UNIVERSIDAD PRIVADA LÍDER PERUANA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Trabajo de investigación

Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020

Para obtener el grado académico de bachiller en ingeniería de sistemas e informática

Autor

Paul Bides Olarte Quispe

Asesor

Rafael Ricardo Quispe Merma

Santa Ana, La Convención, Cusco

2021

Línea de Investigación:

Gestión de los sistemas de información

Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020

Resumen

El trabajo de investigación titulado “Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020”**;** cuyo problema objeto de investigación es: ¿qué mecanismos de seguridad informática son importantes conocer para evitar la vulnerabilidad del sistema de información inalámbrico?; el objetivo propuesto es: conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información inalámbrico; y como hipótesis: los mecanismos de seguridad informática son importantes conocer para evitar la vulnerabilidad del sistema de información inalámbrico. Con el propósito de orientar la investigación dentro de un conjunto de conocimientos, hemos desarrollado el marco teórico que comprende los antecedentes, teorías, conceptos y dimensiones de la primera variable seguridad informática y de la segunda variable vulnerabilidad del sistema de información. El estudio tiene enfoque cuantitativo y descriptivo, el diseño es no experimental y de alcance exploratorio y descriptivo. En el proceso de investigación se ha diseñado y aplicado técnicas e instrumentos para la recolección y procesamiento de datos. Luego se ha realizado las pruebas y contrastación de hipótesis; estableciéndose la conclusión preliminar, que los mecanismos de seguridad informática son importantes conocer para evitar la vulnerabilidad de sistema de información.

Abstrac

The research work entitled "Computer security and the vulnerability of the wireless information system in the Provincial Municipality of La Convention, period 2020"; whose problem under investigation is: what computer security mechanisms are important to know to avoid the vulnerability of the wireless information system ?; The proposed objective is: to know the importance of computer security mechanisms to avoid the vulnerability of the wireless information system; and its hypothesis: the computer security mechanisms are important to know to avoid the vulnerability of the wireless information system. With the purpose of guiding the research within a set of knowledge, we have developed the theoretical framework that includes the antecedents, theories, concepts and dimensions of the first variable computer security and the second variable vulnerability of the information system. The study has a quantitative and descriptive approach, the design is non-experimental and exploratory and descriptive in scope. In the research process, techniques and instruments for data collection and processing have been designed and applied. The initial results of the investigation are presented in tables, with their respective interpretation and analysis, then the tests and hypothesis contrast have been carried out; establishing the preliminary conclusion, that the computer security mechanisms are important to know to avoid the vulnerability of the information system.

INDICE

CAPÍTULO I. Introducción

1.1 Antecedentes del problema

Los gobiernos locales son instituciones fundamentales de las circunscripciones territoriales de las provincias y distritos del país, que conforman parte de la organización geográfica del estado peruano. Estas entidades permiten que los ciudadanos tengan una participación ciudadana en los asuntos y problemas de interés público que aquejan y afectan a la ciudadanía en general. En mérito a ello la ley orgánica de municipalidades, establece que los gobiernos locales poseen autonomía política, económica y administrativa en los asuntos de su competencia y jurisdicción. Las municipalidades son los órganos administrativos de los gobiernos locales y son generadores del desarrollo de su localidad, con personería jurídica de derecho público y plena autonomía para cumplir sus roles y competencias. Los gobiernos cumplen sus roles y competencias a través de las municipalidades. En este contexto la Municipalidad Provincial de La Convención como órgano administrativo del gobierno local tiene el objetivo de satisfacer las demandas y necesidades de los ciudadanos, y garantizar la coparticipación de los ciudadanos en la solución de los problemas económico, sociales y otros de interés local; para ello la municipalidad cumple y desarrolla procesos de prestación de servicios y programas públicos, ejecuta proyectos y actividades, administra y gestiona el territorito local, desarrollo actos de gobierno y de administración; y en este procesos de administración y gestión municipal, los distintos órganos administrativos y operativos de su estructura orgánica utilizan un conjunto de herramientas informáticas y cuentan con un importante parque informático de hardware y software para administrar y gestionar importante información de carácter público y para procesar información relacionados a la custodia, seguridad, gestión, transferencias y movimiento de caudales municipales, los cuales por el hecho mismo de ser información de carácter público amerita que debe ser protegida de las amenazas informáticas externas e ilegales, por lo que es necesario implementar políticas de seguridad informática e implementar

mecanismos de seguridad informática y así evitar la vulnerabilidad del sistema de información municipal.

En una sociedad globalizada donde se dan constantes cambios, las tecnologías de información y comunicación se caracterizan por ser tan dinámicos e innovadoras. En este contexto la seguridad informática en las instituciones públicas municipales se convierte en una herramienta tecnológica de mucha importancia para garantizar la seguridad de la gestión y uso de la información institucional pública municipal, al mismo tiempo se convierte en una necesidad prioritaria para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de las entidades públicas municipales. Cuando no se le da la importancia y prioridad a la seguridad informática, y especialmente cuando no se implementa los mecanismos de seguridad informática, nos enfrentamos ante una situación donde la información digital e institucional pública corre el riesgo de ser afectado, con graves consecuencias por la manipulación ilegal externa de la información institucional pública, por ello es necesario implementar con oportunidad y calidad los mecanismos de seguridad informática en general en las entidades públicas, y en particular en la Municipalidad Provincial de La Convención, especialmente en los órganos de apoyo dentro de la organización municipal, pues éstos órganos a través de las dependencias de recursos humanos, unidad de presupuesto, unidad de abastecimiento, unidad de contabilidad y unidad de tesorería, y operan sistemas informáticos gubernamentales con los cuales los sistemas administrativo ejecutan las distintas etapas del gasto público, para lo cual como herramienta utilizan los distintos módulos del sistema integrado de administración financiera- SIAF. Por lo que estos sistemas informáticos deben estar en continuos procesos de control y tratamiento apropiado en materia de seguridad informática y seguridad de la información.

Los mecanismos de seguridad informática en nuestros tiempos han tomado gran importancia, debido a las innovaciones y cambios tecnológicos en la automatización de la información, debido también a que en el mercado se ofertan y existe en disponibilidad nuevas plataformas tecnológicas. Así mismo la seguridad informática está en riesgo latente, por cuanto existen organizaciones criminales y

delictivas de personas dedicados a cometer delitos informáticos bajo diversas modalidades Desde luego las innovaciones tecnológicas y las actividades informáticas lícitas han permitido interconectarse a través de las redes permitiendo una mejora de los sistemas de trabajo e incidiendo en la productividad económica de las entidades públicas. Pero también estas innovaciones y cambios tecnológicos al mismo tiempo han motivado la aparición de nuevas amenazas y riesgos que pueden atacar, afectar y dañar los sistemas de información digital, poniendo en riesgo la seguridad del sistema de información digital de las entidades públicas, los cuales a su vez pueden afectar la estabilidad, funcionamiento y sostenibilidad de las organizaciones públicas.

Por ello en cuanto no se implementen los mecanismos de seguridad informática, la información institucional digital puede ser afectada y vulnerada por los ataques MITM (Man-in-the-Middle), por los ataques a protocolos de cifrado y los ataques malware. Ante tal situación las entidades públicas en general y en particular la Municipalidad Provincial de La Convención se ve en la imperiosa necesidad de implementar mecanismos de seguridad informática a través de protocolos de encriptación o cifrado, cambio de SSID (Service Set Identifier) y filtrar direcciones MAC (Mac Access Control).

La información digital que administran las organizaciones públicas municipales tiene un valor importante en el desarrollo de sus actividades, en la gestión pública, en la atención de los servicios públicos y en la atención a los ciudadanos, pues la información se convierte en un elemento valioso para los procesos productivos de bienes o servicios públicos en beneficio de los ciudadanos, y así atender las demandas y necesidades de los usuarios, de los ciudadanos y de los administrados, con lo que también se garantiza la calidad de los servicios públicos y el cumplimiento de las retribuciones económicas de parte de los ciudadanos por la prestación de los servicios públicos, por lo tanto, la organización pública municipal debe proteger la información institucional digital. Por tales consideraciones los sistemas de información digital es uno de los activos que requiere ser protegida de forma adecuada frente a cualquier amenaza que ponga en peligro la continuidad de

la prestación de los servicios públicos para los ciudadanos. Es por ello que las organizaciones públicas en general y en particular las municipalidades, están llamadas a diseñar políticas orientadas a gestionar el riesgo sobre la información y los sistemas que la procesan así como a diseñar sistemas eficientes para gestionar el riesgo de tales sistemas. Se inicia entonces, todo un proceso para gestionar la seguridad de la información. Estos riesgos que afrontan las organizaciones municipales hoy en día, han llevado a que éstas entidades desarrollen estrategias, metodologías y procesos técnico informáticos para gestionar con principio de previsión y seguridad todo el hardware y software municipal; por lo que es importante implementar las políticas de seguridad informática para evitar la vulnerabilidad de los sistemas de información; caso contrario puede generar graves y serios problemas a los servicios públicos que presta la organización municipal. En este sentido, los mecanismos de seguridad informática, surge como un instrumento y estrategia de la corporación municipal para persuadir a todos los trabajadores administrativos, acerca de la importancia y sensibilidad de la información digital; requiriéndose un alto compromiso de parte de la organización municipal para la implementación y renovación sostenida de los mecanismos de seguridad informática. Esta seguridad es más relevante considerando el crecimiento constante y sostenido de las plataformas tecnológicas gubernamentales, la gestión de los activos tangibles e intangibles como el hardware, el software, equipos de computación, equipos de red y telecomunicaciones, recurso humano entre otros, que pueden estar expuestos a situaciones de inseguridad. Finalmente por estas consideraciones expuestas y fundamentadas es imperativo y de necesidad e interés público que los trabajadores municipales conozcan la importancia de las políticas y mecanismos de seguridad informática a efectos de que los sistemas de información de la Municipalidad Provincial de La Convención no sean vulneradas por agentes y softwares externos, malignos e ilícitos.

Con estos fundamentos expuestos acerca del problema objeto de investigación, nos motiva a formular en forma clara el problema general y los problemas específicos de la investigación

1.2 Formulación del problema

1.2.1 Problema general

¿Qué mecanismos de seguridad informática nos permiten evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?

1.2.2 Problemas específicos

1. ¿Qué mecanismos de seguridad informática nos permiten evitar los ataques MITM (Man- in-the-Middle) en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?
2. ¿Qué mecanismos de seguridad informática nos permiten evitar los ataques a protocolos de cifrado en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?
3. ¿Qué mecanismos de seguridad informática nos permiten para evitar los ataques malware en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Conocer que mecanismos de seguridad informática nos permiten evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.

1.3.2 Objetivos específicos

1. Conocer que mecanismos de seguridad informática nos permiten evitar los ataques MITM (Man- in-the-Middle) en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.

2. Conocer que mecanismos de seguridad informática nos permiten evitar los ataques a protocolos de cifrado en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.
3. Conocer que mecanismos de seguridad informática nos permiten evitar los ataques malware en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.

1.4 Formulación de hipótesis

1.4.1 Hipótesis general

Los mecanismos de seguridad informática permitirían evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.

1.4.2 Hipótesis específicas

1. Los mecanismos de seguridad informática permitirán evitar los ataques MITM (Man- in-the-Middle) en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.
2. Los mecanismos de seguridad informática permitirán evitar los ataques a protocolos de cifrado en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.
3. Los mecanismos de seguridad informática permitirán evitar los ataques malware en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.

1.5 Justificación de la investigación

1.5.1 Académica

El desarrollo y ejecución de la investigación permitirá afianzar los conocimientos académicos de investigación en tecnologías de información y comunicación, y la

conclusión de la investigación va permitir optar al grado académico de bachiller en ingeniería de sistemas e informática.

1.5.2 Relevancia social

Contribuirá a conocer los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas, los cuales tienen incidencia de carácter social.

1.5.3 Conveniencia

Es conveniente realizar el estudio, por cuanto en la actualidad se desea conocer la importancia de los mecanismos de seguridad informática para garantizar la seguridad y buen uso de la información digital de carácter público.

1.5.4 Implicancias prácticas

Permitirá conocer las buenas prácticas informáticas para evitar que la información en las redes inalámbricas sea vulnerable.

1.5.5 Valor teórico

Contribuirá para conocer de qué manera los ataques informáticos pueden vulnerar la seguridad de la información digital, y a partir de ello se tenga y se tomen las previsiones del caso.

1.5.6 Utilidad Metodológica

Se puede diseñar una metodología, procedimientos y estrategias para crear nuevos instrumentos y mecanismos de seguridad informática, y evitar así la vulnerabilidad de la información digital.

1.5.7 Viabilidad o factibilidad

Existe información necesaria para cumplir con las metas que se tiene con la investigación, al mismo tiempo se cuenta con los recursos económicos, de tiempo y

logísticos necesarios para el logro de los objetivos planteados en la investigación. Por la situación de la pandemia utilizaremos las tecnologías de comunicación virtuales.

1.6 Alcances y limitaciones de la investigación

1.6.1 Alcance

La vulnerabilidad del sistema de información en las entidades públicas municipales producida por las diversas modalidades de ataques informáticos, es un problema que afecta la seguridad en la gestión de la información digital institucional. Por lo que es importante conocer los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020. Siendo este proceso de investigación una oportunidad para poner en prácticas todos aquellos conocimientos que hemos adquirido en la vida universitaria y profesional. Más aún, cuando la investigación permite la interacción con el conjunto de órganos y dependencias municipales que nos rodea en el proceso de investigación, y en dicho proceso dinámico adquirimos verdaderos conocimientos para ponerlos al servicio de la sociedad. La investigación nos permite vislumbrar, examinar y conocer algo nuevo o algo que se desconocía hasta un momento determinado, por eso que termina resultando importante en nuestra formación profesional.

