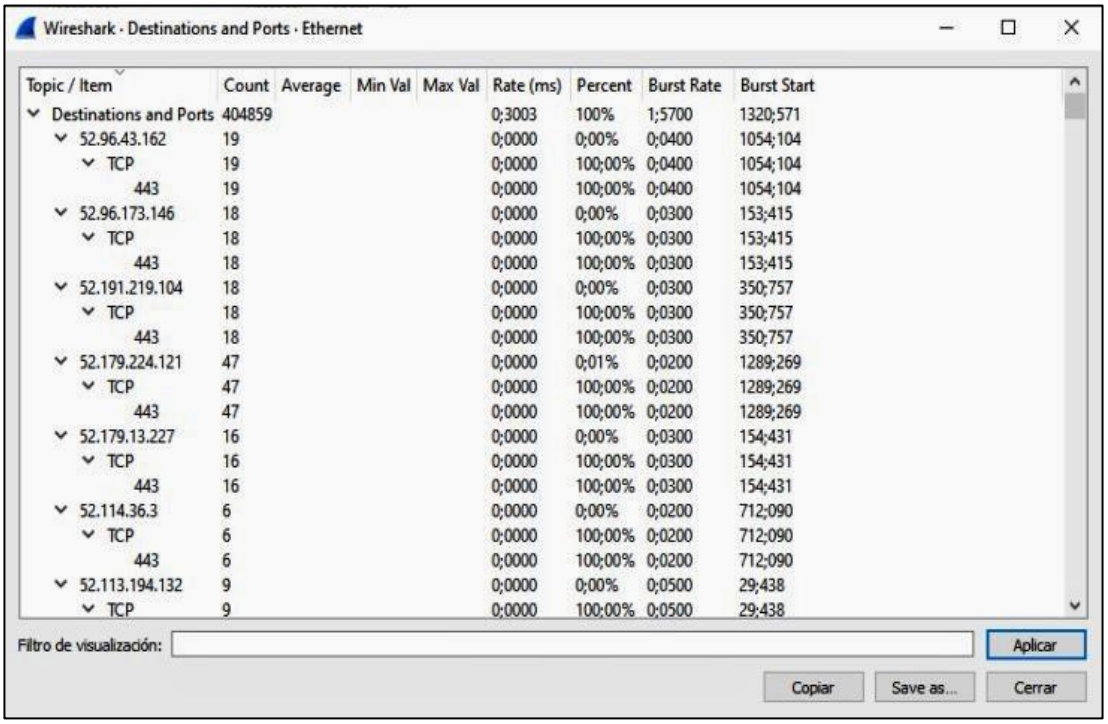


Figura 3.17: Paquetes según el número de puerto

Fuente: [107]

Asimismo, la Figura 3.18 muestra la lista de direcciones, los contadores de paquetes y los contadores de bytes de la ventana de conversaciones del caso de estudio que contiene:

- La hora en que inició la conversación ("*Rel Start*") o ("*Abs Start*").
- La duración de la conversación en segundos y el promedio de unidad mínima de información (*bits*) por segundo en cada dirección.
- Una línea de tiempo en las columnas " *Rel Start*" y "*Duration*".

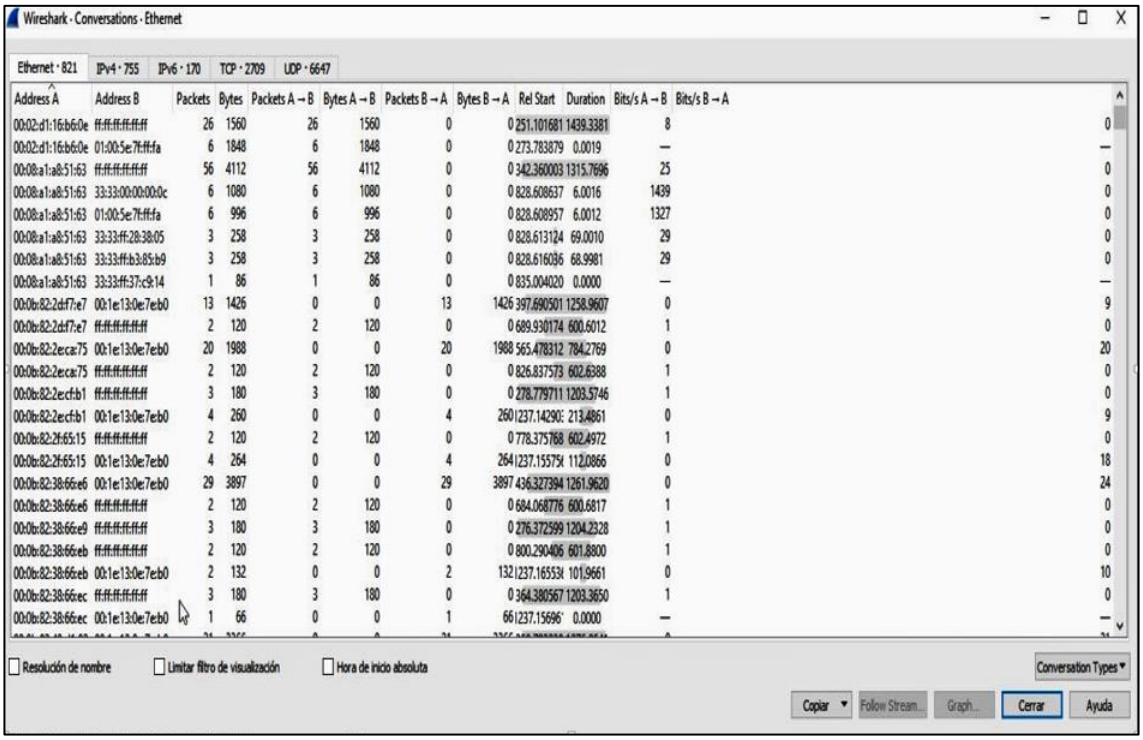


Figura 3.18: Paquete Conversaciones según el caso de estudio

Fuente: [107]

