# ESCUELA MILITAR DE CHORRILLOS
# “CORONEL FRANCISCO BOLOGNESI”


## ESTÁNDARES DE CIBERSEGURIDAD Y LOS SISTEMAS INFORMÁTICOS EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" AÑO 2021

**Tesis para optar el Título Profesional de Licenciado en Ciencias Militares con Mención en Ingeniería**

**Autores**

**Victor José Chinchay Diaz**
**0000-0002-7605-3104**
**Flor Bárbara Gamarra Rojas**
**0000-0003-4593-5048**

**Asesores**

**Mg. Carlos Villanueva Del Castillo**
**0000-0002-8929-7175**
**Mg. Janette De Los Milagros Alva Navarro**
**0000-0003-3391-1065**

**Lima – Perú**

**2021**

## DEDICATORIA

Ante todo, queremos agradecer a Dios todopoderoso por guiarnos por un buen camino, nunca abandonarnos para seguir en pie y avanzar con todas nuestras metas propuestas.

A nuestros padres que son el aliento, motivación, apoyo para seguir adelante y sobre son nuestros guías para realizar las acciones correctas.

Y por último agradecemos infinitamente a todos nuestros asesores, profesores e instructores que nos dieron en todo momento su apoyo para poder concluir esta presente investigación.

## AGRADECIMIENTO

Queremos dar a conocer nuestro agradecimiento en primer lugar a Dios, por su apoyo incondicional porque con él ha sido posible todo este trabajo y gracias a él somos lo que somos y hemos logrado tanto.

Damos infinitas gracias a nuestros padres quienes han sido nuestros guías y motivación para lograr está presente investigación.

También expresar nuestros más sinceros agradecimientos a nuestros asesores Dra. Janette de los Milagros Alva Navarro y Crl(R) Villanueva del Castillo Carlos por siempre brindarnos su apoyo y ayuda para poder concluir esta tan importante investigación la cual es demasiada significativa en nuestra trayectoria profesional.

# RESUMEN

La presente investigación titulada: Estándares de ciberseguridad y los sistemas informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" AÑO 2021; considera dentro de su objetivo principal, determinar cuál es la importancia de los Estándares de Ciberseguridad en los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021.

El método de estudio tiene un enfoque cuantitativo, con un diseño no Experimental, con una población objetiva de 64 cadetes de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" involucrados en el tema de la investigación, con la aplicación de una encuesta para determinar los objetivos de la investigación y comprobar las hipótesis específicas y la hipótesis

general.

Durante el desarrollo de esta presente investigación se llegó a la conclusión general la gran importancia y la toma de conciencia que debemos llegar a tener para la Ciberseguridad, los riesgos que tiene los Sistemas Informáticos y más en un ente militar como lo es la EMCH "CFB", es por eso que se plantea el Estándar de Ciberseguridad 27032, el cual sí le dará un valor agregado y un mejor

concepto y conocimiento a cada usuario.

Como parte final del estudio se exponen las conclusiones y recomendaciones, las cuales son propuestas factibles que se relacionan a la investigación planteada.

# ABSTRACT

This present entitled: Standards of cybersecurity and computer systems at the Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" YEAR 2021; considers within your primary objective, determine what is the importance of the Cybersecurity Standards in Information Systems in the Military School of Chorrillos Coronel Francisco Bolognesi, year 2021.

The study method has a quantitative approach, with a design not Experimental, with a target population of 64 cadets from communications from the Military School of Chorrillos "Coronel Francisco Bolognesi" involved in the subject of the investigation, with the application of a survey to determine the objectives of the research and test specific hypothesis and hypothesis general.

During the development of this present investigation, the general conclusion the great importance and awareness that we must have for Cybersecurity, the risks that it has Information Systems and more in a military entity such as the EMCH "CFB", that is why the Standard of Cybersecurity 27032, which will give you added value and better concept and knowledge to each user.

As a final part of the study, the conclusions and recommendations, which are feasible proposals that relate to the proposed investigation.

# ÍNDICE GENERAL

# INTRODUCCIÓN

En toda organización o institución los sistemas informáticos tienen un alto valor de riesgo por las diferentes amenazas que existe en el ciberespacio y miles de riesgos a través de los cuales pueden ser afectados, las necesidades con respecto a los Estándares de Ciberseguridad en las Instalaciones de la Escuela Militar de Chorrillos, son de amplia importancia, porque muy aparte que le damos un valor agregado a la Institución, esta daría a los integrantes de la Escuela Militar de Chorrillos conocimiento, concientización para prever diferentes tipos de peligros a lo que somos expuestos.

Capitulo I. “El Problema” en este punto se describe de forma clara y concisa el motivo de esta investigación, asi como un enfoque a lo nos estamos enfrentando, objetivos planteados, y una manera adecuada solución acorde a las necesidades de la misma Institución.

Capitulo II. “Marco Teórico”, dentro de este contenido abarcamos los fundamentos teóricos para tener un entendimiento claro y comprender de manera adecuada y precisa nuestro que se ha plantead, además en este punto analizamos el apoyo científico que nos ha servido de guía durante el desarrollo de dicha investigación.

Capitulo III. “Metodología”, en este presente capitulo se indicará todas las metodologías a seguir en la investigación, aparte se menciona las técnicas e instrumentos que se usaron para recolectar y procesar información y por último contiene el proceso que se siguió para el desarrollo de la investigación.

Capitulo IV. “Resultados”, en este capítulo se da a conocer las conclusiones de la investigación, asi como las recomendaciones que se pueden dar para que se ejecute lo planteado.

# CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

## 1.1. Descripción de la problemática

Dentro de la Organización Internacional de Normalización, se creó el estándar 27032, con un enfoque en la ciberseguridad, uno de los mayores riesgos que enfrentan las empresas y organizaciones de todo el mundo en la actualidad. Aunque también contamos con la norma 27001 que se enfoca en la seguridad de la información, la Organización Internacional de Normalización decidió crear un principio enfocado en la ciberseguridad para darle más importancia y tranquilidad a las diversas empresas y organizaciones que existen hoy en día alrededor del mundo.

Los riesgos de la ciberseguridad son las preocupaciones más importantes para las empresas, el 95% de la incidencias en ciberseguridad se deben a errores humanos, es por eso que se ve conveniente y una forma mucho más eficaz para las empresas fortalecer sus mecanismos y protocolos de seguridad informática, y por eso vemos que la ISO 27032 ofrece el uso de buenas prácticas en materia de seguridad de la información, permite contar con procesos de protección de operaciones, de los software, manejo de datos y capacitar a todo el personal a cargo de estas herramientas, ya que son las mayores incidencias que se ven a nivel mundial.