En ese sentido la presente investigación nos permitirá conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención. Por lo que desarrollaremos capacidades y conocimientos para la búsqueda de posibles soluciones a problemas formulados; y así contribuir y garantizar la seguridad de la información digital institucional municipal.

1.6.2 Limitaciones

1.6.2.1 Limitación temporal

La investigación a nivel de elaboración de la tesina o proyecto de tesis se inicia en el 07 de noviembre 2020 y se concluye el 27 de marzo del 2021. A nivel de tesis se inicia en el mes de marzo y concluye en el mes de setiembre del 2021.

1.6.2.2 Limitación espacial

El ámbito físico geográfico, ciudad de Quillabamba, Distrito de Santa Ana, Provincial de La Convención, Región del Cusco

1.6.2.3 Limitación institucional

Municipalidad Provincial de La Convención

1.6.2.4 Limitación conceptual

El estudio se refiere a conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención.

1.6.2.5 Limitación Social

El estudio está circunscrito a los trabajadores de la Municipalidad Provincial de La Convención.

CAPÍTULO II. Marco teórico

2.1 Antecedentes de la investigación

INTERNACIONALES

"Tesis: PLAN DE SEGURIDAD INFORMÁTICO PARA MEJORAR LA CALIDAD EN EL SERVICIO DEL CALL CENTER DE LA EMPRESA Telsat Perú SAC", tesis para optar el título profesional de ingeniero de sistemas e informática. Universidad Nacional del Santa. Chimbote. La tesis plantea como problema general de investigación lo siguiente: ¿De qué manera el plan de seguridad informático mejorará la calidad en el servicio del call center de la empresa Telsat Perú SAC?, y como objetivo general se plantea lo siguiente: Proponer un plan de seguridad informático para mejorar la calidad en el servicio del call center de la empresa Telsat Perú SAC., y luego del estudio establece las siguientes conclusiones: Se propuso un Plan de Seguridad Informático, el cual permitió mejorar la calidad del servicio que brinda el call center de la empresa Telsat Perú SAC, aumentando las ventas en un 231.25%, disminuyendo las quejas en un 34.11%, las llamadas perdidas por falla en la red se redujeron en un 40.34%. Se realizó un análisis del estado en que se encontró la red informática de la empresa, detectándose fallas en la red informática y pérdidas de llamadas, determinando así los activos que tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos. Se identificaron las 11 secciones referidas a la seguridad informática a fin ser evaluadas y luego proponer controles que mejoren la Seguridad informática en la empresa Telsat Perú SAC. El Plan de Seguridad Informático propuesto, establece los mecanismos y requerimientos mínimos establecidos en los estándares desarrollados por los entes reguladores como el estándar de seguridad de información ISO /lEC 27002. Se implementó el Plan de Seguridad Informático en un 80% lo cual permitió definir las políticas de Seguridad Informática en la empresa, de esta manera asegurar la confidencialidad, integridad y disponibilidad de la información." (Angulo Castillo 2014)

"Tesis: DIAGNOSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN LOS SISTEMAS DE INFORMACIÓN PARA PROPONER SOLUCIONES DE

SEGURIDAD A LA RECTIFICADORA GABRIEL MOSQUERA S.A., tesis para optar el título de Ingeniero de Sistemas. Universidad Politécnica Salesiana - Guayaquil. La tesis plantea como problema general de investigación lo siguiente: ¿Por qué los procesos actuales de Seguridad Informática y la Información no son adecuados para la Empresa Rectificadora Gabriel Mosquera S.A.?, y como objetivo general se plantea lo siguiente: Identificar los procesos de Seguridad físicos y lógicos para la información que están implementados en la empresas de servicios para proceder a evaluar , formular , recomendar y plantear soluciones., y luego del estudio establece las siguientes conclusiones. Se cumple con el principal objetivo del proyecto que era realizar un diagnóstico de vulnerabilidades mediantes el análisis de riesgo y desarrollar un plan de seguridad para la información de la empresa Rectificadora Gabriel Mosquera S.A." (Karen Andrea Pintado, 2015)

"Tesis: ANÁLISIS DE VULNERABILIDAD DE REDES INALÁMBRICAS CON HERRAMIENTAS MITM., tesis para optar el título de Ingeniero en Sistemas Computacionales. Universidad Estatal de Milagro. La tesis plantea como problema general de investigación lo siguiente: ¿De qué manera las herramientas MITM vulneran las redes inalámbricas?, y como objetivo general se plantea lo siguiente: Determinar el grado de factibilidad de un ataque MITM de redes inalámbricas mediante Scripts., y luego del estudio establece las siguientes conclusiones. Mediante las pruebas realizadas con la herramienta fluxión en diferentes lugares del Cantón Milagro, las redes inalámbricas son muy vulnerables, a pesar de utilizar los diferentes tipos de proveedores de Internet (NETLIFE, CNT e INPLANET), modelos distintos de router (DLink 610, Cisco-Linksys E900, Huawei HG531s ,Huawei HG532s, Qpcom QP-WR227N, QP-WR330N), los cuales tenían diferentes protocolos de seguridad (WPA, WPA2), en todos las pruebas la víctima fue engañada, facilitando su contraseña de Red Wifi." (Chulli Paredes Jorge, 2019)

NACIONALES

"Tesis: SISTEMA DE GESTIÒN DE SEGURIDAD DE INFORMACIÒN PARA UNA INSTITUCIÒN FINANCIERA, tesis para optar el Título de Ingeniero Informático Universidad Católica Del Perú tesis plantea como problema general de

investigación lo siguiente: ¿De qué manera se implementará el modelo de sistema de gestión de seguridad de información (SGSI) en la institución financiera del Perú?, y como objetivo general se plantea lo siguiente: Proponer un modelo de sistema de Gestión de Seguridad de información (SGSI) en la Institución Financiera del Perú , y luego del estudio establece las siguientes conclusiones: obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución financiera." (AGUILAR, 2006)

"Tesis: METODOLOGÍA PARA UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TÉCNICA PERUANA NTP- 17799 EN LA ADMINISTRACIÓN DE LA MUNICIPALIDAD DISTRITAL DE LAMBAYEQUE SETIEMBRE 2013- FEBRERO 2014, tesis para optar el título profesional de Ingeniero de Sistemas. Universidad Nacional Pedro Ruiz Gallo. La tesis plantea como problema general de investigación lo siguiente: ¿Cuál es la situación actual de la municipalidad de Lambayeque en cuanto a seguridad de la información?, y como objetivo general se plantea lo siguiente: Formular una propuesta metodológica para un Sistema de Gestión de Seguridad de la Información bajo la Norma Técnica Peruana NTP 17799:2008 para la Municipalidad Distrital de Lambayeque, y luego del estudio establece las siguientes conclusiones: Con en el presente trabajo se pudo evidenciar que la Municipalidad de Lambayeque carece de políticas y controles eficientes en cuanto a la seguridad de la red, resguardo de la información y manejo de los riesgos a los que está expuesta. Se demostró que existe la factibilidad técnica, económica y operativa para realizar la Metodología para Sistemas de Gestión de Seguridad de la Información. La Metodología propuesta, permitirá brindar un esquema de seguridad más sólido y eficiente en el uso de los Sistemas de Información una vez implantado. Cabe destacar que la Seguridad de la Información no depende única y exclusivamente de la Metodología para Sistemas de Gestión de Seguridad faltaría la implantación, evaluación y mejoras a dicho plan." (Tarrillo Clavo y Correa Cubas. 2015)

"Tesis: APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA, tesis para optar el título Profesional de Ingeniero Informático Universidad Nacional de Piura tesis plantea como problema general de investigación lo siguiente: ¿ Cómo elaborar un plan de mejora de la seguridad de los activos de información en la Zona Especial de Desarrollo - ZED PAITA?, y como objetivo general se plantea lo siguiente: Aplicar la metodología MAGERIT para elaborar un Plan de Mejora de la Seguridad en los activos de información de la ZED PAITA., y luego del estudio establece las siguientes conclusiones: la metodología MAGERIT aportan una gran ayuda para todo el proceso de análisis de los riesgos, desde la identificación de los activos, la valorización de estos, la identificación de las amenazas." (Briceño Huaygua, 2019)

2.2 Bases teóricas

2.2.1 Identificación y conceptualización de variables

2.2.1.1 Mecanismos de seguridad informática

2.2.1.1.1 Seguridad

"Es un estado o situación personal que nos permite percibir que nos movemos en un espacio libre de riesgos reales o potenciales, la ausencia o la falta de esta puede originar diversos problemas y daños. Por lo tanto debemos entender que la seguridad está relacionada a la certidumbre y a la carencia de riesgo o contingencia, por cuanto no existiendo una certeza absoluta, el factor riesgo siempre estará latente, muy a pesar de las acciones tomadas, por lo tanto nunca existirá una seguridad absoluta". (Aspectos generales de la seguridad informática. 12 de diciembre 2020)

2.2.1.2 Definición de seguridad informática

"La seguridad informática hace referencia a todas las medidas y controles que se deben establecer para el aseguramiento de los sistemas informáticos, impidiendo que

intrusos internos o externos realicen procedimientos no autorizados sobre la red. La seguridad informática comprende la protección de:

1) **Aplicaciones**: Para evitar algún problema de seguridad informática las aplicaciones se deben de descargar en fuentes confiables y actualizarlas frecuentemente.

2) **Comunicaciones**: Es necesario evitar la interceptación de las comunicaciones haciendo uso de canales de comunicación cifrada, además de tener un constante control de las conexiones para impedir conexiones no autorizadas.

3) **Datos**: Para mantener protegidos los datos es necesario realizar constantemente copias de seguridad, el cifrado de la información, realizar un almacenamiento redundante de datos y deshabilitar componentes que supongan la entrada o salida de información no autorizada.

4) **Equipos**: Para evitar el robo de equipos se debe de cifrar los contenidos críticos, controlar o evitar los intentos de conexión de equipos externos no autorizados, y realizar mantenimientos preventivos.

La seguridad informática trata de mantener seguro la: Integridad, Privacidad, Disponibilidad, Control y Autenticidad de la información, que se encuentra almacenada en una computadora.

1) **Integridad**: Se encarga de garantizar que un mensaje o fichero no sea modificado desde su creación o durante su transmisión a través de una red informática hasta llegar al receptor.

2) **Confidencialidad**: Es la necesidad de garantizar que cada mensaje transmitido o almacenado en un sistema informático solo sea leído por el verdadero receptor. Si el texto llega al poder de terceras personas, éstas no podrán tener acceso al contenido del mensaje original.

3) **Disponibilidad**: Se encarga de garantizar la permanente disposición de los servicios a los que los usuarios deseen acceder.

4) **Control**: Permite asegurar que sólo los usuarios autorizados puedan decidir cuándo y cómo permitir el acceso a los servicios o información.

5) **Autenticidad**: Se encarga de garantiza que la identidad del creador de un mensaje o documento sea legítima. Para poder definir a un sistema informático como seguro debe de cumplir con los tres principios básicos de la seguridad de la información de acuerdo al estándar ISO 27002, es decir, mantener segura la integridad, confidencialidad y disponibilidad de la información La finalidad de la seguridad informática es proteger el almacenamiento, procesamiento y transmisión de la información digital en cualquier tipo de red informática para que no pueda ser interceptada por ningún tipo de intruso informático". (Segundo Galindo. J. 2017)

2.2.1.3 Objetivos de la seguridad informática

"Los principales objetivos de la seguridad informática en cualquier tipo de red son los siguientes:

1) Mantener protegida la información digital, el hardware y software de la red.

2) Asegurar el adecuado uso de los recursos y de las aplicaciones del sistema.

3) Identificar las vulnerabilidades con las que cuenta la red, para poder emplear métodos de prevención y de este modo poder proteger la información.

4) Asegurar la confidencialidad, integridad y disponibilidad en los sistemas informáticos.

5) Minimizar los riesgos, amenazas y vulnerabilidades que se encuentren en la red mediante uso de herramientas de protección.

6) Contar con métodos eficaces de acciones de recuperación del sistema en caso de un incidente de seguridad.