En definitiva, la Figura 3.19 refleja el intervalo de los paquetes de red según caso de estudio (CCCA). A continuación, el detalle:

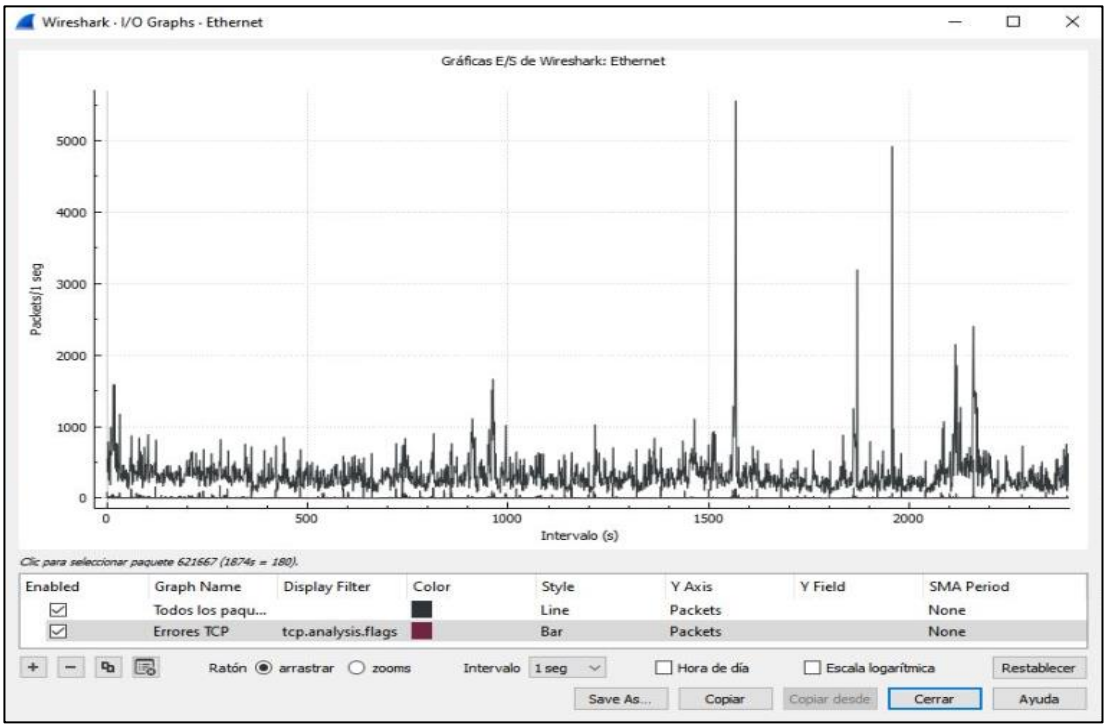


Figura 3.19: Intervalo de los paquetes de red según caso de estudio

Fuente: [107]

3.2 Discusión de resultados

En base a los resultados obtenidos mediante las herramientas de monitoreo y análisis de red se destaca el aporte de [43], al mencionar que la ciberseguridad es el conjunto de diversos programas o herramientas que protegen y proporcionan lineamientos, normas y mejores prácticas para gestionar el riesgo.

De esta forma, la actividad maliciosa (riesgo) que se identifica según el caso de estudio a través de la herramienta PRTG es que: 1) El antivirus Kaspersky y McAfee están caducados, 2) Existe saturación de Espacio de Disco en los computadores, 3) En la red interna los computadores tienen deshabilitado Windows Defender, 4) El Firewall de Windows también está deshabilitado, 5) Los sitios web a los que acceden los usuarios no cuentan con Certificado SSL válido. Mientras que, la herramienta Wireshark demuestra que: 1) El uso de ARP puede ocasionar un riesgo potencial de seguridad debido a la técnica (envenenamiento ARP) utilizada por *hackers* para introducir direcciones MAC falsas y generar desvió de la información, 2) Existen conexiones remotas que están vinculadas a un uso incorrecto de memoria, lo que puede generar fallos y denegación de servicios, donde atacantes pueden conseguir el acceso sin autorización a la información, 3) Existe impedimento de comunicación con sistemas principales en la red y problemas de direccionamiento, 4) El protocolo de red Syslog no posee ningún mecanismo de seguridad, ya que no cuenta con seguridad integrada que garantice el envío de mensajes. Por tanto, se resalta a [40, 49, 50] que mencionan tres fases para mitigar los riesgos: prevención (medida que permite actuar de manera oportuna), localización (medida que ayuda a localizar donde radica el problema a través de la monitorización continua del sistema.), y reacción (medida que permite brindar una respuesta técnica).