La concientización que se debe tener surge a raíz de todos los informes que se van dando sobre los ciberataques ocurridos. Según el Instituto Nacional de Ciberseguridad (INCIBE), en 2018 tramitó cerca de 120.000 incidentes relacionados con ataques informáticos contra particulares y organizaciones en España.

Además, en 2018, el 95% de los incidentes de ciberseguridad fueron causados por error humano, según a IBM X-Force. Por este motivo, las empresas no solo deben preocuparse por los ciberdelincuentes sino también por sus empleados. En contraste, la encuesta estatal de seguridad de la información de PwC de 2018 reveló que las empresas enfrentan 3.4 incidentes de seguridad cibernética anualmente. Estos incidentes de seguridad global causaron $ 4.8 millones en pérdidas.

A consecuencia de esto es que el 49% de directivos tiene claro que sus empresas tienen la falta de un plan integral de seguridad informática.

Por otro lado, las debilidades, falta de conocimiento, la poca importancia que se le da a la ciberseguridad en los sistemas informáticos ha llevado que desde ya hace mucho tiempo se tenga un sinfín de ataques cibernéticos.

En 1999 durante el ataque contra la Agencia de Reducción de Amenazas del Departamento de Defensa en EEUU, una oficina encargada de contrarrestar las amenazas de armas nucleares, biológicas y químicas, robó nombres de usuario y contraseñas y más de 3.000 correos electrónicos, es por eso que sabemos que los sistemas informáticos son demasiados vulnerables.

Tenemos los estándares de seguridad de la red 27001, 27017 y 27018, para mejorar la seguridad de la red de los servicios en la nube, en la nube y actualmente se almacenan en muchas informaciones, por lo que debe ser un receptor que se desplaza más importante y establecido estándares de seguridad de la red en todas las organizaciones. Se han observado miles de ataques en todo el mundo, virus, virus, caballos de troyanos, estafas, ransomware, por eso decimos que decimos que los ataques informáticos son uno de los que están disponibles la amenaza más grande para las empresas y el mundo que actualmente afecta a las personas, las empresas e incluso estado personal. y la sociedad.

Sistemas de información se hallan declaraciones sobre: Bencomo (2012), indicando los sistemas de información son procedimientos técnicos sociales, ya que, además de la tecnología, los factores humanos necesitan, donde trabajan juntos. Se necesitan en incertidumbre, esta complejidad y cambio, que constituyen un elemento básico de la sociedad de la información en la que estamos orientados en la dirección del conocimiento.

Algunos factores a menudo debilitan los sistemas de información en el momento del despliegue, la falta de actualizaciones de software utilizadas y la resistencia a los cambios de los miembros de la organización. El siguiente elemento ocurrió en los Centros de Investigación de la Universidad de Zulia, que significa

actualizar sistemas, encontrar información a través de una herramienta de recopilación de datos de escala Likert dirigida a centros de administradores e institutos de investigación de la Universidad de Zulia.

Algunas tapas de la computadora en uso de calidad, así como su importancia, Morera (2006), estableciendo que la calidad de los sistemas de información debe considerarse responsable compartida por todos los usuarios internos de la organización. La necesidad de agregar que los sistemas de información pueden cerrar los empleos importantes en programas de calidad porque están estrechamente vinculados al trabajo diario en todas las áreas de una organización. El sistema de información es muy complejo y también soluciones para problemas de calidad. Es relevante mencionar que la introducción de los sistemas de información debe ser un fuerte impacto en el comportamiento organizacional. Los sistemas de información varían en sus entradas y salidas, en el tipo de tratamiento y en su estructura. Procesamiento o proceso de datos: para convertirlos en información útil para los usuarios aplicando los procesos más adecuados diseñados por los fabricantes del sistema de información. Funciones de los sistemas de información sobre datos acumulativos: o la recopilación de información debe ser procesada, almacenada y distribuida, de modo que deben conectarse con una forma estable y confiable (Bencomo, 2012).

Según Rodríguez y Laureo (2003), un sistema de información integral para una organización es una herramienta compleja que incluye un gran número de partes o subsistemas, interactuando entre sí a un nivel diferente, incluida la estructura. Hay una vertical y horizontal. Los sistemas de información tienen diferentes niveles de jerarquías:

1. Niveles operativos: donde los procedimientos periódicos se manejan relacionados con diferentes actividades de la organización.

2. Niveles tácticos: cuando se requieren decisiones específicas a corto plazo para que se preparen a partir de datos de transacción o fuentes externas.

3. Nivel estratégico: se implementan decisiones de mayor y largo plazo, respaldando menos en la información oficial de 169 datos de transacciones y dependiendo de gran medida de las fuentes de información externas.

Dieron a conocer, Rodríguez y Daureo (2003), que una organización generalmente tiene algunos tipos de sistemas de información, cada uno de ellos tiene sus propias características y todos desempeñan un papel fundamental en la reunión de la comunicación Noticias de la Organización mencionadas anteriormente. La mayoría de estos sistemas son interdependientes, no necesariamente integrados directamente, directamente para cumplir con los requisitos de diseño o indirectamente debido a la comunicación de comunicación formal o no oficial.

Hemos visto que hoy, actualmente está experimentando diferentes ataques a principios de diciembre, FireEye, una de las compañías de seguridad de red más grandes del planeta, que está en los Estados Unidos, confirmada como víctima de un ataque. En el que se utilizan herramientas internas para convertirse en la implementación de las pruebas de penetración en otras compañías.

También participamos en la vida de hoy, la pandemia, en julio de 2020, la Agencia Nacional de Seguridad Nacional, la Agencia Canadiense de Seguridad de la Red y el Centro Nacional de Seguridad del Reino Unido, advirtió por ataques informáticos contra los científicos británicos para obtener los secretos de las vacunas COVID 19.

En noviembre, Microsoft dijo que se descubrió los ataques de la red de tres países relacionados con los tres países (Oso de fantasía) y Corea del Norte (Cobra y Cerium Hidden), dirigen contra compañías farmacéuticas ubicadas en Canadá, Francia, India, en Corea y los Estados Unidos se unen a la vacuna en algunas etapas de ensayos clínicos.