7) Evitar la fuga de información mediante el constante mantenimiento en la seguridad de la red informática". (Segundo Galindo. J. 2017)

2.2.1.4 Dimensiones de los mecanismos de seguridad informática

2.2.1.4.1 Dimensión de protocolos de encriptación o cifrado

"La encriptación o cifrado es un dispositivo informático de seguridad que permite variar un mensaje enviado, de modo que su texto sea ilegible, mas no para su verdadero destinatario. De modo contrario, la encriptación o descifrado admitirá a ser legible un texto que estaba cifrado. Utilizando la criptografía de clave pública el que emite el texto del mensaje cifrará el mensaje aplicando la clave pública del destinatario; por tanto el receptor es el único que podrá descifrar el texto mensaje utilizando la clave privada y personal". (Sede Electrónica. 12 de diciembre 2020)

"La encriptación, es un método de seguridad informática utilizada en archivos que tengan cierta antigüedad, que en la actualidad son utilizados con mucha frecuencia, sobre todo en los servicios de internet. La encriptación o cifrado de información, es un método que lo convierte totalmente ilegible la información de un documento o de cualquier tipo de información. De tal manera que los archivos se convierten fácilmente inservibles para un usuario que no está autorizado para verlo y leerlo; incluso si lo ha capturado o lo ha captado, si no tiene el password respectivo no logrará verlo ni leerlo. Este método de seguridad se hace uso para proteger archivos y documentos importantes que puede ser acopiada o remitida por medio del internet para cualquier diligencia o gestión. Se cuenta con muchos programas informáticos específicos con diseños especiales para efectuar encriptación de archivos; Windows tiene un instrumento con lo que se puede encriptar nuestros archivos de manera muy veloz y fácil". (¿Qué es encriptación o cifrado de archivos?, 12 de diciembre 2020)

2.2.1.4.2 Dimensión de cambio de SSID (Service Set Identifier)

"Es el nombre que identifica de la manera más ideal a una red inalámbrica. Los sitios de paso inalámbricos publican el Service Set Identifier para que los usuarios finales puedan conocer la red inalámbrica a la que se desean enlazarse. Distintos Service Set Identifier favorecen a coexistir a varias WLAN en el mismo espacio físico. Los

Service Set Identifier deben ser equivalente entre el sitio de acceso inalámbrico y el dispositivo de red inalámbrico para admitir el acceso a la red". (Glosario terminología informática. 12 de diciembre 2020)

"El Service Set Identifier) es una cadena de 0-32 octetos que contiene todas las partes de una red inalámbrica para identificarlos como parte de esa red. La contraseña consiste en un máximo de 32 signos, que en su generalidad son alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo Service Set Identifier. La difusión del Service Set Identifier es una forma de resguardar la red inalámbrica. Esta forma impedirá que otros usuarios descubran su Service Set Identifier o la identificación de red inalámbrica cuando pretendan ver las redes inalámbricas utilizables en su trabajo". (Wikipedia. El SSID. 12 de diciembre 2020)

2.2.1.4.3 Dimensión de filtrar direcciones MAC (Mac Access Control)

"El mecanismo de Mac Access Control no da la ocasión de acceder o frenar que determinadas computadoras con ciertas tarjetas de red se enlacen a internet a través de la red. Se trata de un procedimiento de revisión del acceso que te contribuirá a optimizar la seguridad en el enlace a internet. De esta manera, como el enlace a internet estará limitado a explícitas direcciones Mac Access Control, nadie podrá conectarse sin el debido permiso. El tamiz de direcciones Mac Access Control es mucho más seguro en las redes cableadas que en las redes inalámbricas, ya que en éstas últimas un atacador bandido puede percibir las comunicaciones. El filtrado de Mac Access Control del mismo modo suele usarse en ambientes con sitios de ingresos múltiples. De esta manera podemos impedir que las computadoras usuarias puedan informarse con otros usuarios inalámbricos y sólo lo realicen con la puerta de conexión determinada. Así se mejora la eficacia y el beneficio del acceso a la red. Finalmente, es relevante que no des tu dirección Mac Access Control a ninguna persona que no sea de tu entera confianza; pues se trata de un dato muy privado que sólo corresponde por motivos de seguridad al responsable de los equipo de computadoras." (Qué es una dirección MAC y cómo hacer filtrado de MAC. 12 de diciembre 2020)"

2.2.1.5 Vulnerabilidad del sistema de información en las redes inalámbricas.

2.2.1.5.1 Definición de vulnerabilidad

"En las diferentes clasificaciones y topologías de redes se pueden encontrar vulnerabilidades que de acuerdo con la Enciclopedia de la Seguridad informática el término de vulnerabilidad hace referencia a un estado viciado en un sistema informático que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. De acuerdo al estándar de la Organización Internacional para la Estandarización (ISO) 27001. La vulnerabilidad de un activo de seguridad es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información. Por lo tanto, la vulnerabilidad informática: es un estado, elemento o falla que puede ser ocupado por intrusos para causar algún daño en el sistema o red informática. Si un intruso hace uso de las vulnerabilidades encontradas en el sistema puede realizar diferentes actividades: Ejecutar comandos haciéndose pasar como otro usuario. Tener acceso a información confidencial del sistema informático y del usuario. Eliminar, modificar, monitorear información confidencial. Realizar denegación de servicios. Realizar daños en el hardware o software. Aumentar el riesgo de que la red informática pueda tener más vulnerabilidades.

Las vulnerabilidades tienen un ciclo de vida que se origina desde que se detectan, para luego basarse en la forma en la que un intruso explota las vulnerabilidades encontradas en la red informática, hasta llegar al momento en el que administrador de la red o el programador de la aplicación realiza actividades para llegar a una solución para tratar de disminuirlas o eliminarlas. La mayoría de las vulnerabilidades en un sistema pueden ser ocasionadas por fallas en el diseño o errores de programación e incluso por limitaciones tecnológicas, pero sin importar el tipo de vulnerabilidad estas pueden ser aprovechadas por los intrusos para causar cualquier tipo de daño". (Segundo Galindo. J. 2017)

2.2.1.5.2 Tipos de vulnerabilidades informáticas

"Las vulnerabilidades que pueden presentarse un sistema o red informática deben de tenerse en cuenta para la correcta detección de las mismas.

Comunicaciones o de red: Esta vulnerabilidad está presente al tener una serie de equipos de cómputo conectados entre sí existe la posibilidad de que un intruso acceda a solo uno de los equipos y posteriormente realizar su propagación en toda la red informática.

Emanaciones: Hace referencia a la posibilidad de interceptar radiaciones electromagnéticas para modificar o descifrar la información que es enviada y recibida de un receptor a un emisor. Físicas: Son cualquier posible acceso físico desde las instalaciones hasta el equipo de cómputo que almacena información confidencial para substraerla, modificarla o eliminarla. Es un tipo de vulnerabilidad que se puede llevar a cabo por el mismo personal interno que hace mal uso de las políticas de acceso al sistema informático y medios físicos de almacenamiento de información. Humanas: Son el tipo de vulnerabilidades más comunes en cualquier sistema, porque la falta de capacitación o información genera que los usuarios realicen actividades como el mal uso del equipo de cómputo o políticas de seguridad que den pauta a otros tipos de vulnerabilidades.

Hardware: Es la posibilidad de que alguna pieza física en el sistema informático falle (por un mal diseño, funcionamiento y uso), provocando daños o problemas mientras que se intenta arreglar la falla.

Naturales: Posibilidad de que el sistema informático sufra daños o perdidas causados por el ambiente o desastres naturales, como incendios, tormentas, inundaciones, terremotos. Este tipo de vulnerabilidad se presenta por la falta de medidas de prevención o auditorias de seguridad que revele algún tipo de deficiencia en el espacio geográfico en el que se encuentre ubicada la red informática. Software: Tiene vulnerabilidades conocidas como bugs que hace referencia a un error o defecto en el software provocando que deje de funcionar correctamente. Esta vulnerabilidad es ocupada frecuentemente por intrusos informáticos para lograr acceder al sistema.

Las vulnerabilidades son aprovechadas por intrusos para causar daños físicos y lógicos a un sistema informático, para disminuirlas es necesario realizar la detección de estás, mediante pruebas de infiltración, para mejorar la seguridad y confidencialidad de la información". (Segundo Galindo. J. 2017)

2.2.1.5.3 Detección de vulnerabilidades

"La detección de una vulnerabilidad se pueden identificar a través de un instrumento de detección, para ello se realiza un escaneo de puertos con la finalidad de contrastar cuales están accesibles para pretender lograr datos sobre el servicio que se encuentre circulando en ese instante y con esta información indagar vulnerabilidades coligadas justamente a esos servicios. Se tienen tres formas de detectarse: escáner de vulnerabilidades, análisis manuales y consultando información. Para el escáner de vulnerabilidades se tiene instrumentos como el Nikto la cual opera indagando deficiencias y errores en base a servidores. Otras herramientas son el Nessus y el Nmap. Una de las ventajas de la parte del escáner de vulnerabilidades, es que operan de forma automática, trabajan situando un rango de direcciones IP e inicia el escaneo, el aparato realiza todo el proceso de manera solo. Los análisis manuales son muy necesarios ejecutarlos, ya que, todos los estudios automáticos no revelan de forma automática todas las vulnerabilidades que se pueda tener en un sistema informático; por lo que es necesario efectuar ciertos análisis manuales dentro de las vulnerabilidades detectadas con el objetivo de impedir que se pueda evadir o dejar como cabo suelto. La consulta de información, es el elemento justamente de ocultar datos, se tiene alguna especie de Google hacking por así mencionarlo, o algo por el estilo, utilizar simple servicios, de lo que sería la búsqueda de datos y archivos en la red para poder realizar o encontrar información que pueda servir a la organización para la identificación de algunas vulnerabilidades que puedan contar todos los servicios informáticos". (Romero Castro, M.I. 2018)

2.2.1.6 Teoría general de sistemas

"Un sistema es la sumatoria de las partes de un todo que actúan recíprocamente entre sus elementos con la finalidad de lograr un objetivo previamente determinado. El

objetivo a lograr es la parte principal y la razón de la existencia de un sistema. Constituyen partes del sistema el nivel de complejidad y funcionamiento de los elementos que lo conforman y la correspondencia que concurren entre sus elementos de manera mutua. Los sistemas reciben ingresos o entradas en forma de datos, información, materias primas, energía y otros según la naturaleza del sistema, para luego procesar o transformarlos, y finalmente y proporcionan egresos o salidas que puede ser información, energía, productos, bienes o servicios para darle posterior utilidad. En el ámbito de la informática un sistema puede ser un ordenador o un software, los mismos que portan ingresos de datos, se procesa y se produce la información. Cada sistema se relaciona o se enlaza a otro sistema y a su vez está se contiene con otro sistema, a esto se le llama supra sistema". (Teoría general de los sistemas de información. 12 de diciembre 2020)

2.2.1.6.1 Partes del sistema

"Un sistema tiene las siguientes partes:

1. **Entradas, insumos o inputs**. Son procesos mediante el cual se incorpora información, energía o materia al sistema, los mismos que provienen del ámbito externo
2. **Salidas, productos u outputs**. Son resultados que se obtienen por la operación del sistema, los mismos que se destinan al ámbito externo
3. **Transformadores, procesadores o throughput**. Son acciones y actividades de funcionamiento del sistema, mediante el cual el sistema origina transformaciones, convirtiéndolos las entradas en salidas.
4. **Retroalimentación**. Son casos en el que el sistema convierte sus salidas en entradas de manera sistemática y sostenida
5. **Medio ambiente**. Es todo lo que rodea al sistema y existe fuera del mencionado sistema, lo cual a su vez forma parte de un sistema dentro de otro sistema y así de manera no determinada. A partir de este último factor, se reconocen tres tipos de sistemas:

   a) **Sistemas abiertos.** Cuando comparten información libremente con su medio ambiente.

b) **Sistemas cerrados.** Cuando no comparten información de ningún tipo con su medio ambiente. Son siempre sistemas ideales.

c) **Sistemas semi abiertos o semi cerrados.** Cuando comparten la menor información posible con su medio ambiente, sin llegar a ser cerrados". (Teoría de sistemas ¿Qué es la teoría de sistemas? 12 de diciembre 2020)

2.2.1.7 Sistemas de información

"Es el conjunto de elementos o partes de un todo que interactúan recíprocamente entre sí con la finalidad de apoyar las acciones y operaciones de una entidad pública o privada. La relevancia del sistema de información para las instituciones reside en el entorno en el que se desenvuelven, y que les permiten lograr prerrogativas de competitividad. Todo sistema aporta información cierta, pertinente, creíble que permite efectuar un examen y estudio adecuado de la información, lo cual conduce disminuir costos y optimizar procesos y procedimientos, el cual repercute en obtener ciertas prerrogativas competitivas en el mercado; convirtiéndose en sistemas de información estratégicos y trascendentales que contribuyen a una entidad a obtener una ventaja competitiva con su aporte a sus fines y objetivos estratégicos para incrementar y desarrollar su productividad y competitividad. Los sistemas de caracterizan porque proporciona una forma a las estrategias competitivas a una organización. Su principal función es obtener ventajas que los contrincantes no lo tienen; como costos, precios, servicios con proveedores. Los sistemas de información son forjadores de murallas de ingreso al giro o negocio.

Los sistemas contribuyen al proceso de invención y creación de nuevos bienes, servicios y métodos dentro de una organización, buscan ventajas, como crear nuevos productos y procesos. Los sistemas de información para lograr excelencias competitivas deben de acomodarse ágilmente a los cambios y a las necesidades de las entidades porque el entorno está en constante cambio. Es muy relevante almacenar la información existente que puede servir de sustento para otras circunstancias la disposición de un sistema de archivos informáticos, ya que simboliza un sistema aceptable para recobrar información y su gestión es tan valiosa como cualquier otro recurso de la empresa. Los sistemas computarizados también son muy relevantes para

suministrar información pertinente y cierto para la organización. En el mercado hay dispositivos de sistemas de información para ser utilizados en diversas áreas. Los sistemas de información se pueden instalar para monitorear, proceder según disposiciones preestablecidas y tomar decisiones". (Teoría general de los sistemas de información. 12 de diciembre 2020)

2.2.1.8 Red inalámbrica

"El concepto red se usa para designar al conjunto de los equipos informáticos interconectados que comparten servicios, información, transferencias y abonos de recursos, y otros de similar naturaleza. Por otro lado, el sistema inalámbrico, es un sistema de comunicación electrónica que no usa alambres o cables conductores; dicha comunicación se instala sin requerir cables que conecten físicamente los equipos informáticos. Una red inalámbrica, es aquella que admite enlazar varios nodos sin usar una unión física de equipos informáticos, sino instaurando la comunicación mediante ondas electromagnéticas. La emisión y la recepción de la información demandan dispositivos que actúan como puertos.