En ese contexto, para los autores [68, 69, 71] el monitoreo y análisis de una infraestructura tecnológica es indispensable ya que permite el funcionamiento de la actividad tecnológica de una entidad, empresa u organización. Además de ello, para [89] las ventajas de una adecuada infraestructura tecnológica en el sector financiero pueden ser: 1) Fomentar activos rentables, 2) Automatizar y simplificar los procesos transaccionales, 3) Elevar la competitividad empresarial, 4) Reducir costes, 5) Optimizar el servicio al cliente, entre otras. De esta manera, la importancia del objeto de estudio determinar un procedimiento de gestión para ciberseguridad, que ha criterio

de [1] debe ser considerado y abordado con conciencia y visión estratégica. De acuerdo con, [28] [29] un procedimiento de gestión es importante para: 1) Comprender las consecuencias de los incidentes, 2) Determinar prioridades para el tratamiento de riesgos, 3) Monitorizar y controlar la efectividad del tratamiento. En definitiva, para [26] [33] las acciones en un procedimiento deben: minimizar el riesgo (a través de medidas o controles), transportar el riesgo (mediante la contratación de un seguro) o aceptar el riesgo (monitorizarlo para controlar que no se incremente).

3.3 Desarrollo de la propuesta

En base a los resultados obtenidos y el aporte investigativo de los autores [34] [35] [36] [97] [98] se establece y sintetiza las fases para el procedimiento de gestión para ciberseguridad en la infraestructura tecnológica del sector financiero. A continuación, el detalle (Figura 3.19):

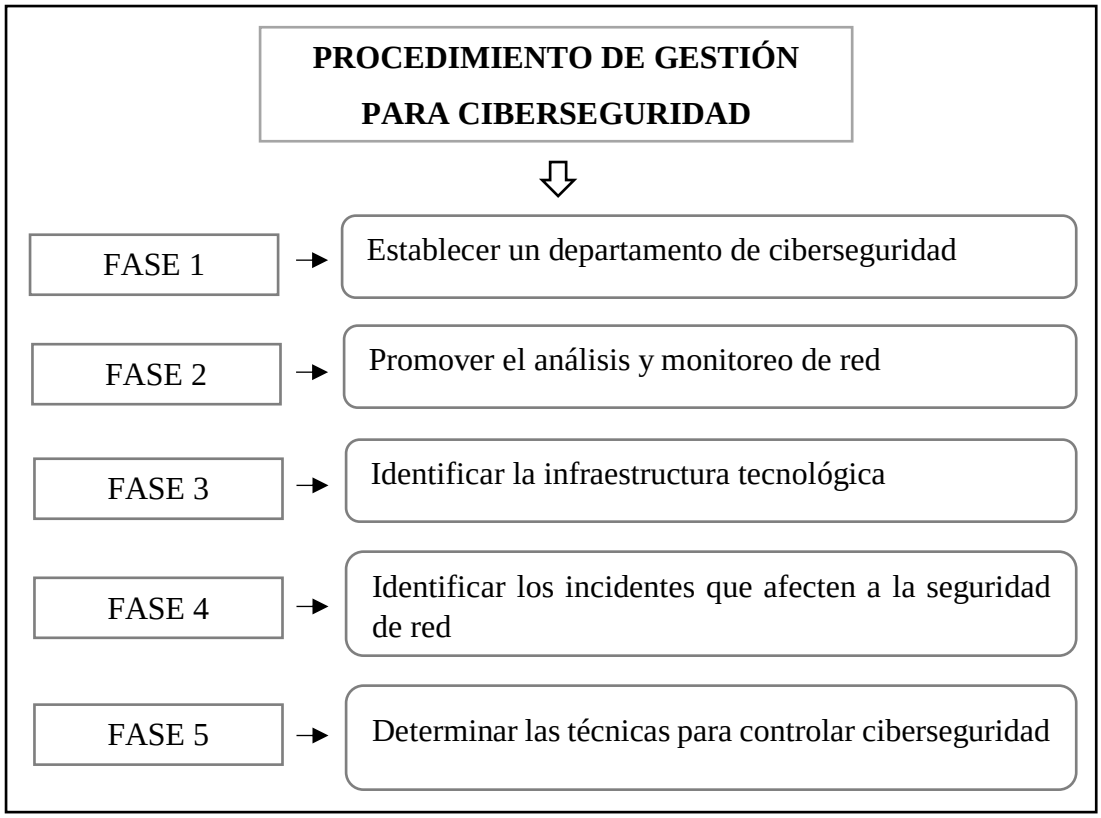


Figura 3.20: Fases para el procedimiento de gestión para ciberseguridad

Fuente: Elaboración propia

Fase 1: Establecer un departamento de ciberseguridad

Las entidades financieras que se encuentren en el Segmento 1 Regulado por la SEPS deben fomentar la seguridad de información de las diferentes herramientas financieras, por ende se sugiere establecer un departamento de ciberseguridad en base a objetivos institucionales que cuenten con procesos de autogestión para solventar problemas de seguridad en la infraestructura tecnológica.