En Estonia, el primer ataque serio en la infraestructura de la red de un país ha experimentado. Estonia ha sufrido un fuerte ataque de red en abril y mayo de 2007, que es la continuación del espacio de la red relacionado durante el retiro del memorial de las memorias de la Unión Soviética de los soldados caídos en la Segunda Guerra

Mundial. Con un mitin y manifestaciones en las calles Tallin, Estonia ha sufrido una serie de ataques informáticos que han dejado los sitios web, bancos, escuelas sin algún tipo de prestación de servicio. En pocos días, requiere el apoyo de expertos de la OTAN y los países aliados que contienen daños. (USA, 2021) En Perú, se han registrado más de 2.6 mil millones de ataques durante 2020, de 41 mil millones en América Latina y el Caribe. Solo en octubre, noviembre y diciembre, hubo 801 millones de esfuerzos en el país. Durante este período, la amenaza se sabe que los enlaces de estafa se expanden por América Latina con un documento HTML que intenta desviar un navegador de Internet a un sitio perjudicial. El malware de la web se ha convertido en el método más conocido para la propagación de documentos contaminados y es regularmente la puerta de entrada al ransomware.

La cantidad de asaltos en la web sigue siendo excepcionalmente alta, sin embargo, la mayor perturbación es el refinamiento y la viabilidad de los delitos de la organización que la utilización de la tendencia de la innovación y el poder del cerebro hecho por el hombre (AI) para fomentar los asaltos designados. Hay una posibilidad más notable. Para decirlo claramente, los ciberdelincuentes pueden causar más daño con menos esfuerzo. "En 2020, se mostró la posibilidad de invertir energía y activos en asaltos más valiosos, por ejemplo, el ransomware. Además, son remotos con movimientos más refinados para engañar a las víctimas y acercarse lo suficiente a la organización. Ajustándose a otro tiempo de trabajo", aclara Franz Erni, Country Director de Fortinet Perú. No sólo se puede ver la organización del centro sino también el patrón hacia los asaltos marginales. La utilización de IOT gadgets y el clima básico moderno son casos de pasajes criminales

Para 2021, Fortinet identifica una tendencia significativa diferente de la aparición de nuevos bordes inteligentes, lo que significa que se ajustan a las redes y se amplían de acuerdo con las necesidades del usuario. , Esto no solo creará diferentes vectores de ataque, sino que también permitirá que los dispositivos se comprometan a cooperar entre sí para acercarse a las víctimas a una velocidad de 5G.

En la posibilidad de que se presente un movimiento dudoso, se le alarmará y dirigirá y dará un círculo de vuelta a las encuestas representativas requeridas. El

hardware para limitar el peligro de interrupción o ruptura de nuestra estrategia de protección empresarial, incluyendo la oficina de "Proposición de Erni", que se actualiza rutinariamente, accesible desde el productor. Según un punto de vista empresarial, debemos añadir la fuerza del razonamiento informático (IA) y la IA superficial (ML). La seguridad en África es la organización central, abarcando regiones, algunas nieblas, lugares de trabajo de las sucursales y hogares lejanos para los representantes.

Ahora en la Escuela Militar contamos con un Big Data en los sistemas informáticos, lo cual nos hace demasiado vulnerables hacia otras instituciones, personas, los cuales vienen amenazando con más frecuencia estos últimos años, hoy en día no estamos garantizados con nada, se desconoce muchos puntos de seguridad para brindar a los equipos, muchas veces fácilmente engañados, muchas páginas con la seguridad no adecuada, y como entidad militar nos debemos dar cuenta que necesitamos todos los sistemas informáticos, las redes informáticas, las aplicaciones, como los software de diferentes equipos, de la manera más segura, porque nuestros documentos clasificados, personal civil y militar son entes muy importantes y decisivos para cualquier situación de guerra u operación, los pertenecientes a la Institución tienen la información sin mucha protección, mientras que entidades de otros países le ponen mucho énfasis a este punto tan importante, es por eso que vemos conveniente poner un Estándar de ciberseguridad, y esto también incluye la mejor formación de los oficiales y la concientización de la ciberseguridad, para dar mayor énfasis y seguridad a dicha entidad. En diferentes escuelas militares de otros países se ha visto el interés de dar énfasis a los sistemas informáticos, un ejemplo tenemos en Brasil, “Tenemos cursos externos para militares de las tres fuerzas y también en el mercado universitario, para postgrados. En el futuro, queremos contratar personas que conozcan el área para trabajar aquí, o que puedan dar servicio de consultoría”, dice un General del Ejercito de Brasil. Así como Brasil hay muchos países que ya le ponen interés a la ciberseguridad desde mucho tiempo atrás, nosotros estamos recién despertando en este campo el cual ya le están poniendo empeño por lo cual es que tenemos más teatros de operaciones que incluye el ciberespacio, el cual debemos darles importancia al ya haber guerras de este tipo y especializarnos a nivel nacional y a nivel Escuela Militar.

## 1.2. Delimitación de la investigación.

### 1.2.1. Delimitación espacial

El desarrollo de esta investigación tiene lugar en el espacio geográfico nacional y de acuerdo al detalle siguiente:

Entidad: Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

Distrito: Chorrillos

Ciudad: Lima

### 1.2.2. Delimitación temporal

La delimitación temporal de esta investigación se encuentra demarcada por el año 2021.

### 1.2.3. Delimitación social

La población que será objeto de estudio en esta tesis se encuentra constituida por los cadetes de la Escuela Militar de Chorrillos.

## 1.3. Formulación del problema

### 1.3.1. Problema Principal

¿Cuál es la importancia de los Estándares de Ciberseguridad en los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021?

### 1.3.2. Problemas secundarios

¿Cuál es la importancia de los Estándares de Ciberseguridad en la red de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021?

¿Cuál es la importancia de los Estándares de Ciberseguridad en las aplicaciones de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021?

¿Cuál es la importancia de los Estándares de Ciberseguridad en la información de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021?

## 1.4. Objetivos de la investigación

### 1.4.1. Objetivo general

Determinar cuál es la importancia de los Estándares de Ciberseguridad en los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021

### 1.4.2. Objetivos específicos

OE1:

Determinar la importancia de los Estándares de Ciberseguridad en la red de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021

OE2:

Determinar la importancia de los Estándares de Ciberseguridad en las aplicaciones de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021

OE3:

Determinar la importancia de los Estándares de Ciberseguridad en la información de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021

## 1.5. Justificación e importancia de la investigación

En el siguiente estudio de investigación se muestra porque es de gran interés para cada uno de los que conforman la organización y es de gran importancia porque

responde a la necesidad de implementar Estándares de Ciberseguridad en los sistemas informáticos en la Escuela Militar de Chorrillos, los cuales se basan en brindar un estado de confianza a la información que viaja a través de la red informática y además habrá una mayor concientización en la importancia de la ciberseguridad y se pondrá más énfasis al estudio de la misma.