Las redes inalámbricas admiten implantar conexiones entre ordenadores y otros equipos de cómputo, sin que sea necesario instalaciones de cableado, lo que permite una mejor comodidad y un ahorro de recursos en locales e infraestructura. Así mismo podemos señalar aspectos importantes y ventajas que tiene cualquier instalación mediante una red inalámbrica; es así, que es muy sencilla de instalar, no lleva cableado, evita agujeros en las paredes de la infraestructura, son instalaciones más elegante, tiene buen estilo o apariencia, están conectados entre un número importante de dispositivos y computadoras, tablets, faxes, celulares, impresoras, fotocopiadores, equipos de diversa naturaleza, entre otros. Un aspecto negativo, es que este tipo de redes, tiene una seguridad menor y de posible vulnerabilidad, por cuanto, si no se le protege con cierta eficiencia y garantía, los intrusos ciberdelincuentes pueden ingresar y generar daños. Es relevante mencionar que para poder instalar y configurar una red inalámbrica, es necesario disponer de una serie de elementos que son totalmente necesarios. Así se requiere de un enrutador de tipo inalámbrico, conexión a internet con banda ancha, dispositivos de red inalámbrica y

un módem; solo así se podrá poner en operación la red. Par instalar se tiene que cumplir algunos pasos necesarios, tales como colocar el enrutador, reducir lo que son las interferencias, configurar la clave de seguridad que va a tener la red. De acuerdo al tipo de cobertura, la red inalámbrica puede clasificarse como Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN) o Wireless Wide Area Network (WAN). La red WPAN es frecuente en la tecnología Bluetooth**.** No obstante, también dentro de la red WPAN se recurre al uso de tecnologías tales como ZigBee y el infrarrojo para poder poner en funcionamiento lo que es cualquier red inalámbrica que se precie. Mientras, los sistemas WiFi suelen establecer redes WLAN**.** Las tecnologías basadas en WiMAX**,** por su parte, permiten establecer redes WMAN, mientras que las redes WAN se usan con comunicaciones GMS**,** HSPAo3G"**. (**Definición de red inalámbrica. 12 de diciembre 2020)

2.2.1.9 Ataques informáticos

"En la actualidad los dispositivos electrónicos (smartphones, tablets, laptops, desktops) están conectados a través de Internet, motivo por el cual los equipos de los usuarios son propensos a sufrir ataques informáticos en cualquier tipo de red. Un ataque informático es aquel que trata de aprovechar alguna falla o debilidad en el hardware o software, con el objetivo de causar algún tipo de daño o problemas específicamente a un sistema informático o red". (Segundo Galindo. J. 2017)

2.2.1.10 Clasificación de los ataques informáticos

"Los ataques informáticos se pueden clasificar en dos categorías como:

1. **Ataques físicos:** Se caracteriza por que la red puede sufrir algún tipo de daño causado por el entorno en el que se encuentre ubicada u ocasionada por el hombre. En esta categoría se puede encontrar con la amenaza de sufrir desastres naturales, que son eventos que ocasionan la pérdida de bienes, servicios, información, y alteraciones en el ambiente en el que suceden, por ejemplo:

- ✓ **Incendio:** Pueden ser ocasionados por la falla de instalaciones eléctricas defectuosas, uso inadecuado de materiales inflamables, por la falta de revisión y mantenimiento a las instalaciones. Algunas de las recomendaciones para minimizar el riesgo de un incendio en una red son: El área en la que se encuentren las computadoras debe evitar tener combustibles o inflamables. Contar con mecanismos de ventilación y detección de incendios. Revisar que la topología de la red no sobrecargue los enchufes con demasiadas clavijas, distribuir las cargas equitativamente. Tener un reglamento de seguridad que prohíba ingerir alimentos, bebidas y fumar dentro de la instalación. Antes de realizar alguna reparación de la instalación eléctrica, desconectar el interruptor general y compruebe la ausencia de energía, para evitar algún incidente.
- ✓ **Inundación:** Puede ser ocasionada por la falta de drenajes naturales o artificiales provocando la invasión de agua por excesos de escurrimiento superficial en la instalación.
- ✓ **Terremotos**: Son ocasionados por fenómenos sísmicos, en ocasiones son producidos a gran escala provocando la pérdida de vidas humanas, aparatos e información, pero la mayoría de las veces son producidos a una escala menor que solo es detectada por instrumentos muy sensibles.

2. **Disturbios o sabotaje:** Son ocasionados por personas que hacen uso de las computadoras, con el objetivo de causar algún daño en la red, para evitar la pérdida de información ocasionada por el sabotaje se recomienda el constante respaldo de la información en el sistema.

3. **Ataques lógicos:** Se caracteriza por que la red puede sufrir algún tipo de daño en el software o en la pérdida de información. En esta categoría se pueden clasificar en dos:

   Ataques pasivos: Caracterizada por obtener información mediante la monitorización de la red sin modificar la comunicación. Su principal objetivo es el análisis del tráfico para conocer todo lo que pasa por la red y la intercepción de datos para tener conocimiento de la información que se tiene guardada, que envía o recibe el usuario. La intercepción es un proceso en el cual un intruso

(persona, organización o software) capta la información que un emisor envía a un receptor, por lo tanto el intruso puede obtener información privada (contraseñas, claves bancarias) que suelen ser ocupados para otros fines. La intercepción es un ataque pasivo por lo que es difícil reconocer si algún usuario está siendo atacado al no producirse ninguna alteración en el sistema. Un método de prevención es el cifrado de la información que se envía a través de la red. Este ataque es contra la confidencialidad del usuario o red.

Ataques activos: Se caracteriza por que existe una modificación en el flujo de datos que se transmite y existen interrupciones, modificación y suplantación de identidad. La interrupción es un proceso en el cual un intruso destruye algún recurso del sistema o no permite que el usuario acceda a los recursos de la red (software, hardware), además de poder inhabilitar el acceso a la información, es decir que no se permite operar de forma normal el sistema. Este ataque es contra la disponibilidad de la información o red. Modificación es el proceso en el cual un intruso no solo ingresa sin autorización, sino que también puede realizar una alteración en la información que se envía o recibe a través de la red o realiza cambios en algún software provocando que funcione de forma diferente. Este ataque es contra la integridad del usuario o red. La Suplantación de identidad es un proceso en el cual un intruso trata de hacerse pasar por una identidad diferente, provocando diferentes daños por que el intruso puede acceder a los recursos privilegiados de la red con la identidad que fue robada. Este ataque es contra la autenticidad del usuario o red.

Cualquier tipo de red es vulnerable a sufrir ataques informáticos cuando la seguridad informática no está en constante actualización y mantenimiento. Es necesario mantener seguros o actualizar los dispositivos de conectividad que se emplean, usualmente son ocupados como medio de intrusión que podrían provocar daños a nivel software o hardware en la red". (Segundo Galindo. J. 2017)

2.2.1.11 Dimensiones de vulnerabilidad del sistema de información en las redes inalámbricas.

2.2.1.11.1 Ataques MITM (Man-in-the-Middle)

"Es un tipo de ataque que se caracteriza por interceptar la comunicación e información entre dos o más interlocutores, consiguiendo suplantar la identificación de uno o de otro de los interlocutores, hecho que ocurre según el interés del interceptador para ver y leer la información, o si quiere modificarla la comunicación a su libre antojo, de tal manera que las respuestas y comunicaciones recibidas pueden estar dadas por el atacante informático y no por el interlocutor válido y legítimo. Este ataque consiste en interceptar la comunicación entre dos o más interlocutores. Para ello, alguien anónimo llamado "X" se sitúa entre ambos e intercepta los mensajes de A hacia B, conociendo la información y a su vez dejando que el mensaje continúe su camino. Habitualmente este tipo de ataques son muy peligrosos y muy difíciles de descubrirlos**,** ya que uno de los propósitos del atacante es evitar que sea descubierto, para tal fin utilizan varias técnicas que hacen casi imposible la detección. Así la comunicación entre A y B ocurre de manera normal como si fuera legitima, sin embargo el atacante puede decidir si la comunicación interceptado continuará, si lo hará con la misma información o si lo hará con otro mensaje modificado que pudiera suponerle una ventaja o beneficio". (Instituto Nacional de Ciberseguridad- INCIBE. 14 de diciembre 2020)

"Un ataque Man in the Middle es la técnica mediante el cual un hacker entra en el tráfico de información de dos partes vinculadas entre sí en una información, fingiendo pasar por cualquiera de ellos, haciendo creer que se están comunicándose entre ellos, cuando en la realidad es el intermediario quien recibe la información.

El objetivo principal de los hackers es estar bien capacitado para entrar a la comunicación privada de una entidad pública o privada, y así poder manipular a su gusto y antojo, ya sea mediante coacciones o bajo la forma de eliminación de información, generando una auténtica anarquía informática en los sistemas de información. Aunque sean ataques disímiles para cada escenario, que pueden ser en

forma individual de manera organizada entre varias personas de forma concurrente. El más frecuente para atacar una página web o un sistema de información es incrustar un código malicioso en el equipo de la posible víctima, intentando llegar lo antes posible a la información que se desee atacar; para lo cual incluso el hacker puede utilizar otras técnicas y métodos maliciosos. Este ataque se caracteriza por ser intermediario cibercriminal o un programa malicioso, que se incrusta entre la víctima y la fuente de información, como cuentas bancarias, cuentas personales, cuenta institucional, correos, email y otras similares. Por ello la finalidad es interceptar, ver, leer o maniobrar de una manera muy efectiva los datos entre la víctima y su información, sin que nadie se dé cuenta, de que hay una tercera persona incluida en la operación. Para filtrarse en los sistemas de información, los hackers tienen varios métodos para indagar cualquier debilidad y aprovecharse de manera ilícita". (Rodríguez, Andrés. ¿Qué es un ataque Man in the Middle. 12 de diciembre 2020)

2.2.1.11.2 Ataques a protocolos de cifrado

"Es un protocolo abstracto o concreto que cumple funciones concernientes a la seguridad informática, implementando técnicas criptográficas. Un protocolo se refiere reglas de formalidad obligatorias que rigen los actos informáticos y describen la manera en que un algoritmo debe utilizarse. Un protocolo bien especificado contiene detalles de la estructura de la información y sus caracteres, sitio en el cual puede utilizarse para implementar versiones interoperables múltiples de un programa. Los protocolos criptográficos son utilizados ampliamente para transportar información de manera segura a nivel de aplicación y uso. Un protocolo criptográfico generalmente reúne por lo menos una de las siguientes características y procedimientos: Establecimiento de claves. Autenticación de entidades. Cifrado simétrico y autenticación de mensajes. Transporte de datos en forma segura a nivel de aplicación. Métodos de no repudio. Por ejemplo, Transport Layer Security (TLS) es un protocolo criptográfico utilizado en conexiones web (HTTP) seguras; posee un dispositivo de autenticación de entidades basado en el sistema X.509, una fase de arreglo de claves, en la cual se decide una clave de cifrado simétrico empleando

criptografía de clave pública; y una función de transporte de información de nivel de aplicación. Estos tres aspectos tienen interconexiones importantes.

El estándar TLS no provee soporte para no repudio. Hay otros tipos de protocolos criptográficos también e incluso el término mismo tiene varias interpretaciones distintas. Los protocolos criptográficos de aplicación utilizan con mucha frecuencia uno o más técnicas de conformidad a las claves, a los cuales a veces se los llama "protocolos criptográficos". De hecho, el TLS emplea el intercambio de claves de Diffie-Hellman, el cual si bien no forma parte del TLS, puede ser visto como un protocolo criptográfico por sí mismo para otras diligencias. Los protocolos criptográficos logran ser visualizados de manera formal en un nivel abstracto en algunas oportunidades. Una diversidad de protocolos criptográficos va más allá de los objetivos habituales de la confidencialidad de la información, integridad y autenticación a asegurar; también una pluralidad de otras peculiaridades deseadas de colaboración mediada por los ordenadores. Las firmas ciegas se puede utilizar para generar movimiento de dinero en efectivo de manera digital y portar credenciales digitales para mostrar que una individuo ostenta un cualidad o derecho, sin que se dé a conocer la identificación de la persona o las identificaciones de los terceros con los cuales esa persona llevo a cabo transacciones de manera virtual. El sellado de tiempo digital se puede utilizar para señalar que había información, incluso de carácter confidencial, en un determinado momento.

El cómputo multipartito seguro se puede utilizar para computarizar réplicas, como en el caso de las apuestas; para ello basándose en información de carácter confidenciales, de tal manera que una vez concluido el protocolo, los participantes solo conocen la entrada de datos que ellos llevaron a cabo y la respuesta. Las firmas innegables incluyen protocolos interactivos que le permite al firmante explicar un fraude y delimitar quienes pueden contrastar la firma. El cifrado prescriptible extiende el cifrado estándar haciendo matemáticamente improbable que un atacante evidencie la presencia de una comunicación de texto plano. Las mezclas digitales crean informaciones que son difíciles de rastrear en los sistemas informáticos. (Wikipedia. Protocolo criptográfico. 12 de diciembre 2020)

2.2.1.11.3 Ataques malware

"El ataque malware se refiere a un software que deteriora dispositivos informáticos, sustrae información e impone la anarquía en la comunicación digital. Existen varios tipos de malware, como virus, troyanos, spyware, ransomware y otros, sin embargo pueden ser advertidos con una óptima herramienta antimalware como AVG AntiVirus FREE. El malware va creado a menudo conjunto de hackers que generalmente buscan obtener ilegalmente dinero, para ello desarrollan el malware por su cuenta o comercializándolo al mejor comprador en la "red oscura". El malware se puede crear y utilizar como instrumento de protesta, como una forma de comprobar la seguridad informática; incluso como arma de guerra entre gobiernos. En cualquier situación, sea cual fuese el motivo de su creación, el malware siempre conjetura una noticia negativa en cuanto llegue hasta su computadora personal, y esa mala noticia es lo que se quiere impedir.