Fase 2: Promover el análisis y monitoreo de red

La información es un contenido sensible por ende para conocer y diagnosticar el estado de la infraestructura tecnológica de las entidades financieras es indispensable utilizar herramientas que permitan analizar y detectar las áreas más vulnerables de la red para con ello evitar pérdidas económicas. Estas herramientas pueden ser:

- OpManager
- PRTG
- Wireshark
- OWASP

Debido a que son multiplataforma, es decir que pueden utilizarse en varios entornos o sistemas operativos. En este caso, en las entidades financieras los sistemas operativos utilizados con frecuencia son Linux y Windows, por ello el disponer de herramientas multiplataforma permitirá optimizar el tiempo, facilitar la instalación y mejorar la funcionalidad.

Fase 3: Identificar la infraestructura tecnológica

El conjunto de dispositivos que conforma una infraestructura tecnológica debe ser identificada claramente para tomar como referencia las áreas que se pretende proteger, además es fundamental conocer las herramientas financieras que son consideradas como las más vulnerables para los ciberataques.

- Zimbra: Correo institucional.
- Billetera Electrónica: Servicio web y móvil que permite realizar transferencia y pagos de servicios básicos.
- Página Web: Medio informativo donde las entidades financieras exponen los servicios.

Fase 4: Identificar los incidentes que afecten a la seguridad de red

El objetivo es identificar los puntos débiles o incidencias que pueden afectar las herramientas financieras, planteándose que existen diversas técnicas que vulneran la información, por lo cual es necesario realizar pruebas capturando paquetes en base a protocolos de comunicación de red abiertos y verificando el estado de la infraestructura tecnológica. En base aquello:

- Protocolos de comunicación de red: ARP, TCP, ICM, SMTP, SYSLOG, UDP.
- Infraestructura tecnológica: Comprobación SSL, Estado del antivirus, entre otros.

Fase 5: Determinar las técnicas para controlar ciberseguridad

Una vez definido los riesgos, amenazas o actividad maliciosa es necesario determinar las técnicas para solucionar la seguridad de las herramientas financieras. En ese contexto:

- Los desarrolladores de software deben llevar a cabo un proceso de validación de datos de entrada.
- Evitar la pérdida de información al autenticarse en las herramientas financieras.
- Mitigar la exposición de datos sensibles que afecten a la entidad financiera.
- Deshabilitar la ejecución remota de códigos en servicios web.
- Evadir el uso de componentes, extensiones con vulnerabilidades conocidas.
- Establecer periódicamente el mantenimiento de equipos para gestionar las actualizaciones.
- Prevenir el almacenamiento de contraseñas en los navegadores, entre otras.

CAPITULO IV.-

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Se concluye que la ciberseguridad es el conjunto de políticas, herramientas, directrices, procedimientos de gestión de seguridad, métodos de gestión de riesgos, entre otros que permiten proteger a los usuarios del ciberentorno y los activos organizacionales. Por tanto, un procedimiento de gestión es un conjunto de fases que permiten controlar los componentes de una infraestructura de manera segura y eficiente.

Ahora bien, la actividad maliciosa que se identificó según el caso de estudio mediante la herramienta PRTG es que el antivirus Kaspersky y McAfee están caducados, existe saturación de Espacio de Disco en los computadores, la red interna los computadores tienen deshabilitado Windows Defender, entre otros. Mientras que, la herramienta Wireshark demuestra que el uso de ARP puede ocasionar un riesgo potencial de seguridad debido a la técnica (envenenamiento ARP) utilizada por hackers para introducir direcciones MAC falsas, existen conexiones remotas que están vinculadas a un uso incorrecto de memoria, existe impedimento de comunicación con sistemas principales en la red y problemas de direccionamiento, otros. En base aquello, se determinó un procedimiento de gestión para ciberseguridad según el análisis de las herramientas de monitoreo de red.

Por tanto, el procedimiento abarca cinco fases como: 1) Establecer un departamento de ciberseguridad, 2) Promover el análisis y monitoreo de red, 3) Identificar la infraestructura tecnológica, 4) Identificar los incidentes que afecten a la seguridad de red, 5) Determinar las técnicas para controlar ciberseguridad; cada una con el respectivo detalle conforme al análisis de las herramientas de monitoreo de red. En definitiva, las entidades financieras del Segmento 1 Regulado por las SEPS deben contar con un procedimiento y personal capacitado en el área de ciberseguridad, puesto que si no lo tienen pueden presentar sanciones, pérdidas económicas y vulnerabilidad debido a riegos que afectan funciones como disponibilidad, autenticidad, integridad y confidencialidad.

4.2 Recomendaciones

Se recomienda las herramientas multiplataforma como OpManager, PRTG, Wireshark y OWASP para monitorear y analizar la infraestructura de red con el objetivo de determinar en tiempo real la actividad maliciosa (riesgos) presente en la entidad financiera. Además de ello, estas herramientas pueden utilizarse en varios entornos o sistemas operativos para optimizar el tiempo, facilitar la instalación y mejorar la funcionalidad.

Por consiguiente, es indispensable que el sector financiero disponga de un Certificado SSL para que las herramientas tecnológicas como: correo electrónico, página web, billetera electrónica, entre otras; proteja la transferencia de datos dentro del dominio. Al mismo tiempo, es necesario mantener o adquirir una consola de administración de antivirus vigente para evitar conexiones innecesarias a los dispositivos y robo de datos o información.