### 1.5.1. Justificación teórica

Para respaldar la definición del problema y su razón de ser, este estudio proporciona elementos adicionales para respaldar esta afirmación. En este estudio creemos que los estándares de ciberseguridad pueden mejorar la seguridad de los sistemas informáticos de la Escuela Militar de Chorrillos, esto se debe a que el mayor problema viene de la persona o el ente que utiliza dicho sistema y al tener un Estándar se proporcionara conciencia, conocimiento y un amplio estudio de dichos parámetros de ciberseguridad.

### 1.5.2. Justificación práctica

Esto es muy importante porque la investigación realizada por empresas de ciberseguridad sugiere que los ciberataques han evolucionado significativamente. Como resultado, es necesario vigilar más la seguridad del sistema de información de la Escuela Militar de Chorrillos.

La importancia de desarrollar esta investigación radica en mejorar la seguridad de la información en los sistemas informáticos a partir de las nuevas tendencias en las tecnologías de la información y las comunicaciones, facilitando así el campo de estudio.

### 1.5.3. Justificación tecnológica

(Roig Ferriol y Oltra Badenes, 2015), indican que en un entorno competitivo los sistemas informáticos y las tecnologías emergentes, orientan sus objetivos

estratégicos a través de la aplicación de las Tecnologías de Información para su desarrollo organizacional (p.27).

La presente Investigación se justificó tecnológicamente, ya que los Sistemas Informáticos permiten optimización y automatización de los procesos y estos requieren Estándares de Ciberseguridad que mejore la seguridad de los mismos.

## 1.6. Factibilidad de la investigación

### Factibilidad Operativa

No habrá inconveniente para ejecutar, será la Implementar Estándares de Ciberseguridad para la mejora de la seguridad de los Sistemas Informáticos en la Escuela Militar de Chorrillos que permitirá la mejora de la seguridad de los Sistemas Informáticos en la Escuela Militar de Chorrillos.

### Factibilidad Técnica

Para Implementar Estándares de Ciberseguridad se cuenta con el apoyo del departamento de Telemática de la Escuela Militar de Chorrillos, nos brindarán los detalles de los sistemas informáticos los cuales servirán para poder analizar la gestión de ciberseguridad y así poder acercarnos a obtener un Estándar, además de prever ataques cibernéticos en la misma entidad

### Factibilidad Económica

Desde un punto de vista técnico, los estándares de ciberseguridad no están muy extendidos porque se desconocen en la Academia del Ejército de Cholyos, pero los autores de este estudio dedican tiempo en todo el horario de trabajo para aprovechar los beneficios durante toda la semana, incluidos los fines de semana. . Además, el autor

es el único que financia este estudio, que se presupuesta en función de los recursos financieros disponibles.

# CAPÍTULO ll: MARCO TEÓRICO

## 2.1. Antecedentes de la investigación

### 2.1.1 Antecedentes internacionales

(Romero, 2018) La investigación se realizó dentro de una tesis titulada: "CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL" INSTITUTO NACIONAL DE CIBERSEGURIDAD – ESPAÑA 2018.

En este trabajo de investigación, los objetivos generales son: Dar a conocer cuales son las amenazas, ataques y vulnerabilidades de seguridad informática más comunes en los sistemas de control industrial. Realizar una propuesta teórica para evitarlas y mitigarlas. Estrategias de investigación aplicadas en este proyecto de investigacion es Análisis del problema a resolver, Estudio de casos, Recopilación de información de los diferentes riesgos, Recopilación de información de soluciones ante amenazas, ataques y vulnerabilidades, Análisis estadístico de información de riesgos y sus soluciones, Interpretación de datos estadísticos, Estructuración y escritura del documento final que contenga soluciones para el problema planteado.

(Hermida, Alonso & Panizo, Alonso, 2018) La investigación se realizó dentro de una tesis titulada: CIBERSEGURIDAD APLICADA A LA E-DEMOCRACIA: ANÁLISIS CRIPTOGRÁFICO Y DESARROLLO DE UNA METODOLOGÍA PRACTICA DE EVALUACIÓN PARA SISTEMAS DE VOTO ELECTRÓNICO REMOTO Y SU APLICACIÓN A LAS SOLUCIONES MÁS RELEVANTES - UNIVERSIDAD DE LEÓN- ESPAÑA 2018. En este trabajo de investigación, los objetivos generales son: El objetivo final es un lanzamiento progresivo de la visión, basado en parámetros técnicos y sobre todo seguridad total. El método de la investigación que se aplicó a la presente tesis trata de contribuir a la materia desarrollando una metodología práctica de evaluación de sistemas de voto electrónico remoto transversal, para después aplicarla a los esquemas más relevantes hasta la fecha. La conclusión es que siendo ésta una tesis de marcado cariz práctico, el presente

capítulo 5 dedicado al análisis y comparativa de los sistemas de VER más relevantes, ha supuesto la culminación del proceso de desarrollo de una metodología holística de evaluación.

(Noguera, 2019) La investigación se realizó dentro de una tesis titulada: IMPLEMENTACION DE UN SISTEMA DE DETECCIÓN DE INTRUSOS PARA VENEZOLANA DEL VIDRIO C.A UNIVERSIDAD CENTRAL DE VENEZUELA – CARACAS 2019. En este trabajo de investigación, los objetivos generales son: El método de investigación aplicado a esta tesis depende de su naturaleza, que depende de los criterios de investigación tecnológica. La conclusión de esta tesis es que podemos constatar que el objetivo propuesto se ha logrado con éxito gracias al desarrollo de las distintas etapas, desde la recolección de información, análisis de necesidades hasta la implementación del IDS para Venezuela. del Vidrio CA

(Álvarez, 2018) La investigación se realizó dentro de una tesis titulada: LA GERENCIA Y EL PROBLEMA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES MODERNAS (CASO GANDALF COMUNICACIONES, C.A), UNIVERSIDAD JOSE ANTONIO PÁEZ, SAN DIEGO 2018. En este trabajo de investigación, los objetivos generales son: La investigación de las cuestiones de gestión y seguridad de la información en las organizaciones modernas (Caso de comunicación GANDALF, CA) es la compañía con herramientas que pueden abordar el problema de la gestión de la seguridad de la información L, y seguir de esta manera, para competir en ambos países y en los mercados internacionales. El método de investigación se aplica a esta tesis por el método de historia / documento, que se considera relevante y lleno de problemas y objetos de estudios discutidos en este estudio, mientras que el problema requiere enfoques para los teóricos, actividades y tecnología, ciencia y conocimiento de la creatividad, independientemente de lo político o enfoque educativo. La conclusión de la tesis actual dijo: Las organizaciones modernas, como las comunicaciones de Gandalf, son actualmente sensibles a los problemas de seguridad de la información, a través de los ataques recientes, han pasado

por los transmisores de gran desarrollo. Con el surgimiento de nuevos riesgos, nuevas amenazas y vulnerabilidades, obligó a las organizaciones a requerir personal de seguridad de información altamente calificada, lo que les permite saber que conocen sobre tecnologías y comunicación nuevos y nuevos estándares. Disponible se puede hacer de acuerdo con las necesidades de la organización.