La siguiente relación detalla los tipos más comunes de malware, no obstante, existen muchos más:

Virus: Al igual que sus homónimos biológicos, los virus se incrustan a los archivos limpios y lo contaminan a otros archivos limpios; logran propagarse con total descontrol, logrando dañar las funciones esenciales de un sistema de informático, así como a descartar o invalidar archivos informáticos.

Troyanos: Este tipo de malware se hace pasar por software legítimo o se esconde en un programa genuino que se ha maniobrado. Actúan de manera discreta y crear puertas traseras en la seguridad para lograr el ingreso de otro malware. Spyware: este malware acecha desde la oscuridad y va tomando nota de lo que se hace en el internet, incluyendo, entre otras cosas, contraseñas, números de tarjetas de crédito y formas de navegación informática.

Gusanos: Los gusanos contaminan redes completas de dispositivos, que pueden ser de internet, mediante el uso de interfaces de red; para lo cual utilizan los equipos infectados para seguir atacando a otros dispositivos.

Ransomware: Este malware acostumbra a bloquear los equipos de cómputo y los archivos informáticos, y condicionan para borrarlo todo si no se paga un rescate de tipo económico.

Adware: Es un software de carácter publicitario, su naturaleza no es maliciosa, pero cuando es agresivo puede carcomer la seguridad con la única finalidad de mostrar anuncios, el cual puede apertura un camino simple a otros tipos de malware.

Botnets: Son redes de equipos informáticos contaminados y obligados a laborar en contubernio y bajo la orden de un atacante.

El ataque malware nos encamina al principio de prevenir más que curar, y evitar así software desagradable y extraños maliciosos que se presentan mediante el internet, en los correos electrónicos extraños, en perfiles falsos, en las ofertas tentadoras; siendo éstos las principales técnicas de propagación del malware. No es factible conocer qué avisos publicitarios son peligrosos, por lo que es mucho mejor bloquearlos todos mediante un bloqueador de anuncios fiable.

El malware puede hallarse en cualquier lugar, sin embargo, su presencia es más recurrente en sitios web con poca seguridad en el servidor, como los sitios web pequeños e internos. Si se circunscribe a los sitios grandes y reputados se reducirá en gran medida el riesgo de encontrarse con malware. Los hackers han encontrado modos de filtrar sus virus en todos los rincones de la web. Para conseguir una seguridad real, es necesario combinar unos hábitos en línea saludables con un software antimalware potente y fiable como AVG AntiVirus FREE, que detecta y detiene el malware antes de que infecte su PC, Mac o dispositivo móvil.”. (¿Qué es el malware? Cómo funciona el malware y cómo eliminarlo. 14 de diciembre 2020).

2.2.2 Operacionalización de variables

2.2.2.1 Operacionalización de la variable independiente: Mecanismos de seguridad informática

Variable Independiente	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítems de Reactivos	Escala de Valoración
Seguridad informática	"La seguridad informática hace referencia a todas las medidas y controles que se deben establecer para el aseguramiento de los sistemas informáticos, impidiendo que intrusos internos o externos realicen procedimientos no autorizados sobre la red…" Segundo Galindo. J. (Ob. Cit.)	Es el trabajo que realizan los trabajadores de la municipalidad responsables de conocer e implementar los mecanismos de seguridad informática, a través de los protocolos de encriptación o cifrado, cambio de SSID (Service Set Identifier) y filtraciones de direcciones MAC (Mav Access Control). Además fue evaluado mediante la escala de valoración, los mecanismos de seguridad informática en los niveles de nunca, casi nunca, a veces, casi siempre y siempre.	Protocolos de encriptación o cifrado	Ilegibilidad de los datos	1, 2, 3	N= Nunca CN= Casi Nunca AV= A Veces CS= Casi Siempre S= Siempre
				Seguridad de los archivos informáticos		
				Programas informáticos de seguridad		
			Cambio de SSID (Service Set Identifier)	Protección de la red	4, 5, 6	N= Nunca CN= Casi Nunca AV= A Veces CS= Casi Siempre S= Siempre
				Identificación de la red		
				Uso de la red		
			Filtrar direcciones MAC (Mac Access Control)	Conexión a internet	7, 8, 9	N= Nunca CN= Casi Nunca AV= A Veces CS= Casi Siempre S= Siempre
				Seguridad en el acceso a internet		
				Seguridad de los datos		

2.2.2.2 Operacionalización de la variable dependiente: Vulnerabilidad del sistema de información en las redes inalámbricas

Variable Dependiente	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítems de Reactivos	Escala de Valoración
Vulnerabilidad del sistema de información en las redes inalámbricas	"La vulnerabilidad informática es un estado, elemento o falla que puede ser ocupado por intrusos para causar algún daño en el sistema o red informática. Si un intruso hace uso de las vulnerabilidades encontradas en el sistema puede realizar diferentes actividades, como ejecutar comandos haciéndose pasar como otro usuario; tener acceso a información confidencial del sistema informático y del usuario; eliminar, modificar, monitorear información confidencial; realizar denegación de servicios; realizar daños en el hardware o software; y aumentar el riesgo de que la red informática pueda tener más vulnerabilidades…" Segundo Galindo. J. (Ob. Cit.)	Es el trabajo que realizan los trabajadores de la municipalidad responsables de conocer y evitar la vulnerabilidad de sistema de información en las redes inalámbricas, que se pueden darse a través de los ataques MITM (Man-in-the-Milddle), ataques a protocolos de cifrado y ataques malware. Además fue evaluado mediante la escala de valoración la vulnerabilidad del sistema de información en las redes inalámbricas, en los niveles de nunca, casi nunca, a veces, casi siempre y siempre.	Ataques MITM (Man-in-the-Milddle)	Interceptación de comunicación	1, 2, 3	N= Nunca CN= Casi Nunca AV= A Veces CS= Casi Siempre S= Siempre
				Suplantación de identidad		
				Tráfico ilegal de datos		
			Ataques a protocolos de cifrado	Averiguaciones al transporte de datos	4, 5, 6	N= Nunca CN= Casi Nunca AV= A Veces CS= Casi Siempre S= Siempre
				Averiguaciones a los caracteres de los datos e información		
				Descifrar mensajes informáticos		
			Ataques malware	Daño a dispositivos informáticos	7, 8, 9	N= Nunca CN= Casi Nunca AV= A Veces CS= Casi Siempre S= Siempre
				Sustraer datos informáticos		
				Virus informático		

2.3 Marco conceptual

- **Ataque informático:** "Es un intento planificado e intencionado ocasionado por una o más personas para causar deterioro y perjuicio o generar problemas a un sistema informático o red. Un ataque informático aprovecha cualquier debilidad o falla en el software, en el hardware y en las personas que forman parte de un ambiente informático; para obtener un beneficio, por lo general de tipo económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización. El ataque informático es una técnica mediante el cual un persona, mediante un software pretende usurpar el control, desestabilizar o dañar otro sistema informático de carácter formal y legal". (Ataque Informático. 11 de diciembre 2020)
- **Delitos informáticos:** "Son conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación". (Diario el peruano. Normas Legales. Ley de delitos informáticos N° 30096. 27 de setiembre 2013)
- **Encriptación:** "Es ocultar un mensaje con una contraseña. Desde un punto de vista informático consiste en aplicar un algoritmo asociado a una o varias contraseñas, que convierte la información en una cadena de letras, números y símbolos sin sentido". (Computer Hoy. Qué es la encriptación. 10 de diciembre 2020)
- **Entidad pública:** "Se considera Entidad pública a toda organización del Estado Peruano, con Personería jurídica de Derecho Público, creada por norma expresa en el que se le confiere mandato a través del cual ejerce funciones dentro del marco de sus competencias y atribuciones, mediante la administración de recursos públicos, para contribuir a la satisfacción de las necesidades y expectativas de la sociedad, y como tal está sujeta al control, fiscalización y rendición de cuentas".

(Presidencia del Consejo de Ministros. Municipio aldía. Concepto de Entidad Pública. 10 de diciembre 2020)

- **Estructura orgánica:** "La estructura orgánica es un instrumento de gestión que ayuda a definir con claridad las funciones de las diferentes unidades administrativas de una organización pública, privada o de otra índole". (Paredes A. y Asociados. Estructura Orgánica. 10 de diciembre 2020).
- **Filtrar:** "ES un programa diseñado para reconocer qué contenido se permite mostrar, principalmente para limitar el acceso a cierta información y datos de la web. El filtro establece qué compendio estará servible en una computadora o red particular. El filtro es para prevenir a las personas ver contenido que el propietario de la computadora u otras autoridades consideran censurable". (Wikipedia. Filtro de contenido. 10 de diciembre 2020)
- **Hardware y software:** "Hardware es el conjunto de componentes físicos de los que está hecho el equipo y software es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo". (GCFGlobal. ¿Qué es hardware y software? 10 de diciembre 2020).
- **Inalámbrico:** "El inalámbrico se usa en el ámbito informático para acceder a la conexión de nodos sin necesidad de una conexión utilizando cables, ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos". (Redes Inalámbricas. 10 de diciembre 2020)
- **Informática:** "La Informática es la rama de la ingeniería que estudia el hardware, las redes de datos y el software necesarios para tratar información de forma automática". (Escuela Superior de Ingeniería Informática. La informática. 10 de diciembre 2020)
- **Municipalidad:** "Es la institución del estado, con personería jurídica, facultada para ejercer el gobierno de un distrito o provincia, promoviendo la satisfacción de las necesidades de la población y el desarrollo de su ámbito". Es el órgano administrativo de los gobiernos locales. (Presidencia del Consejo de Ministros. Municipio al día. Quehacer Municipal. 10 de diciembre 2020)

- **Políticas de seguridad informática:** "Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan". (La Universidad en Internet. Políticas de seguridad informática. 10 de diciembre 2020)
- **Protocolo:** "Es un conjunto formal de estándares y normas que rigen tanto el formato como el control de la interacción entre los diferentes dispositivos dentro de una red o sistema de comunicación, permitiendo así que puedan transmitir datos entre ellos". (Lifeder.com. Protocolo en informática. 10 de diciembre 2020).
- **Red:** "Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc.". (Gorgona S. Luis. Teoría de redes de computadoras. 10 de diciembre 2020)
- **Seguridad informática:** "Es un procedimiento para prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de resguardo en contra de intrusos en el uso de nuestros equipos informáticos con propósitos maliciosas o con la finalidad de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente". (Universidad Internacional de Valencia. ¿Qué es la seguridad informática y como puede ayudarme? 10 de diciembre 2020).
- **Sistema:** "Es un conjunto de elementos conexos entre sí, y funciona como un todo completo. Si bien cada uno de los elementos de un sistema puede funcionar de forma independiente, siempre formará parte de una estructura mayor nivel. De la misma manera un sistema puede ser parte de otro sistema": (Significado de Sistema.15 de Octubre 2020)
- **Sistemas administrativos:** "Conjunto de elementos interrelacionados entre los que existe cohesión y unidad de propósito en la gestión administrativa. Comprende normas, técnicas, métodos y procedimientos que regulan los sistemas de abastecimiento, presupuesto, contabilidad, tesorería, personal, entre otros".

(Presidencia del Consejo de Ministros. Municipio aldia. Sistemas Administrativos. 10 de diciembre 2020)

- **Sistema informático:** "Es un sistema automatizado de almacenamiento, procesamiento y recuperación de datos, que aprovecha las herramientas de la computación y la electrónica para llevar a cabo su serie compleja de procesos y operaciones. En otras palabras, un sistema informático es un computador de alguna índole". (Sistema Informático. 10 de diciembre 2020).
- **Sistema Integrado de Administración Financiera-SIAF:** "Son sistemas informáticos que automatizan los proceso, procedimientos y trámites financieros, que son necesarios realizar para registrar los ingresos por fuentes de financiamiento, rubro y tipo de recursos; así como los diversos gastos que realiza la entidad pública". (Farías Pedro y Pimenta Carlos. Sistema Integrado de Administración Financiera. 10 de diciembre 2020).
- **Tecnologías de información y comunicación:** "Conjunto de tecnologías desarrolladas para administrar información y enviarla de un lugar a otro lugar. Comprende un abanico de tecnologías para acopiar datos y recuperarla después, remitir y recibir datos de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes y documentos". (Aprenda en Línea. Plataforma Académica para la Investigación. 10 de diciembre 2020)
- **Vulnerabilidad:** "Es una debilidad o fallo en un sistema de información que pone en peligro la seguridad de la información, archivos y datos, pudiendo permitir que un atacante pueda afectar la integridad, disponibilidad o confidencialidad de la misma, por lo que es importante encontrarlas y eliminarlas lo antes posible." (Instituto Nacional de Ciberseguridad. Amenazas versus vulnerabilidad. 10 de diciembre 2020).