Por último, se sugiere la implementación de un procedimiento de gestión para ciberseguridad en la infraestructura del sector financiero que brinde técnicas de acción para la protección de la información para evitar actividad maliciosa y la exposición de datos.

BIBLIOGRAFÍA

[1] M. Cando y P. Medina, «Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica,» *3C TIC,* vol. 10, nº 1, pp. 17-25, 2021.

[2] W. Rosas, F. Medina y J. Mesa, «Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas,» *ESPACIOS,* vol. 41, nº 7, pp. 27-41, 2019.

[3] D. Rowe, B. Lunt y J. Ekstrom, «The role of cyber-security in information technology education,» *SIGITE,* vol. 11, nº 9, pp. 20-32, 2011.

[4] H. Alduhaidahawi, J. Zhang, M. Salam y M. Sebai, «The financial technology (fintech) and cybersecurity,» *International Journal of Research in Business and Social Science,* vol. 9, nº 6, pp. 123-133, 2020.

[5] L. Almagro, F. Urrutia y A. Daniell, Educación en ciberseguridad. Planificación del futuro mediante el desarrollo de la fuerza laboral, Estados Americanos: OAS, 2020.

[6] BID, Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe, Estados Americanos: IADB, 2020.

[7] J. Vacca, Cyber security and IT infrastructure protection, Amsterdam: Elsevier Inc., 2014.

[8] A. Risteski, M. Bogdanoski, M. Stoilkovski y M. Jovanovic, Cyber security issues of telecommunication infrastructure, Washington, DC: IOS Press, 2014.

[9] SEPS, «Norma de control para la administración del riego operativo y riesgo legal en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria,» SEPS-IGT-IR-IGJ-2018-0279, Ecuador, 2018.

[10] BCE, «Ley de Régimen Monetario y Banco del Estado,» Banco Central del Ecuador, Ecuador, 2010.

[11] SB, «Código Orgánico Monetario y Financiero,» Superintendencia de Bancos, Ecuador, 2020.

[12] SEPS, «Ecuador tiene un total de 887 cooperativas de ahorro y crédito,» Superintendencia de Economía Popular y Solidaria, Ecuador, 2021.

[13] J. Alarcon, «Bancos privados en el Ecuador,» Brainly, Ecuador, 2018.

[14] F. Ojeda, V. Moreno y M. Torres, «Risk management and cybersecurity in the popular and solidarity financial sector of Ecuador,» *CIENCIAMATRIA,* vol. 8, nº 9, pp. 4-18, 2020.

[15] A. Peraza, «Herramientas financieras,» *Academia,* vol. 10, nº 8, pp. 1-12, 2018.

[16] E. Bello, «Learn about cybersecurity tools to protect your company,» *Innovation & Entrepreneurship Business,* vol. 90, nº 78, pp. 31-42, 2021.

[17] G. O'Donnell, «Ciberseguridad en el sector financiero: una gran preocupación para el 2020,» ecaldima, España, 2020.

[18] L. Remolina, «Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología,» UCC, Bogotá D.C, 2019.

[19] UNC, «Política de seguridad de la información para la Universidad Nacional de Córdoba,» UNC, Argentina, 2018.

[20] WeLiveSecurity, «Importancia de la gestión de incidentes para la seguridad de la información,» WS, España, 2016.

[21] SB, «Gestión de seguridad informática,» Superintendencia de Bancos , Ecuador, 2017.

[22] MINTIC, «Seguridad y privacidad de la información,» Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia, 2016.

[23] R. Barzanallana, «Gestión de la seguridad en sistemas de información,» UMU, España, 2017.

[24] CEUPE, «Seguridad informática y protección de datos,» Centro Europeo de Postgrado y Empresa, Madrid, 2021.

[25] IIMV, «Seguridad informática,» Instituto Iberoamericano de Mercados de Valores, Ecuador, 2014.

[26] J. Páez, «Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la política nacional de ciberseguridad del Ecuador,» ESPE, Ecuador, 2020.

[27] Incibe, «Gestión de riesgos. Una guía de aproximación para el empresario,» Instituto Nacional de Ciberseguridad, España, 2015.

[28] H. Tohidi, «The role of risk management in IT systems of organizations,» *Procedia Computer Science,* vol. 3, nº 1, pp. 881-887, 2011.

[29] H. Ibrahim, S. Islam y M. Abdur, «An integrated cyber security risk management approach for a cyber-physical system,» *Applied Sciences,* vol. 8, nº 898, pp. 1-29, 2018.

[30] S. Ambore, C. Richardson, H. Dogan, E. Apeh y D. Osselton, «A resilient cybersecurity framework for Mobile Financial Services (MFS),» *Journal of Cyber Security Technology,* vol. 3, nº 4, pp. 202-224, 2017.

[31] N. Raj, N. Khanal, C. Tsokos y K. Pokhrel, «Cybersecurity: a predictive analytical model for software vulnerability discovery process,» *Journal of Cyber Security Technology,* vol. 5, nº 1, pp. 41-69, 2021.

[32] F. Catota, G. Morgan y D. Sicker, «Cybersecurity incident response capabilities in the Ecuadorian financial sector,» *Journal of Cybersecurity*, vol. 4, nº 1, pp. 1-20, 2018.