(Tibaquira, 2015) La investigación se realizó dentro de una tesis titulada: METODOLOGÍA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS PARA LA PLATAFORMA SIEM DE UNA ENTIDAD FINANCIERA BASADA EN LA NORMA ISO/IEC 27035 E ISO/IEC 27005, BOGOTA – 2015. En el presente proyecto de investigación se ha puesto como objetivo general: Conceptualizar y ayudar a los métodos de episodio de seguridad los ejecutivos y peligro la junta identificada con ocurrencias experimentadas en la fundación SIEM de establecimientos monetarios con respecto a las directrices ISO/IEC 27035 e ISO/IEC 27005. La técnica de examen utilizada en este artículo depende del significado de un modelo de episodios de seguridad de datos de los ejecutivos. Peligran los ejecutivos de estas ocurrencias identificadas a partir de la aplicación y ejecución de los aparatos SIEM (Security Event Correlator). La representación del modelo de administración sigue un amplio ámbito de normas, ISO 27035 para las ocurrencias de seguridad y 27005 para el peligro los ejecutivos. El resultado de este trabajo es que es factible hacer un modelo exhaustivo que incorpore las ocurrencias de los ejecutivos y los peligros de la junta directiva identificados con estos episodios, a la luz de las normas de ISO 27035: 2011 e ISO 27005: 2008. Examen de las partes que son importantes para la fundación del entorno donde se ejecuta la norma.

### 2.1.2 Antecedentes nacionales

(Inoguchi & Macha, 2016) El estudio realizado en la tesis llamada: GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ, 2016, UNIVERSIDAD SAN IGNACIO DE LOYOLA – LIMA 2016. El propósito general de este estudio es de

conseguir un valor de bastante consideración de seguridad para las pymes, el cual se logrará con los resultados obtenidos en la investigación y posteriormente recomendando e indicando una propuesta para gestión y prevención de seguridad informática, y esta tendría la posibilidad de ser válido para la gran mayoría de pymes de distintos rubros o giros de negocio, la única sola condición es que la pyme se plantee llevar a cabo la propuesta de seguridad informática resultante. La metodologia que se utilizo en este estudio de investigación es un metodo con la que se ha podido llevar esta investigación como la operacionalización de las variables y técnicas de recolección de datos hasta los métodos que se usará para el estudio que se hará. La conclusión a Empresa Zavala Cargo S.A.C. tiene una carencia del uso de estrategias contra ataques de Seguridad Cibernética, que respalden su información cibernética dando acceso así a una forma de decidir de manera más segura.

(Huaura, 2019) La investigación se realizó dentro de una tesis titulada: GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESAS DEL SECTOR TELECOMUNICACIONES UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS – LIMA, PERÚ 2019. El propósito de este documento es: Determinar que la gestión de riesgos de seguridad de la información según NTPISO / IEC 31000 influye en las revisiones de riesgos para las empresas de la industria de las telecomunicaciones. El método de encuesta propuesto en esta encuesta fue un método basado en computadora (respaldado por las normas internacionales NTP ISO / IEC 31000 e ISO / IEC 27005) para ayudar en esta característica de eficiencia del trabajo. Un estudio realizado encontró que la gestión de riesgos de seguridad de la información para las empresas de la industria de las telecomunicaciones bajo la norma internacional NTP ISO / IEC 31000 impacta la gestión de riesgos para las empresas de la industria de las telecomunicaciones. Al mismo tiempo, logra establecer los criterios para un análisis de riesgos coherente, configurando el panorama actual de la compañía y proporcionando indicadores y cifras de gestión que apoyan permanentemente a la alta dirección.

(Bruderer, Vega, 2019) El estudio realizado en la tesis llamada: DISEÑO DE UN MODELO DE CIBERSEGURIDAD PARA DISPOSITIVOS MÓVILES EN EL SECTOR EMPRESARIAL, PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ – LIMA, PERU 2019. La presente tesis tiene como finalidad: Implementar un prototipo de ciberseguridad para equipos móviles en el ámbito empresarial. El enfoque de investigación que se propuso fue que se compilara información de los estándares de NIST y de la ISO 27032 para comenzar a preparar un prototipo de ciberseguridad con el que se pueda implantar controles para resguardar y dar seguridad a los equipos móviles y la Big data manipulada por ellos. En la investigación de esta tesis se llegó como conclusión que los dispositivos móviles a pesar de ser muy útiles tienen varias vulnerabilidades propias de ellos y en el uso de ellos que los hace un objetivo atractivo para los atacantes cibernéticos para afectar la confidencialidad, seguridad de la Big data de las instituciones, empresas o clientes. Por esta razón, para enfrentar este problema lo que se propone como proyecto de fin de curso es implementar un prototipo de gestión de ciberseguridad para equipos móviles del ámbito empresarial.

(Mansilla, 2020) El estudio realizado en la tesis llamada: IMPLEMENTACIÓN DE PROGRAMAS DE CUMPLIMIENTO EN CIBERSEGURIDAD COMO UNA PRÁCTICA DE BUEN GOBIERNO CORPORATIVO EN LAS ENTIDADES QUE FORMAN PARTE DEL SISTEMA FINANCIERO PERUANO, PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ – LIMA, PERÚ 2020. La presente tesis tiene como finalidad: Este trabajo de investigación busca identificar la necesidad de implementar el programa de cumplimiento de la seguridad de la red como una buena práctica de gobierno corporativo en las entidades en el sistema financiero del Perú, teniendo en cuenta este país, no lejos de la víctima de una banda de red y desarrollando esta economía digital. , casi la fortaleza y las instituciones financieras del gobierno central a través de medidas específicas de seguridad de la red, están considerando la implementación de las políticas de implementación, las instrucciones., Funciones sindicales, entre otras acciones. En esta tesis, afirma que buscan determinar la necesidad de proteger los ataques de los ciberdelincuentes o evitar los ataques en las entidades en el sistema financiero de Perú, gracias a la implementación de diversos programas de buena

ejecución de seguridad de la red es una buena práctica. Gobierno corporativo. En este caso, se ha concluido que la implementación del Programa de Cumplimiento de la Ciberseguridad proporcionará una mayor confianza para la gestión de riesgos digitales, lo que proporcionará apoyo vasto en la organización y, sobre todo, influirá directamente para prevenir y minimizar los riesgos determinados por su financiera y natural. Empresas de acuerdo a su tamaño y naturaleza.