CAPITULO III. Metodología de la investigación

3.1 Tipo o enfoque de la investigación

El presente estudio desde el enfoque de la finalidad es una investigación básica; desde el enfoque del diseño es una investigación no experimental; desde el enfoque del tiempo es una investigación transversal y desde el enfoque de su naturaleza es una investigación cuantitativa. “La investigación pura está destinada a aportar conocimiento generalizables. Es netamente intelectual o cognoscitiva, orientada a enriquecer el conocimiento teórico científico. La investigación no experimental se caracteriza porque el investigador no tiene control alguno de las variables independientes, se basa en la observación de los hechos, sin intervenir en el mismo. La investigación transversal es aquella investigación cuyo estudio se circunscribe a un momento temporal, un segmento del tiempo durante el año a fin de medir la situación en ese tiempo específico. La investigación es cuantitativa es cuando la preponderancia del estudio se basa en recoger y analizar datos para la cuantificación y cálculo de los mismos. Son los modelos más definidos.” (Rivas Yi, G.A. 2011).

3.2 Diseño de la investigación

El diseño de investigación del presente estudio es de carácter no experimental, pues observaremos los fenómenos objeto de estudio tal como se presentan en su contexto original, para luego estudiarlos. Es decir, es una investigación donde no hacemos variar intencionalmente las variables independientes. “El diseño de investigación es el conjunto de estrategias, procedimientos y metodologías definidas y elaboradas previamente para desarrollar el proceso de investigación.” (Carrasco 2015). En esta etapa el investigador determina el tipo de diseño a utilizar en su investigación con la finalidad de dar respuesta a problema planteado. “El diseño de investigación no experimental, son aplicables a las investigaciones cuyas variables independientes no se han manipulado. Se analizan y estudian los hechos y fenómenos de la realidad después de su ocurrencia.” (Carrasco 2015).Es no experimental porque en el trabajo

de investigación no se manipuló a las variables con las que se trabajó, tampoco se intervino para cambiar su comportamiento o las condiciones en que se manifiesta.

3.3 Alcance de la investigación

Por el nivel de rigurosidad y profundidad, la presente investigación es de alcance descriptivo y correlacional. “Un estudio es de alcance o de nivel descriptivo cuando nos relata acerca las peculiaridades, caracteres internas y externas, propiedades y rasgos esenciales de los hechos y fenómenos de la realidad, en un determinado momento y tiempo histórico concreto.” (Carrasco 2015). Es de alcance descriptivo porque se explica el problema que se encuentra tal cual se presenta en un lugar y periodo determinado. La investigación descriptiva se sustenta en técnicas como la encuesta, la entrevista, la observación. "Un estudio es correlacional, cuando su finalidad es conocer la relación o grado de asociación que concurre entre dos o más variables en un entorno en particular. Cuando las variables resultan correlacionadas, significa que al variar una variable también la otra variable varia, la mencionada correlación puede ser positiva o inversa. Si es positiva quiere decir que sujetos con altos valores en una variable tienden a revelar altos valores en la otra variable, si es inversa significa que sujetos con altos niveles en una variable tienden a revelar bajos valores en la otra variable, si no hay correlación entre ambas variables con ello se indica que éstas varían sin seguir un patrón sistemático entre sí.” (Hernández 2015).

3.4 Población y muestra

3.4.1 Descripción de la población

El universo total objeto de estudio está conformado por los 2,300 trabajadores de la Municipalidad Provincial de La Convención. Y la población con características muy similares y comunes, llamados unidades de muestreo, son todos los trabajadores vinculados a la gestión de los sistemas administrativos e informática, en ella se concentran 43 trabajadores.

3.4.2 Selección de la muestra

La muestra está determinado por el sub conjunto de los trabajadores de la Municipalidad Provincial de La Convención directamente que operan y administran los sistemas informáticos municipales que son 43 trabajadores, el cual ha sido seleccionado por muestreo no probabilístico sobre la cual se efectuará la observación o medición correspondiente. De esta muestra se seleccionó el tamaño muestral de 20 trabajadores mediante un muestreo no probabilístico, quienes aportarán la información más relevante a los propósitos de la investigación.

3.5 Recolección de datos

3.5.1 Diseño de instrumentos

Los instrumento de recolección de datos, son recursos del cual nos hemos servido como investigador para acercarnos a los fenómenos, y así extraer la información requerida. Los instrumentos de investigación utilizados están vinculados a las técnicas o procedimiento de investigación que hemos desarrollado en el proceso de investigación. En la presente investigación se utilizará las técnicas de las encuestas, observación, entrevistas, las fuentes documentales y el internet, y como instrumentos se utilizará cuestionarios, guías y fichas de observación, guías y fichas de entrevista, fichas bibliográficas y archivos informáticos. “Las técnicas son los procedimientos e instrumentos que utilizamos para acceder al conocimiento. Dentro de las cuales tenemos las encuestas, entrevistas, observaciones.” (Arias, F. 1974). “Los instrumentos son un conjunto de preguntas estructurados y no estructurados sobre los hechos y aspectos de una determinada realidad que interesan en una determinada investigación, para que sean contestados por la población o por una muestra representativa.” (Arias, F. 1974).

“La encuesta es una técnica de investigación muy apropiada, especialmente para la investigación social, debido a su utilidad, versatilidad, sencillez y objetividad de los datos que con ella se obtiene.” (Carrasco (2015).

La encuesta es una técnica que nos ha permitido la recolección de datos mediante un listado de preguntas estructuradas para ser tratada estadísticamente, desde una perspectiva cuantitativa. El instrumento utilizado fue el cuestionario con un conjunto de preguntas preparadas y estructuradas de acuerdo a los objetivos de la investigación y con una escala de apreciación y valoración

"La observación es una técnica que permite analizar, verificar y examinar con atención los acontecimientos que se suscitan y a partir de ello registrar la información que interesa a los objetivos de la investigación." (Carrasco (2015). Mediante la técnica de la observación nos ha permitido obtener información a través de la verificación de las diferentes características, tipologías, particularidades, circunstancias, manifestaciones, expresiones, fenómenos y hechos en el ámbito de estudio; se ha enfatizado la observación directa de manera sistematizada y controlada. El instrumento utilizado fueron las guías y fichas estructuradas y no estructuradas para registrar los hechos fácticos de los actores involucrados materia de investigación.

"La entrevista es una técnica mediante el cual se mantiene una conversación con una o varias personas para dar a conocer al interesado sus respuestas sobre algún asunto." (Carrasco 2015). Mediante la entrevista hemos establecido un dialogo y conversación con los actores involucrados intervinientes en el proceso de la investigación, los cuales nos han permitido precisar y aclarar las interrogantes materia de investigación y el logro de los objetivos de la investigación. El instrumento hemos utilizado fueron las guías y fichas estructuradas y no estructuradas para registrar la información alcanzada de parte de los informantes claves acerca del problema materia de investigación.

También hemos recurrido a las fuentes documentales, como una técnica de búsqueda de datos o temas publicados en los diferentes documentos escritos referidos en los temas y problema de investigación; para lo cual hemos utilizado como instrumento las fichas bibliográficas. Finalmente hemos recurrido a la técnica del internet con la finalidad de la búsqueda y selección de información en las distintas

páginas webs; para lo cual como instrumento utilizado los archivos informáticos. A continuación, ponemos a consideración la encuesta a aplicar en el proceso de la investigación; complementariamente se utilizará otros instrumentos de investigación como guías y fichas de observación, guías y fichas de entrevista, fichas bibliográficas y archivos informáticos.

ENCUESTA

UNIVERSIDAD PRIVADA LÍDER

PERUANA

ESCUELA DE PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

CUESTIONARIO DE LA VARIABLE INDEPENDIENTE: SEGURIDAD INFORMÁTICA

Título de Tesis: Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020

Objetivo de Investigación: Conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.

Estimada autoridad, funcionario y/o servidor municipal, el presente cuestionario contiene un conjunto de proposiciones que describen el grado de conocimiento de los mecanismos de seguridad informática en la Municipalidad, para ello debe responder con la mayor sinceridad y objetividad posible a cada una de las preguntas, en concordancia a cómo piense o actúe. El cuestionario está compuesto por un total de 09 ítems; los cuales tienen una escala de valoración. Recuerde que no hay respuestas buenas o malas, todas son de gran utilidad. Responde todas las preguntas con un aspa (X), y debe de marcar una sola respuesta por cada ítem

Leyenda de la escala de valoración: N= Nunca, CN= Casi Nunca, AV= A Veces, CS= Casi Siempre, S= Siempre

DATOS GENERALES:

Cargo: ……Profesión: ……Años de servicios en el sector público: …… Condición Laboral: ……Edad: ……Sexo: ……

Ítem	**Cuestionario de Preguntas**	**Escala de Valoración**				
	Dimensiones: 03	**N**	**CN**	**AV**	**CS**	**S**
	Variable Independiente: Seguridad Informática					
Protocolos de encriptación o cifrado						

01	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de encriptación o cifrado es un procedimiento que lo vuelve completamente ilegible los datos de un documento y lo vuelve prácticamente inservible para un usuario no autorizado a leerlo, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
02	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de encriptación o cifrado es un sistema de seguridad de mucha utilidad para resguardar información importante que puede ser almacenada o enviada vía internet para cualquier trámite, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
03	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de encriptación o cifrado permiten utilizar programas especialmente diseñados para realizar encriptación de archivos, fácil y rápidamente, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
	Cambio de SSID (Service Set Identifier)					
04	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de cambio de SSID (Service Set Identifier) protegen su red inalámbrica para preservar la información que se tiene, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
05	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de cambio de SSID (Service Set Identifier) difunden adecuadamente el SSID para que los usuarios finales puedan					

	identificar y proteger la red local inalámbrica a la que desean conectarse, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
06	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de cambio de SSID (Service Set Identifier) protegen la red para evitar que otros usuarios ajenos detecten y utilicen su SSID o el nombre de la red inalámbrica para fines que no corresponden, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
	Filtrar direcciones MAC (Mac Acces Control)					
07	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de filtrar direcciones MAC te da la oportunidad de permitir o impedir que determinados ordenadores con determinadas tarjetas de red se conecten a internet a través de su red, y que se pueda evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
08	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de filtrar direcciones MAC son un sistema de acceso que te ayudará a mejorar la seguridad en el acceso a internet, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
09	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de filtrar direcciones MAC le da seguridad a los datos privados que solo concierne por razones de seguridad al administrador de tus ordenadores, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					

ENCUESTA

UNIVERSIDAD PRIVADA LIDER

PERUANA

ESCUELA DE PROFESIONAL DEINGENIERIA DE SISTEMAS E INFORMÁTICA

CUESTIONARIO DE LA VARIABLE DEPENDIENTE: VULNERABILIDAD DEL SISTEMA DE INFORMACIÓN EN LAS REDES INALÁMBRICAS

Título de Tesis: Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020

Objetivo de Investigación: Conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020

Estimada autoridad, funcionario y/o servidor municipal, el presente cuestionario contiene un conjunto de proposiciones que describen el grado de conocimiento de la vulnerabilidad del sistema de información en las redes inalámbricas en la Municipalidad, para ello debe responder con la mayor sinceridad y objetividad posible a cada una de las preguntas, en concordancia a cómo piense o actúe. El cuestionario está compuesto por un total de 09 ítems; los cuales tienen una escala de valoración. Recuerde que no hay respuestas buenas o malas, todas son de gran utilidad. Responde todas las preguntas con un aspa (X), y debe de marcar una sola respuesta por cada ítem

Leyenda de la escala de valoración: N= Nunca, CN= Casi Nunca, AV= A Veces, CS= Casi Siempre, S= Siempre

DATOS GENERALES:

Cargo: ……Profesión..... Años de servicios en el sector público: ……Condición Laboral: ……..……Edad: ……Sexo: ……

Ítem	**Cuestionario de Preguntas**	**Escala de Valoración**				
	Dimensiones: 03	**N**	**CN**	**AV**	**CS**	**S**

	Variable Dependiente: Vulnerabilidad del sistema de información en las redes inalámbricas					
	Ataques MITM (Man –in-the- Middle)					
01	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos MITM (Man –in-the- Middle) pueden interceptar la comunicación entre dos o más interlocutores, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
02	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos MITM (Man –in-the- Middle) pueden suplantar la identidad de uno u otro según se requiera para ver la información y modificarla a su antojo, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
03	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos MITM (Man –in-the- Middle) es un tráfico ilícito de datos de dos partes vinculados entre sí en una comunicación, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
	Ataques a protocolos de cifrado					
04	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos a protocolos de cifrados son averiguaciones que realizan los hackers acerca del transporte de datos a nivel de aplicación utilizando programas informáticos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
05	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos a protocolos de cifrados son averiguaciones que realizan los hackers. Acerca de los caracteres de la confidencialidad, integridad y autenticación de los datos e					

	información para fines ilícitos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
06	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos a protocolos de cifrados son averiguaciones que realizan los hackers para descifrar los mensajes de texto plano o contraseñas de seguridad, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
	Ataques malware					
07	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos malware son software que dañan dispositivos y siembra el caos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
08	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos malware son software que sustraen datos e información para fines ilícitos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
09	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos malware son virus que se adhieren e infectan a archivos limpios, llegando a dañar las funciones esenciales de una data, y que pueden vulnerar el sistema de información de las redes inalámbricas?					

3.5.2 Aplicación de instrumentos

3.5.2.1 Diseño del material

El material para la aplicación de los instrumentos previamente se planificará y se organizará, para lo cual se ha considerado el problema materia de investigación, los objetivos, hipótesis y las variables de la investigación, se diseñó adecuadamente los

contenidos y preguntas de las encuestas, se prepararon las guías y fichas de observación, fichas y guías de entrevistas, fichas bibliográficas y se acumularon en archivos informáticos.