[33] DNV, «The three-pillar approach to cyber security: processes are crucial,» Horizon Graphic, Washington D.C, 2021.

[34] ESAN, «Pasos para implementar un sistema de seguridad de información,» Monterrico, Lima, 2019.

[35] M. Huaura, «Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones,» UNMM, Lima, 2019.

[36] P. Morales y P. Medina, «Cibersecurity for learning plataforms in higher education institutions in Tungurahua province of Ecuador,» *3C TIC. Cuadernos de desarrollo aplicados a las TIC,* vol. 10, nº 2, pp. 49-75, 2021.

[37] CNO, «Guía de ciberseguridad,» Cnostatic, Colombia, 2019.

[38] SENDA, «Procedimiento de gestión de incidentes de seguridad de la información,» MISP, Chile, 2019.

[39] BCE, «Manual de procedimiento para la gestión de incidentes de seguridad de la información y ciberseguridad,» Banco Central del Ecuador, Ecuador, 2019.

[40] W. Alvarado y I. Changoluisa, «Análisis de la ciberseguridad a la infraestructura tecnológica de la Universidad Técnica de Cotopaxi,» UTC, Ecuador, 2019.

[41] A. Valdez, «Introducción a la ciberseguridad,» *Tecnology,* vol. 67, nº 90, pp. 25-45, 3C TIC.

[42] N. Arias y J. Celis, «Modelo experimental de ciberseguridad y ciberdefensa para Colombia,» UL, Bogotá D.C, 2015.

[43] M. Romero y G. Figueroa, Introducción a la seguridad informática y el análisis de vulnerabilidades, España: 3ciencias, 2018.

[44] W. Pérez y M. Ramos, «Propuesta de una política de ciberseguridad para las Fuerzas Armadas,» ESPE, Ecuador, 2020.

[45] R. Sáinz, Ciberseguridad, la protección de la información en un mundo digital, UNIGRAF, S.L: España, 2016.

[46] M. Arévalo, «ISO 27032, el estándar enfocado en ciberseguridad,» Pirani, Colombia, 2020.

[47] Incibe, «El mercado de la ciberseguridad alcanzará los 80.000 millones de euros en 2018,» Instituto Nacional de Ciberseguridad, España, 2016.

[48] OEA, «Ciberseguridad Marco NIST. Un abordaje de la ciberseguridad,» Organización de los Estados Americanos, EEUU, 2019.

[49] B. Sanou, «Guide to developing a national cybersecurity strategy,» ITU, Suiza, 2018.

[50] D. Chatterjee, Cybersecurity readiness: a holistic and high-performance approach, SAGE Publications: USA, 2021.

[51] P. Moncayo, «Herramientas jurídicas para garantizar la ciberseguridad del estado. Análisis comparado de Colombia, Chile y Ecuador,» UCE, Ecuador, 2019.

[52] InnoTec, «Ciberamenazas,» Entelgy, España, 2013.

[53] P. Alfaro, E. García, A. Díaz y S. Sánchez, «Riesgos y amenazas en el ciberespacio. Situación actual,» CSDN, Madrid, 2013.

[54] Y. Wilches, «Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo PYMES,» UNI, Ecuador, 2015.

[55] Y. Sierra, «Ciberseguridad,» Lemontech, España, 2021.

[56] N. Montaño, «Ciberseguridad, valor añadido de empresa,» Ambit, Barcelona, 2020.

[57] J. Bautista, «Situación actual de las empresas en torno a la ciberseguridad,» Conexure, España, 2020.

[58] Widefense, «Ciberseguridad empresas: beneficios,» WD, España, 2020.

[59] J. Bustamante, «Ventajas de la ciberseguridad,» Disete, Colombia, 2021.

[60] R. Ryder y A. Madhava, Cyber crisis management: overcoming the challenges in cyberspace, London: Bloomsbury Publishing, 2019.

[61] D. Kosutic, Ciberseguridad en 9 pasos. El manual sobre seguridad de la información para el gerente, Zagreb: EPPS Services Ltd, 2012.

[62] M. Arceneaux, «15 cybersecurity fundamentals for water and wastewater utilities,» WaterISAC, Washington D.C, 2019.

[63] M. Porrúa y B. Contreras, Cibersecurity: risks, progress, and the way forward in Latin America and the Caribbean, USA: Creative Commons, 2016.

[64] J. Lewis, «Experiencias avanzadas en políticas y prácticas de ciberseguridad,» BID, Estados Unidos, 2016.

[65] J. Rodríguez, «Diseño de una metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales en instituciones

financieras de la economía popular y solidaria basadaen las buenas prácticas de la PCI DSS,» SEK, Ecuador, 2019.

[66] A. Villavicencio, «Ciberseguridad en el sector cooperativo del Ecuador,» *ICORED*, vol. 4, nº 27, pp. 16-19, 2016.

[67] A. Alonso, «Infraestructura tecnológica,» CEUPE, Madrid, 2021.

[68] M. Yunda, «Procedimiento gestión de seguridad informática,» CB, Bogotá D.C, 2018.

[69] EducareCorp, «Infraestructura tecnológica,» GEducare, México, 2019.

[70] M. Campos, «Infraestructura IT,» Avansis, España, 2020.

[71] S. Munévar, «Diseño de una infraestructura tecnológica funcional dentro de un plan piloto propuesto para la implementación de teletrabajo,» EAN, Colombia, 2013.