(Alcantára, 2015) La investigación se realizó dentro de una tesis titulada: GUÍA DE IMPLEMENTACIÓN DE LA SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001, PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA COMISARIA DEL NORTE P.N.P EN LA CIUDAD DE CHICLAYO, UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO – CHICLAYO, PERÚ 2015. La presente tesis tiene como finalidad: Aportar a que se pueda haber una mejora en el sector de seguridad de la Información, apoyado en la norma ISO/IEC 27001, en la institución Policial Comisaria del Norte – Chiclayo.

El procedimiento de la presente tesis se ha podido ver por más factible el uso de las habilidades de recolección de datos como son las encuestas, entrevistas, así como fichas de observación, como medio para poder extraer la información y su posterior interpretación; y es asi como la verdadera problemática respaldado en la ejecución de la Norma ISO/IEC 27001, teniendo como objetivo obtener y saber las debilidades y deficiencias para mejorar en el ámbito de seguridad e integridad de la información en los sistemas de almacenamiento de Big data de aquella empresa. La presente tesis tiene como conclusión: Con aquella estrategia de Capacitación y Concienciación habiéndose implementado en aquella Organización, se logró incrementar el conocimiento, y su vez mejorar el nivel de capacitación para el personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado personal comprometido con la seguridad en favor de la institución.

## Bases teóricas

### 2.2.1 Base teórica (Variables independiente y sus indicadores)

#### Variable independiente: ESTÁNDARES DE CIBERSEGURIDAD

(kaspersky, s.f.) La ciberseguridad es el proceso de proteger computadoras, servidores, dispositivos móviles, sistemas electrónicos y redes, y ataques maliciosos. Esto se denomina seguridad informática o seguridad de la información electrónica.

Los estándares de ciberseguridad son técnicas desarrolladas en documentos publicados para proteger el entorno de red de usuarios, computadoras u organizaciones. Todo aquel entorno incluye toda la información que almacena un Big data, a nuestros propios usuarios, redes, dispositivos, todo el software, procesos, aplicaciones, sistemas que puedan tener alguna conexión o enlace con las redes o ciberespacio.

El objetivo principal de aquellos estándares es para reducir los riesgos, incluyendo prevención o atenuación de ciber-ataques proporcionado por agentes expertos en ciber-delincuencia. Estos materiales consisten en colecciones de herramientas, políticas de seguridad, conceptos de seguridad, salvaguardas de seguridad, guías, enfoques de gestión de riesgos, acciones, capacitación, mejores, prácticas, aseguramiento y tecnologías.

(GrupoACMSConsultores, s.f.)La normativa ISO 27032 es aquel novedoso estándar de ciberseguridad difundida en Julio de 2012 por La Organización Internacional de Normalización.

La norma ISO/IEC 27032: brinda un amplio ambiente de guía para reforzar la impenetrabilidad del espacio del amplio ambiente cibernético en defensa de los malware que puedan haber o amenazas de ciber-ataques que puedan atentar el estado de Ciberseguridad de cualquier entidad o empresa, este presente estándar nos pretende garantizar la seguridad apropiada para el intercambio de información a través de la red, espacio cibernético, para asi poder librarnos de ser víctimas de un Cibercrimen y poder reducir riesgos en Internet.

La Organización Internacional de Normalización asegura la calidad y seguridad contra cualquier clase de operaciones que se realizan a través del Ciberespacio y cualquier actividad online es por eso que el desarrollo de la ISO es fundamental en cualquier empresa.

Esta norma nos facilitara la colaboración y navegación segura y confiable para poder estar seguros con la privacidad del ordenador, información, red y la privacidad principal de todas las personas alrededor del mundo. Ayudará a prepararse para detectar cualquier amenaza y responder los ataques de una manera eficiente.

Gracias a la ISO 27032 permitirá luchar contra ataques de ransomware, malware, spyware, ingeniería social, phishing y hackers que puedan atentar con la seguridad se nuestra información o vida privada.

Decir ciberespacio nos exige tener una visión mucho más amplia acerca de la definición de seguridad de la información, une aspectos que relacionan la interacción sobre las redes de personas soportados por entornos TIC.

Por otro lado, tenemos al NIST que por sus siglas en español significa Instituto Nacional de Normas y Tecnología el cual tiene a cargo el desarrollo de lo que hoy se conoce como Cybersecurity Framework (CSF) el cual está basado en estándares ya aceptados por el gran ecosistema de Ciberseguridad. Esta es una herramienta para la gestión de riesgos de ciberseguridad, la cual también incluye la innovación tecnológica y es flexible para adecuarse a cualquier tipo de organización.

La gran ventaja y diferencia que se ha presentado en este Marco de Ciberseguridad es su simplicidad para poder transmitir distintas estrategias técnicas que se ajuste al negocio de tal manera que este lo comprenda y su flexibilidad para adecuarse o encajar en cualquier Organización.

El Cybersecurity Framework consta de tres componentes principales:

Framework Core: son deseados resultados de ciberseguridad, los cuales son alineados en base a Referencias informativas de los diferentes estándares aceptados por la misma industria. Esta consta de tres partes: funciones, categorías y subcategorías.

Funciones: Identificar, proteger, detectar, responder y recuperar.

Identificar: este servicio contribuirá a extender y acrecentar un nivel de conocimiento de toda la entidad para asi ordenar o dirigir algún tipo de peligro de ciberseguridad encontrada en los distintos tipos de datos, sistemas y al identificar estos riesgos relacionados con la ciberseguridad permitirá que la organización centre o priorice sus fuerzas, teniendo en cuenta su enfoque de administración de diferentes tipos de peligros y las carencias encontradas.

Proteger: se describirá cualquier medida a adoptar para una seguridad acorde y adecuada a la situación en la que se encuentre. Esta función tendrá como fin limitar o contener el impacto severo de aquel evento que atente la ciberseguridad.

Detectar: definirá las actividades que se darán en el evento de ciberseguridad, con el fin de identificar y hacer un descubrimiento oportuno sobre alguna ocurrencia que nos pueda afectar o nos pueda poner en riesgo a nuestro espacio cibernético.

Responder: esta función tiene como misión tomar medidas con respecto a un incidente de ciberseguridad que se haya podido detectar, con el fin de desarrollar la capacidad de hacerle frente y contener el dicho impacto para no ser perjudicados de forma severa.