3.5.2.2 Recolección de datos

Para la recolección de datos de desarrollará las siguientes acciones:

- Preparación de las técnicas e instrumentos de recolección de datos.
- Remisión oficio a la entidad municipal, comunicando el inicio del proceso de investigación
- Aprobar la validez y confiabilidad de los instrumentos de investigación.
- Recolección de datos propiamente dicho, para lo cual se procedió con la aplicación de cuestionario de preguntas a los trabajadores
- Analizar los datos obtenidos mediante los cuestionarios, a través de procedimientos estadísticos.
- Desarrollar diálogos y conversaciones con los actores involucrados intervinientes en el proceso de la investigación, los cuales permitieron contribuir a precisar y aclarar las interrogantes materia de investigación.
- Entrevistas con los informantes claves.
- Observación y verificación de las características y hechos en el ámbito de estudio.
- Recolección y selección de documentos bibliográficos acerca de las variables de estudio, los mismos que son parte del marco teórico.
- Recolección y selección documentaria acerca de la problemática de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en la Municipalidad Provincial de La Convención.
- Recolección y selección de información de páginas web e internet.
- Recolección y selección bibliográfica de acerca de los documentos técnicos, legales y administrativos de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información.

3.5.2.3 Procesamiento de datos

El procesamiento de datos se realizará de la siguiente manera:

- Revisión y control de los datos recopilados.
- Codificación de los datos recopilados.
- Tabulación de las encuestas por medio de herramientas informáticas y estadísticas.
- Almacenamiento de los datos en hojas de cálculo y programas estadísticos.
- Preparación y sistematizar la información para facilitar su análisis posterior.
- Evaluación y selección de los paquetes estadísticos en relación lógica al tipo de investigación.
- Utilización de herramientas informáticas y software como Excel y Word.
- Procesamiento informático de los datos recopilados.
- Redacción de los resultados del procesamiento de datos.

CAPÍTULO IV. Aspecto administrativo

4.1. Cronograma de actividades

N°	Actividades	Cronograma																			
		Semanas/Mes																			
		Del 07 al 14-11-20	Del 15 al 21-11-20	Del 22 al 28-11-20	Del 29-11 al 05-12-20	Del 06 al 12-12-20	Del 13 al 19-12-20	Del 20 al 22-12-20	Del 23 al 26-12-20	Del 27-12-2020 al 02-01-21	Del 03 al 09-01-21	Del 10 al 16-01-21	Del 17 1l al 23-01-21	Del 24 al 30-01-21	Del 31-01-21 al 06-02-21	Del 07 al 13-02-21	Del 14 al 20-02-21	Del 21 al 27-02-21	Del 28-02 al 06-03-21	Del 07 al 13-03-21	Del 14-al 20-03-21	Del 21 al 27-03-21
I Etapa de investigación																					
01	Planificación de las actividades de investigación	X	X																		
02	Organización de las actividades de investigación	X	X																		
03	Control y seguimiento a las actividades de investigación	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
04	Ejecución de las actividades de investigación			X	X	X															
05	Finalización de las actividades de investigación					X	X														
II Etapa académica administrativa																					
01	Trámites administrativos en la Universidad			X	X	X								X	X	X	X	X	X	X	
02	Pagos de derechos en la Universidad			X	X	X								X	X	X	X	X	X	X	

03	Entrega de la tesina o proyecto de tesis a la Universidad							X														
04	Evaluación y revisión de la tesina de parte de la Universidad							X	X	X	X	X	X	X	X	X	X	X	X	X		
05	Levantamiento de observaciones en caso de existir																			X		
06	Aprobación del trabajo de investigación																				X	
07	Programación y sustentación del trabajo de investigación																				X	
08	Entrega del grado académico de bachiller																					X

4.1.1 Cronograma de actividades para la elaboración de la tesis

N°	Actividades	Cronograma						
		Meses/Año						
		Marzo 2021	Abril 2021	Mayo 2021	Junio 2021	Julio 2021	Agosto 2021	Setiembre 2021
I Etapa de Planificación de la Investigación:								
01	Coordinaciones administrativa y académicas con la universidad	X	X	X	X	X	X	
02	Revisar de la normatividad interna de la universidad	X	X					
03	Reunión con interesado para coordinar, sensibilizar, internalizar y comprometer en el proceso de investigación	X	X	X				
04	Proceso de organización y planificación para la elaboración de la tesis	X	X					
05	Determinación de la línea de investigación con el tesis	X	X					
06	Programación de los recursos para la investigación	X	X					
07	Implementación de técnicas y herramientas para la investigación	X	X	X				
08	Revisión e identificación del marco teórico	X	X					
09	Reunión con el tesista para determinar las variables y el problema de investigación	X	X					
10	Reunión con el tesista para la elaboración de la tesis	X	X	X	X	X	X	
11	Elaboración del plan de tesis	X						
II Etapa de Ejecución de la Investigación:								

A. Etapa de Investigación:								
01	Redacción del problema objeto de investigación de la tesis		X	X				
02	Redacción del marco teórico de las variables de investigación de la tesis		X	X				
03	Redacción de la metodología de la investigación de la tesis		X	X				
04	Desarrolla las técnicas e instrumentos de investigación de la tesis		X	X				
05	Recolección y procesamiento los datos de origen primario y secundario de la tesis		X	X	X			
06	Redacción de la tesis			X	X			
B. Etapa Académica Administrativa:								
01	Trámites administrativo en la universidad		X	X	X	X	X	
02	Presentación de la tesis				X			
03	Designación de asesor de tesis	X	X					
04	Revisión y observación de la tesis				X	X		
05	Levantamiento de observaciones de la tesis					X		
06	Aprobación de la tesis					X		
07	Presentación de la tesis en forma definitiva					X		
08	Designación de dictaminantes de la tesis					X		
09	Revisión y observación a la tesis de parte de los dictaminantes					X	X	
10	Levantamiento de observaciones a tesis						X	
11	Sustentación de la tesis						X	

12	Obtención de grado académico de bachiller							X

4.2. Recursos humanos y materiales

Grado de Instrucción	Cantidad	Capacidades y competencias	Cargo	Disponibilidad de tiempo
Profesional	01	Conocimientos en investigación científica	Asesor Universitario	Completa
Profesional	01	Conocimientos en investigación científica	Asesor particular	Parcial
Egresada Universitaria	01	Conocimientos básicos en investigación	Tesista	Completa

4.2.1. Recursos materiales

Tipo de Materiales	Cantidad	Unidad de Medida
Uso de Equipos de Computo	02	Unidad
Uso de Equipos de impresora	01	Unidad
Uso de Muebles	02	Unidad
Uso de Equipos de filmación	01	Unidad
Uso de Equipos de grabación	01	Unidad
Compra de textos	03	Unidad
Compra de materiales de escritorio	10	Unidad

4.2.2. Presupuesto

I Presupuesto de Ingresos:					
N°	Fuente de Financiamiento (1)	Unidad de Medida (2)	Cantidad (3)	Precio Unitario (4)	Presupuesto (5)=(3)x(4)
01	Aporte propio en dinero efectivo	Desembolso	01	8,000.00	8,000.00
02	Aporte propio valorizado en recurso tiempo	Hora	500	50.00	2,500.00
Total Ingresos					**10,500.00**
II Presupuesto de Gastos:					
N°	Detalle (1)	Unidad de Medida (2)	Cantidad (3)	Precio Unitario (4)	Presupuesto (5)=(3)x(4)
Bienes:					
01	Compra de textos	Unidad	03	150.00	350.00
02	Compra de materiales de escritorio	Unidad	10	20.00	200.00
Servicios:					
02	Asesoramiento y elaboración externa de tesina	Servicio	01	4,200.00	4,200.00

	Servicio de alquiles de equipos	Servicio	01	500.00	500.00
03	Movilidad local	Mes	06	50.00	300.00
04	Alimentación y refrigerios	Mes	06	50.00	300.00
06	Servicio de redacción de texto en formato APA	Servicio	01	200.00	200.00
07	Servicios de internet	Hora	100	1.00	100.00
08	Servicio de impresión	Hoja	1000	0.10	100.00
09	Servicio de fotocopiado	Hoja	3000	0.10	300.00
10	Servicio de anillado	Unidad	06	5.00	30.00
11	Servicio de empastado	Unidad	05	40.00	200.00
12	Pago de derecho de graduación	Pago	01	2,000.00	2,000.00
13	Pago de derechos de constancias y otros de la Universidad	Pago	05	100.00	500.00
14	Gastos sociales en sustentación de tesina	Servicio	01	820.00	820.00
15	Gastos de imprevistos	Imprevistos	04	100.00	400.00
Total Gastos					**10,500.00**

5. Bibliografías

Angulo Castillo, Alexa Madelyn (2014). Tesis: Plan de seguridad informático para mejorar la calidad en el servicio del call center de la empresa Telsat Perú SAC". Tesis para optar el título profesional de ingeniero de sistemas e informática. Universidad Nacional del Santa. Chimbote

Aprenda en Línea. Plataforma Académica para la Investigación. (10 de diciembre 2020). Obtenida en http://aprendeenlinea.udea.edu.co/lms/investigacion/mod/page/view.php?id=3118#:~:text=%22Las%20Tecnolog%C3%ADas%20de%20la%20Informaci%C3%B3n,abanico%20de%20soluciones%20muy%20amplio.&text=F%C3%A1cil%20acceso%20a%20todo%20tipo,tipo%20de%20proceso%20de%20datos.

Arias, Fernando (1974). Introducción a la técnica de investigación en ciencias de la administración y del comportamiento, México, Trillas.

Aspectos generales de la seguridad informática. (12 de diciembre 2020). Obtenida en http://repositorio.utc.edu.ec/bitstream/27000/536/1/T-UTC-1052%281%29.pdf

Ataques informáticos. (11 de diciembre 2020). Obtenida en https://www.ecured.cu/Ataque_inform%C3%A1tico#:~:text=Un%20ataque%20inform%C3%A1tico%20consiste%20en,del%20sistema%2C%20que%20luego%20pasa

Aguilar, Moisés Antonio Villena (2006) Tesis: Sistema de gestión de Seguridad de información para una Institución financiera. Obtenida en: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/362/VILLENA_MOIS%C3%89S_SISTEMA_DE%20GESTI%C3%93N_DE_SEGURIDAD_DE_INFORMACI%C3%93N_PARA_UNA_INSTITUCI%C3%93N_FINANCIERA.pdf?sequence=1&isAllowed=y

Briceño Huaygua, Cristhian Abijail (2019) .Tesis: APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA. Obtenida en: https://repositorio.unp.edu.pe/bitstream/handle/UNP/2061/INF-BRI-HUA-2019.pdf?sequence=1&isAllowed=y

Chulli Paredes Jorge, Espinosa Plaza Bryan (2019) .Tesis: Análisis de Vulnerabilidad de redes inalámbricas con Herramientas MITM. tesis para optar el título de Ingeniero en Sistemas Computacionales. Universidad Estatal de Milagro , Obtenida en: http://repositorio.unemi.edu.ec/bitstream/123456789/4460/1/AN%C3%81LISIS%20DE%20VULNERABILIDAD%20DE%20REDES%20INAL%C3%81MBRICAS%20CON%20HERRAMIENTAS%20MITM.pdf

Carrasco, S. (2015). Metodología de la Investigación (9na. Ed.). Lima Perú. Edit. San Marcos de Aníbal Jesús Paredes Galván

Computer Hoy. Qué es la encriptación. (10 de diciembre 2020). Obtenida en https://computerhoy.com/noticias/software/que-es-encriptacion-como-encriptar-tu-ordenador-movil-tablet-35047#:~:text=Encriptar%20o%20cifrar%20una%20informaci%C3%B3n,n%C3%BAmeros%20y%20s%C3%ADmbolos%20sin%20sentido.

Dávila Hurtado, Edson Alberto y Correa Cubas, Juan Carlos (2015). Tesis: Metodología para un sistema de gestión de la seguridad de la información basado en la norma técnica peruana NTP- 17799 en la administración de la municipalidad distrital de Lambayeque setiembre 2013- febrero 2014. Tesis para optar el título profesional de ingeniero de sistemas. Universidad Nacional Pedro Ruiz Gallo. Lambayeque

Definición de red inalámbrica. (12 de diciembre 2020). Obtenida en https://definicion.de/red-inalambrica/

Diario el Peruano Normas Legales. Ley de delitos informáticos N° 30096, de fecha 27 de setiembre 2013

Escuela Superior de Ingeniería Informática. La Informática. (10 de diciembre 2020). Obtenida en https://www.informatica.us.es/index.php/conoce-tu-futura-escuela/la-informatica#:~:text=La%20Inform%C3%A1tica%20es%20la%20rama,sigue%20leyendo%20un%20poco%20m%C3%A1s.