[72] FUNIBER, «Infraestructura tencológica de software,» FIS, España, 2020.

[73] L. Sánchez, A. Reyes, D. Ortíz y F. Olarte, «El rol de la infraestructura tecnológica en relación con la brecha digital y la alfabetización digital en 100 instituciones educativas de Colombia,» *Calidad en la educación*, vol. 23, nº 47, pp. 112-144, 2017.

[74] L. Juárez, «Infraestructura IT,» IJAM, México, 2019.

[75] J. Pacheco, «WEB y empresas,» 29 febrero 2020. [En línea]. Available: https://www.webyempresas.com/herramientas-financieras/. [Último acceso: 01 06 2021].

[76] OAS, «Manual de políticas de tecnología de la información de la DIGEIG,» DIGEIG, República Dominicana, 2012.

[77] I. Albarrán, C. Heredero y A. Montero, «Uso del correo electrónico: un análisis empírico en la UCM,» *ESPACIOS*, vol. 3, nº 30, pp. 1-30, 2018.

[78] H. Delgado, «Ventajas y beneficios de tener una página web en internet,» Akus, México, 2021.

[79] M. Fernández, El impulso de la billetera móvil en su repercusión en la inclusión financiera del Perú, Lima: PIRHUA, 2018.

[80] M. Holguín y M. Maldonado, «La aceptaciónde la billetera móvil en empresas influyentes del Ecuador,» USFQ, Ecuador, 2011.

[81] C. Padilla, «La importancia de contar con correo electrónico empresarial,» Migesa, España, 2017.

[82] EFIEMPRESA, «Páginas web empresariales y su valor estratégico,» Efiempresa LLC, España, 2020.

[83] EUATM, «Introducción al web,» ETS, España, 2015.

[84] Software Group, «Principales impulsadores para lanzar una billetera móvil,» SG, España, 2018.

[85] R. Martínez, «Chatbots transaccionales,» inConcert, España, 2019.

[86] L. González, «Consultas IVR transaccionales,» Mitrol, Argentina, 2019.

[87] N. Dumlao, «Botón de Pagos en Ecuador,» Emprende 300, Ecuador, 2020.

[88] Software DELSOL, «Tarjeta de débito-crédito,» Mengíbar, España, 2019.

[89] SoftDoit, «Software financiero: mejora el proceso de contabilidad y finanzas del negocio,» Softwaredoit, España, 2020.

[90] SEPS, «Nueva segmentación Sector Financiero Popular y Solidario,» Superintendencia de Economía Popular y Solidaria, Ecuador, 2014.

[91] Biess, «Reglamento a la Ley General de Instituciones del Sistema Financiero,» Banco del Instituto Ecuatoriano de Seguridad Social, Ecuador, 2012.

[92] K. García, «Cooperatives of savings and credit of Ecuador and its incidence in the formation of the social capital,» *ESPACIOS,* vol. 39, nº 28, pp. 32-39, 2018.

[93] R. Curiazi, M. Dorigatti y T. Menzani, La integración, clave para el éxito de los actores de la economía popular y solidaria, Ecuador: Intendencia de Información Técnica, Investigación y Capacitación, 2017.

[94] P. Estrella y C. Terán, «Evaluación y propuesta de gestión de las tecnologías de información y comunicaciones para las Cooperativas de Ahorro y Crédito del Ecuador,» EPN, Ecuador, 2017.

[95] R. Ruiz y F. Mayorga, «Auditoría informática, para la evaluación de riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito Prodvisión, de la provincia de Tungurahua, cantón Pelileo,» UTA, Ecuador, 2021.

[96] Ministerio de Administraciones Públicas, MAGERIT – version 2: methodology for information systems risk analysis and management, Madrid: NIPO, 2016.

[97] H. Santiso, J. Koller y M. Bisaro, «Seguridad en entornos de seguridad virtual,» *Security in Virtual Education Environments,* vol. 14, nº 14, pp. 67-88, 2016.

[98] B. Merino, «Análisis de tráfico con Wireshark,» INTENCO, España, 2020.

[99] U. o. Oregon, «All in one network graphing and monitoring,» NSRC, Oregon, 2017.

[100] I. Adrem Software, «Netcrunchh,» AdremSoft, New York, 2016.

[101] Z. Corp, «Open Manager User Guide,» Manage Engine, Chennai, 2017.

[102] M. Faisal, «Using Openms to analyze the irregularities of the Internet Network,» State Politechnic of Jakarta, Jakarta, 2018.

[103] D. Leiva, «Manual PRTG Network Monitor,» Paessler AG, Nuremberg, 2018.