Recuperar: identificara las actividades necesarias para recuperar o restaurar alguna capacidad o servicio que se haya podido perder o deteriorar a consecuencia de algún incidente de ciberseguridad.

Categorías: existen 23 categorías las cuales se dividen en las cinco funciones ya mencionadas. Estas categorías no son demasiadas detalladas, sin embargo, fueron diseñadas para cubrir la gran amplitud de los objetivos de ciberseguridad para cualquier organización.

Subcategorías: por conocimiento se sabe que existe 108 subcategorías, estas son estadísticas que tienen por modelo los resultados los cuales nos da cualquier tipo de apoyo y esto mejoraría un programa de ciberseguridad. Debido a que este Marco de ciberseguridad está orientado y tiene

como objetivo los resultados y no establece algún parámetro que diga cómo lograrlo o como alcanzar dichos resultados, esta parte del Core permitirá implementaciones basadas en el riesgo que se acomodan a las distintas necesidades de las organizaciones.

Niveles de implementación del CSF: estos niveles describirán el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización muestran las diferentes características que opta este Marco de ciberseguridad. Los mencionados niveles son: Parcial, riesgo informado, repetible y adoptado. Estos describen que tan bien están integradas están las decisiones acerca los riesgos de ciberseguridad y el grado con el que recibe la información de ciberseguridad de entes externos. Lo recomendable es que todas las organizaciones terminen en el nivel deseado, el más alto no quiere decir que sea el mejor para alguna entidad, se debe elegir el más recomendable, se debe asegurar que cumpla con al menos con todos los objetivos a cumplir de dicha organización.

Perfiles: este componente nos indicara los requisitos, objetivos organizacionales, recursos, tolerancia al riesgo, todo esto de acuerdo al Framework Core. También se utilizará para identificar distintas oportunidades que se tendrá para desarrollar el estado de ciberseguridad comparando el perfil que tenemos con el perfil deseado, el cual será el objetivo de nosotros. Al identificar nuestro perfil podremos evaluarnos y realizar una evaluación de manera objetiva, con el fin de mejorar la situación actual haciendo cambios de procedimientos, estrategias, prioridades, estrategias de liderazgo y poder adquirir nueva tecnología, que nos ayude a lograr el perfil objetivo.

El Cybersecurity Framework se presenta como una herramienta muy útil que permitirá gestionar los riesgos de ciberseguridad de manera flexible y adaptable a cualquier situación u organización.

Otro punto importante que vemos hoy en día es la ciberseguridad, pero en los servicios de almacenamiento cloud, una gran interrogante que se tiene comúnmente es sobre la seguridad con la que se pueden tratar nuestros documentos, sobre todos los contratos que se ven involucrados y otros. Las diferentes empresas que prestan dicho

servicio garantizan la seguridad a todos sus clientes. Existen diferentes normas o estándares que ayudan a fortalecer la ciberseguridad en servicios cloud asi como garantizar la integridad y confidencialidad de la información alojada en la nube.

ISO 27001: es un estándar que describe la forma correcta de gestionar la seguridad de la información del interior de una Organización. A nivel global esta es la principal norma de seguridad para la conducción de la información.

La norma 27001 direcciona sus objetivos a que las entidades u organizaciones conozcan los riesgos cercanos al manejo de la información para poder minimizarlos y gestionarlos por medio de un proceso sistemático, adaptable y eficiente para los cambios que se pudieran presentar frente a los riesgos de la tecnología.

Para obtener dicha certificación como la 27001, la organización deberá cumplir con algunos pasos:

Etapa previa: en esta etapa la empresa debe proponer y analizar una metodología a seguir para gestión de riesgos, definir el alcance del sistema de seguridad, determinar los posibles riesgos y evaluarlos, para eso también se evaluaremos la implementación de medidas correctivas y controles para atenuar dichos riesgos.

Auditoria de revisión: el personal experto que viene del exterior evaluara que todo lo anterior este planteado y que se cumpla como debe ser, para luego dar inicio al proceso de certificación.

Auditoria principal: un grupo de expertos en el área de ciberseguridad y agentes externos verificara que las medidas adoptadas sean las ideales y cumplan con todos los requisitos para llegar al objetivo, si esto estaría en orden, la empresa seria certificada.

Revisiones periódicas: al haberse ya aprobado la certificación, el organismo monitoreara y vigilara la organización durante 3 años para asegurarse y cerciorarse que se cumpla con los esfuerzos de seguridad de todos los datos.

ISO 27017: es un estándar de seguridad la cual proporciona controles tanto para clientes como para los diferentes proveedores que se relación con los servicios de la

nube, su importancia radica en la gran precisión que puede establecer los clientes con los proveedores de los servicios de la nube, de gran importancia ya que el cliente puede exigirle sus problemas a solucionar y el proveedor puede brindarle toda la información requerida.

El objetivo de esta norma es fortalecer la ciberseguridad y la gestión del servicio referido a medidas de seguridad, tecnología de cifrado y localización geográfica de datos. Esta norma tiene 37 controles en la nube los cuales son basado en la norma 27002 junto a 7 adicionales los cuales ayudaran a fortalecer la seguridad de los servicios cloud.

ISO 27018: esta norma comprende un largo compendio de diferentes buenas prácticas que hace referencia a los controles de protección de datos para servicios cloud. Esta dicha norma tiene como fin delimitar las normas, controles y procedimientos que los proveedores deben aplicar ya que son los principales afectados cuando hay un riesgo inminente. Además, garantiza el cumplimiento de la norma legal en lo que se refiere a datos personales, lo cual es un punto importante que a nivel mundial se cuida y es confidencial.

Después de haber visto todas las normas esenciales para un seguro y confiables servicios cloud hemos evaluado a los proveedores que cumplan con todo lo requerido, las cuales son:

Amazon Web Services: cumple con todas las leyes y regulaciones, además de ser transparente en lo que se refiere al cumplimiento de todas las normativas a optar por un seguro servicio.

Google Cloud: esta nos pone al tanto a todos los usuarios que cumple con todas las normativas y certificaciones con la que nos garantiza la ciberseguridad de todos nuestros datos que se manejar y navegan a través de la nube.

Microsoft Azure: este servicio se ha motivado y levantado con el gran ejemplo que brinda Microsoft ofreciendo un software empresarial para construir una infraestructura en la nube la cual sea confiable y segura, la cual cuenta con todas las normativas y certificaciones que requiere los servicios cloud.