Farías Pedro y Pimenta Carlos. Sistema Integrado de Administración Financiera. (10 de diciembre 2020). Obtenida en http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/08B8FDE2C856ADB705257ABD005EE899/$FILE/104_pdfsam_.pdf

GCFGlobal. ¿Qué es hardware y software?. (10 de diciembre 2020). Obtenida en https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/

Gorgona S. Luis. Teoría de redes de computadoras. (10 de diciembre 2020). Obtenida en https://www.oas.org/juridico/spanish/cyber/cyb29_computer_int_sp.pdf

Glosario terminología informática. (12 de diciembre 2020). Obtenida en http://www.tugurium.com/gti/termino.php?Tr=Service%20Set%20Identifier

Hernández, R., Fernández, C & Baptista, P. (2010) Metodología de la investigación. México DF: Mc Graw Hill Interamericana

Instituto Nacional de Ciberseguridad. Amenazas versus vulnerabilidad. (10 de diciembre 2020). Obtenida en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

Instituto Nacional de Ciberseguridad- INCIBE. (14 de diciembre 2020). Obtenido en https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

Karen Andrea Pintado, Cesar Luis Urtado (2015).Tesis: DIAGNOSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN LOS SISTEMAS DE INFORMACIÓN PARA PROPONER SOLUCIONES DE SEGURIDAD A LA RECTIFICADORA GABRIEL MOSQUERA S.A. Obtenida en : https://dspace.ups.edu.ec/bitstream/123456789/10349/1/UPS-GT001276.pdf

La Universidad en Internet. Políticas de seguridad informática. (10 de diciembre 2020). Obtenida en https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/#:~:text=Las%20pol%C3%ADticas%20de%20seguridad%20inform%C3%A1tica%20consisten%20en%20una%20serie%20de,las%20pol%C3%ADticas%20de%20seguridad%20inform%C3%A1tica%3F

Lifeder.com. Protocolo en informática. (10 de diciembre 2020). Obtenida en https://www.lifeder.com/protocolo-informatica/#:~:text=El%20protocolo%20en%20inform%C3%A1tica%20es,puedan%20transmitir%20datos%20entre%20ellos.

Paredes A. y Asociados. Estructura Orgánica. (10 de diciembre 2020). Obtenida en https://alfredoparedesyasociados.com/estructura-organica-y-funcional/

Presidencia del Consejo de Ministros. Municipio aldia. Quehacer Municipal. (10 de diciembre 2020). Obtenida en https://municipioaldia.com/municipalidades-del-peru/

Presidencia del Consejo de Ministros. Municipio aldia. Concepto de Entidad Pública. (10 de diciembre 2020). Obtenida en https://municipioaldia.com/normaslegales/norma-legal-40041106/

Presidencia del Consejo de Ministros. Municipio aldia. Sistemas Administrativos. (10 de diciembre 2020). Obtenida en https://municipioaldia.com/organizacion-municipal/administracion-municipal/sistemas-administrativos/#:~:text=El%20sistema%20administrativo%20es%20el,Personal%2C%20Abastecimientos%2C%20entre%20otros.

¿Qué es encriptación o cifrado de archivos?. (12 de diciembre 2020). Obtenida en https://culturacion.com/que-es-encriptacion-o-cifrado-de-archivos/

Qué es una dirección MAC y cómo hacer un filtrado de MAC. (12 de diciembre 2020). Obtenida en https://www.gadae.com/blog/direccion-mac-filtrado-mac/

¿Qué es el malware?. Cómo funciona el malware y cómo eliminarlo. (14 de diciembre 2020). Obtenida en https://www.avg.com/es/signal/what-is-malware

Rivas Yi, Gisella Aurora (2011) Metodología de la Investigación Científica. Edit. UAP. Lima. Perú

Redes Inalámbricas. (10 de diciembre 2020). Obtenida en https://redesinalambricasmonterrey1.wordpress.com/tipos-de-redes-inalambricas/concepto/

Rodríguez, Andrés. ¿Qué es un ataque Man in the Middle. (12 de diciembre 2020). Obtenida en https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/

Romero Castro, Martha Irene. Manabi. Ecuador. Edit. Área de Innovación y Desarrollo, S.L. (12 de diciembre 2020). Obtenida en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Sede Electrónica. (12 de diciembre 2020). Obtenida en https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/-

/asset_publisher/1RphW9IeUoAH/content/1024-que-es-la-encriptacion-o-cifrado-?inheritRedirect=false#:~:text=La%20encriptaci%C3%B3n%20o%20cifrado%20es,un%20mensaje%20que%20estaba%20cifrado.

Segundo Galindo, Janeth (2017). Tesis: Propuesta de prevención de ataques informáticos de una red LAN, mediante el escaneo de vulnerabilidades. Tesis para optar el título de ingeniero en computación. Universidad Autónoma del Estado de México. Atlacomulco México

Significado de Sistema (15 de Octubre 2020). Obtenida en https://www.significados.com/sistema/

Sistema Informático. (10 de diciembre 2020). Obtenida en https://www.caracteristicas.co/sistema-informatico/

Tarrillo Clavo, Edsson Alberto y Correa Cubas, Juan Carlos (2015). Tesis: Metodología para un sistema de gestión de la seguridad de la información basado en la norma técnica peruana NTP- 17799 en la administración de la municipalidad distrital de Lambayeque setiembre 2013 - febrero 2014. Tesis para optar el título profesional de ingeniero de sistemas. Universidad Nacional Pedro Ruiz Gallo. Facultad de ingeniería civil, sistemas y arquitectura. Escuela profesional de ingeniería de sistemas

Teoría general de los sistemas de información. Sara Rivera, Isaura. (12 de diciembre 2020) Obtenida en https://es.slideshare.net/isara1/teoria-general-de-los-sistemas-de-informacion

Teoría de sistemas ¿Qué es la teoría de sistemas?. (12 de diciembre 2020). Obtenida en https://concepto.de/teoria-de-sistemas/#ixzz6gYID8Fc6

Universidad Internacional de Valencia. ¿Qué es la seguridad informática y como puede ayudarme?. (10 de diciembre 2020). Obtenida en

https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Wikipedia. Filtro de contenido. (10 de diciembre 2020). Obtenida en https://es.wikipedia.org/wiki/Filtro_de_contenido#:~:text=En%20inform%C3%A1tica%2C%20un%20filtro%20de,una%20m%C3%A1quina%20o%20red%20particular.

Wikipedia. El SSID. (12 de diciembre 2020). Obtenida en https://es.wikipedia.org/wiki/SSID

Wikipedia. Protocolo criptográfico. (12 de diciembre 2020). Obtenida en https://es.wikipedia.org/wiki/Protocolo_criptogr%C3%A1fico

ANEXOS

ENCUESTA

UNIVERSIDAD PRIVADA LIDER PERUANA

ESCUELA DE PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

CUESTIONARIO DE LA VARIABLE INDEPENDIENTE: SEGURIDAD INFORMÁTICA

Título de Tesis: Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020.

Objetivo de Investigación: Conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.

Estimada autoridad, funcionario y/o servidor municipal, el presente cuestionario contiene un conjunto de proposiciones que describen el grado de conocimiento de los mecanismos de seguridad informática en la Municipalidad, para ello debe responder con la mayor sinceridad y objetividad posible a cada una de las preguntas, en concordancia a cómo piense o actúe. El cuestionario está compuesto por un total de 09 ítems; los cuales tienen una escala de valoración. Recuerde que no hay respuestas buenas o malas, todas son de gran utilidad. Responde todas las preguntas con un aspa (X), y debe de marcar una sola respuesta por cada ítem

Leyenda de la escala de valoración: N= Nunca, CN= Casi Nunca, AV= A Veces, CS= Casi Siempre, S= Siempre

DATOS GENERALES:

Cargo: ……Profesión: ……Años de servicios en el sector público: …… Condición Laboral: ……Edad: ……Sexo: ……

Ítem	**Cuestionario de Preguntas**	**Escala de Valoración**				
	Dimensiones: 03	**N**	**CN**	**AV**	**CS**	**S**
	Variable Independiente: Seguridad Informática					
Protocolos de encriptación o cifrado						

01	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de encriptación o cifrado es un procedimiento que lo vuelve completamente ilegible los datos de un documento y lo vuelve prácticamente inservible para un usuario no autorizado a leerlo, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
02	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de encriptación o cifrado es un sistema de seguridad de mucha utilidad para resguardar información importante que puede ser almacenada o enviada vía internet para cualquier trámite, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
03	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de encriptación o cifrado permiten utilizar programas especialmente diseñados para realizar encriptación de archivos, fácil y rápidamente, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
	Cambio de SSID (Service Set Identifier)					
04	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de cambio de SSID (Service Set Identifier) protegen su red inalámbrica para preservar la información que se tiene, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
05	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de cambio de SSID (Service Set Identifier) difunden					

	adecuadamente el SSID para que los usuarios finales puedan identificar y proteger la red local inalámbrica a la que desean conectarse, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
06	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de cambio de SSID (Service Set Identifier) protegen la red para evitar que otros usuarios ajenos detecten y utilicen su SSID o el nombre de la red inalámbrica para fines que no corresponden, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
	Filtrar direcciones MAC (Mac Acces Control)					
07	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de filtrar direcciones MAC te da la oportunidad de permitir o impedir que determinados ordenadores con determinadas tarjetas de red se conecten a internet a través de su red, y que se pueda evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
08	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de filtrar direcciones MAC son un sistema de acceso que te ayudará a mejorar la seguridad en el acceso a internet, y que se puede evitar los ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					
09	¿La Municipalidad le ha puesto en su conocimiento, si los protocolos de filtrar direcciones MAC le da seguridad a los datos privados que solo concierne por razones de seguridad al administrador de tus ordenadores, y que se puede evitar los					

	ataques informáticos y la vulnerabilidad de la información en las redes inalámbricas?					

ENCUESTA

UNIVERSIDAD PRIVADA LIDER PERUANA

ESCUELA DE PROFESIONAL DEINGENIERIA DE SISTEMAS E INFORMÁTICA

CUESTIONARIO DE LA VARIABLE DEPENDIENTE: VULNERABILIDAD DEL SISTEMA DE INFORMACIÓN EN LAS REDES INALÁMBRICAS

Título de Tesis: Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020

Objetivo de Investigación: Conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020

Estimada autoridad, funcionario y/o servidor municipal, el presente cuestionario contiene un conjunto de proposiciones que describen el grado de conocimiento de la vulnerabilidad del sistema de información en las redes inalámbricas en la Municipalidad, para ello debe responder con la mayor sinceridad y objetividad posible a cada una de las preguntas, en concordancia a cómo piense o actúe. El cuestionario está compuesto por un total de 09 ítems; los cuales tienen una escala de valoración. Recuerde que no hay respuestas buenas o malas, todas son de gran utilidad. Responde todas las preguntas con un aspa (X), y debe de marcar una sola respuesta por cada ítem

Leyenda de la escala de valoración: N= Nunca, CN= Casi Nunca, AV= A Veces, CS= Casi Siempre, S= Siempre.

DATOS GENERALES:

Cargo: ……Profesión: ……Años de servicios en el sector público: ……Condición Laboral: ……..……Edad:..... Sexo: ……

Ítem	Cuestionario de Preguntas	Escala de Valoración				
	Dimensiones: 03	N	CN	AV	CS	S
	Variable Dependiente: Vulnerabilidad del sistema de información en las redes inalámbricas					
	Ataques MITM (Man –in-the- Middle)					
01	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos MITM (Man –in-the- Middle) pueden interceptar la comunicación entre dos o más interlocutores, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
02	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos MITM (Man –in-the- Middle) pueden suplantar la identidad de uno u otro según se requiera para ver la información y modificarla a su antojo, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
03	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos MITM (Man –in-the- Middle) es un tráfico ilícito de datos de dos partes vinculados entre sí en una comunicación, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
	Ataques a protocolos de cifrado					
04	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos a protocolos de cifrados son averiguaciones que realizan los hackers acerca del transporte de datos a nivel de					

	aplicación utilizando programas informáticos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
05	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos a protocolos de cifrados son averiguaciones que realizan los hackers acerca de los caracteres de la confidencialidad, integridad y autenticación de los datos e información para fines ilícitos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
06	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos a protocolos de cifrados son averiguaciones que realizan los hackers para descifrar los mensajes de texto plano o contraseñas de seguridad, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
	Ataques malware					
07	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos malware son software que dañan dispositivos y siembra el caos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
08	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos malware son software que sustraen datos e información para fines ilícitos, y que pueden vulnerar el sistema de información de las redes inalámbricas?					
09	¿La Municipalidad le ha puesto en conocimiento, que si los ataques informáticos malware son virus que se adhieren e infectan a archivos limpios, llegando a dañar las funciones esenciales de una					

	data, y que pueden vulnerar el sistema de información de las redes inalámbricas?					

Gracias por su atención. Quillabamba, diciembre 2020

Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENCIONES
Problema General	**Objetivo General**	**Hipótesis General**	**Variable Independiente**: Seguridad Informática	Filtrar direcciones MAC (Mac Access Control)
¿Qué mecanismos de seguridad informática nos permiten evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?	Conocer que mecanismos de seguridad informática nos permiten evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020	Los mecanismos de seguridad informática permitirían evitar la vulnerabilidad del sistema de información en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020		Protocolos de encriptación o cifrado
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Especifico**		Cambio de SSID (Service Set Identifier)
¿Qué mecanismos de seguridad informática nos permiten evitar los ataques MITM (Man- in-the-Middle) en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?	Conocer que mecanismos de seguridad informática nos permiten evitar los ataques MITM (Man- in-the-Middle) en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020	Los mecanismos de seguridad informática permitirán evitar los ataques MITM (Man- in-the-Middle) en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.	**Variable Dependiente:** Vulnerabilidad del sistema de información en las redes inalámbricas	Ataques MITM (Man-in-the-Milddle)
¿Qué mecanismos de seguridad informática nos permiten evitar los ataques a protocolos de cifrado en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?	Conocer que mecanismos de seguridad informática nos permiten evitar los ataques a protocolos de cifrado en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020	Los mecanismos de seguridad informática permitirán evitar los ataques a protocolos de cifrado en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.		Ataques a protocolos de cifrado
¿Qué mecanismos de seguridad informática nos permiten para evitar los ataques malware en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020?	Conocer que mecanismos de seguridad informática nos permiten evitar los ataques malware en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020.	Los mecanismos de seguridad informática permitirán evitar los ataques malware en las redes inalámbricas de la Municipalidad Provincial de La Convención, periodo 2020		Ataques malware