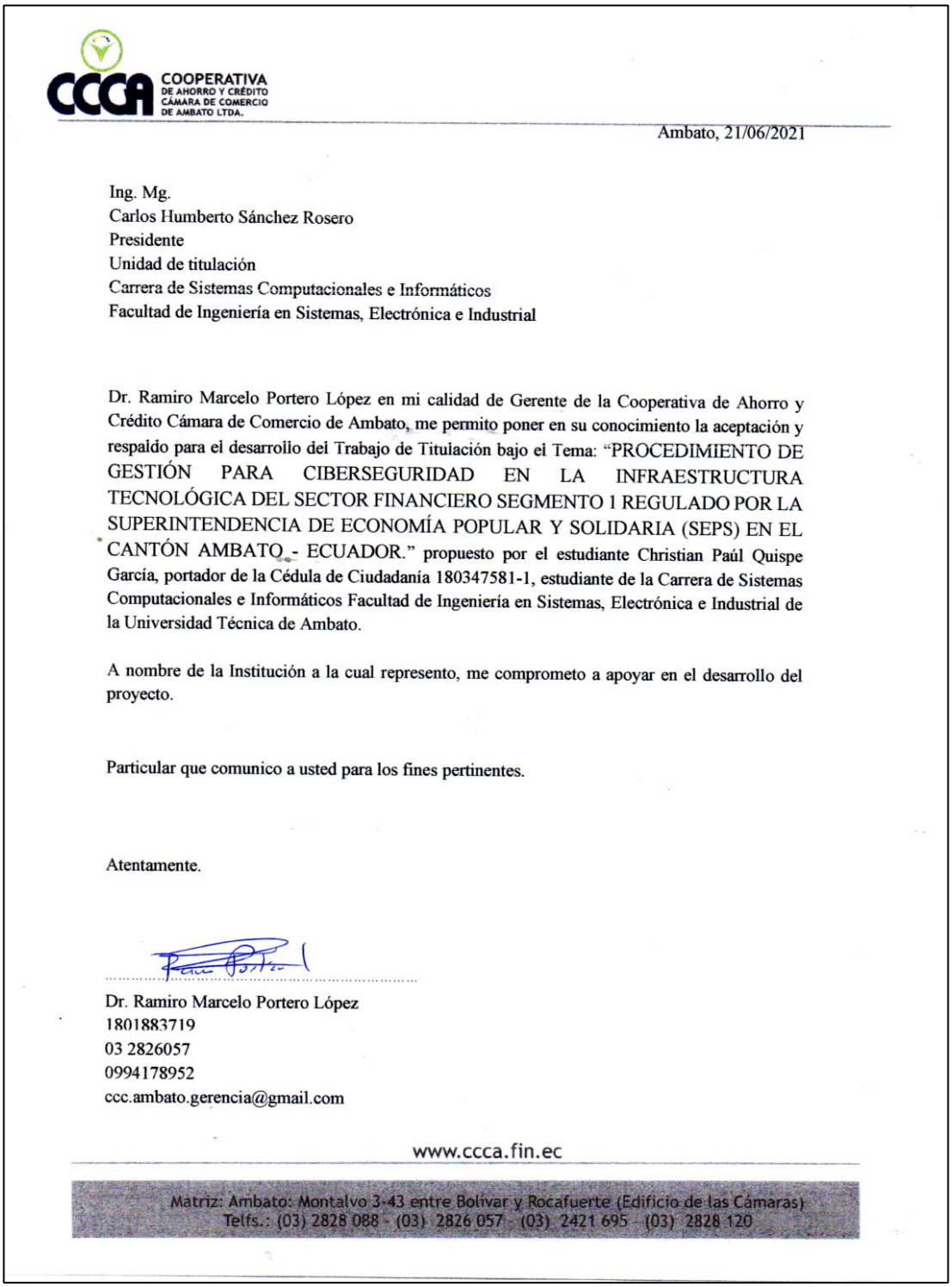
[104] S. Lerena, «Kit de prensa Pandora,» Artica Soluciones Tecnológicas, Madrid, 2017.

[105] G. Combs, G. Harris y G. Ramirez, «Wireshark User's Guide,» Syngress, Dubin, 2019.

[106] R. G. Dirk, «PRTG,» Paessler, 08 Junio 2017. [En línea]. Available: https://127.0.0.1/group.htm?id=0&tabid=1. [Último acceso: 22 Julio 2021].

[107] G. Combs, «Wireshark,» Wireshark Team, Kansas City, 1998.

ANEXOS



COOPERATIVA DE AHORRO Y CRÉDITO CÁMARA DE COMERCIO DE AMBATO LTDA.

Ambato, 21/06/2021

Ing. Mg.
Carlos Humberto Sánchez Rosero
Presidente
Unidad de titulación
Carrera de Sistemas Computacionales e Informáticos
Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Dr. Ramiro Marcelo Portero López en mi calidad de Gerente de la Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato, me permito poner en su conocimiento la aceptación y respaldo para el desarrollo del Trabajo de Titulación bajo el Tema: "PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO - ECUADOR." propuesto por el estudiante Christian Paúl Quispe García, portador de la Cédula de Ciudadanía 180347581-1, estudiante de la Carrera de Sistemas Computacionales e Informáticos Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

A nombre de la Institución a la cual represento, me comprometo a apoyar en el desarrollo del proyecto.

Particular que comunico a usted para los fines pertinentes.

Atentamente.

Dr. Ramiro Marcelo Portero López
1801883719
03 2826057
0994178952
ccc.ambato.gerencia@gmail.com

www.ccca.fin.ec

Matriz: Ambato: Montalvo 3-43 entre Bolívar y Rocafuerte (Edificio de las Cámaras)
Telfs.: (03) 2828 088 (03) 2826 057 (03) 2421 695 (03) 2828 120

Anexo 1. Carta Aceptación caso estudio

Fuente: Asistente TI - Investigador