Por ultimo tenemos a la Implementación de un Marco de Ciberseguridad ISO 27032, la cual define las Guías en este contexto y se concentra en dos áreas: por un lado se buscara cubrir todos los espacios o huecos que puedan haber dejado las normas o estándares anteriores de seguridad en un ámbito más amplio, en el que aparecen nuevos ataques y riesgos a los cuales debemos enfrentar y por otro lado tenemos el proceso de colaboración entre los agentes que cooperan en el mismo entorno, lo que se denomina hoy en día Marco de seguridad.

El Marco de Ciberseguridad que se desarrollará tendrá una aproximación a la gestión de riesgos en 4 diferentes áreas:

Prevención: esta se basará en la implementación de medidas e implantación de controles los cuales sean capaces de contener o evadir algún posible impacto que atente contra los eventos de ciberseguridad.

Protección y detección: en esta área se implementará los controles que estén direccionados a la gestión de seguridad y a la monitorización de eventos de riesgos de seguridad con el fin de detectar peligros y adelantarse a la protección para dichos eventos que puedan desequilibrar la protección.

Respuesta y comunicación: se debe estar alerta ante cualquier posible incidente referido a la seguridad de la información o ciberseguridad y esta área actuara de tal manera que minimice los elementos peligrosos y mitigue los riesgos que estén materializados de tal manera que si hubiera daños o se sea vulnerado sea de manera mínima.

Recuperación y aprendizaje: son las acciones que se efectúa para restaurar los sistemas que se hayan podido dañar y servicios que se relacionen con el ciberespacio y a partir de esto se definirá procedimientos, estrategias para minimizar la probabilidad de posibles incidentes o riesgos que atenten la ciberseguridad.

El Marco de ciberseguridad de la ISO 27032 sugiere un proceso que sigue nuestra metodología y se desarrolla en las siguientes fases:

Fase I – Entendimiento de la Organización: esta fase nos permitirá disponer de un inventario de activos de los servicios, realiza un trabajo muy importante de inmersión en los procesos a desarrollar la empresa para lograr un entendimiento y conocer el funcionamiento y permitir saber el uso del Ciberespacio en sus diferentes servicios. Para lograr llevar a cabo esta fase es necesario tener en cuenta diferentes puntos como: revisar productos, servicios, el marco normativo en uso, conocer los flujos de información en los distintos tipos de procesos, las técnicas a desarrollar para la seguridad y revisar o recopilar información para la seguridad de cualquier entidad.

Fase II – Análisis de Riesgos: la decisión de tomar decisiones estará basada en gestión de riesgos de la ciberseguridad, en cuanto nos referimos a controles, medidas de seguridad a nivel informático. En esta fase se tendrá en cuenta aspectos como eventos críticos, vulnerabilidades, amenazas, impacto y riesgo que se produce en el espacio cibernético.

Fase III – Plan de acción: esta fase permitirá redactar el plan que nos hará conocer la priorización y medidas que se deberán optar para desarrollar la consecución de alineamientos de la ISO/IEC 27032 en base a las exigencias de esta misma. Este dicho plan afrontara diversas estrategias las cuales deberán aplicarse a todos los niveles de la organización:

Fase IV – Implementación: frecuentemente esta es la etapa que más esfuerzo requiere, ya que todas las acciones mencionadas se verán plasmadas en el plan de acción. La ISO/IEC 27032 tiene como característica que al usuario que la emplea lo obliga a ser proactivo con las medidas de seguridad y a su vez pone énfasis a las estrategias de prevención para los procesos que incluyan al ciberespacio. El punto principal de esta fase es la focalización en la implementación de controles la cual se debería tener mayor énfasis a la gestión de ciberseguridad y se debe tener en cuenta aspectos como la monitorización TIC, gestión de incidentes, existencia de política de seguridad, planes de concientización al personal y los diferentes marcos existentes para el intercambio o mezcla de información.

**Indicador 1: Seguridad de la información**

La seguridad de la información se encarga de proteger las redes informáticas de los ciber terroristas, mediante la adopción de medidas preventivas y reactivas que puedan proteger o proteger la información almacenada en esta red.

Es un elemento imprescindible de la empresa para el desarrollo de sus actividades, porque los datos a tratar son fundamentales para el futuro de la empresa. Además, también debemos considerar la seguridad de la información que enfrenta los riesgos, analizarlos y prevenirlos y buscar soluciones rápidas para eliminarlos o removerlos para que sean seguras para nuestra vida privada.

La seguridad de la información, como concepto, se basa en cuatro pilares: disponibilidad, integridad, confidencialidad y autenticación.

Disponibilidad: Acceda a la información según sea necesario, sujeto a confidencialidad. Evite el "bloqueo" del sistema permitiendo el acceso ilegal, bloqueando el permiso al correo …

Confidencialidad: Información accesible solo para personal autorizado. La información de la Big data debe estar seguro que no esté con personas indebidas que no deban tenerla y la maniobren de mala manera.

Integridad: Información correcta sin modificaciones no autorizadas ni errores. Se protege frente a vulnerabilidades externas o posibles errores humanos.

Autenticación: Información que viene a ser de un usuario que es quien dice ser. Se le debe asegurar para asi garantizar que el propósito u origen de aquellos datos o información es la verídica.

La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:

Electrónicos

En papel

Audio y vídeo, etc.

La Seguridad de la Información ha estado en desarrollo en estas últimas décadas, además ha evolucionado considerablemente. Se ha convertido en una carrera acreditada mundialmente. Dentro del éste área se ofrecen muchas especializaciones que se pueden incluir al realizar la auditoría del Sistema de Gestión de Seguridad de la Información ISO-27001, como pueden ser:

Planificación de la continuidad de negocio

Ciencia forense digital

Administración de Sistemas de Gestión de Seguridad

La seguridad de la información incluye asegurar que los recursos de los sistemas de información de la empresa se utilicen de la manera prevista y que el acceso a la información recibida, además de controlar esa modificación sea realizada únicamente por personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

Los objetivos de la seguridad informática:

Los activos de información son los contenidos que la Seguridad de la Información debe asegurarlos. Por lo que son tres elementos lo que forman los activos:

Información: es el objeto de mayor valor para la empresa.

Equipos: suelen ser software, hardware y la propia organización.

Usuarios: son las personas que usan la tecnología de la organización.

**Indicador 2: Seguridad de las redes**

La seguridad de red es algún tipo de trabajo hecho con el fin de asegurar el acceso, el uso y la integridad de la red y los datos corporativos.

Incluye tecnologías de hardware y software.

Está orientada a diversas amenazas.

Evita que ingresen o se propaguen por la red.

• La seguridad de red eficaz gestiona el acceso a la red. (Egresado de la Universidad Católica San Pablo, s.f.) La ciberseguridad engloba Diferentes avances, artilugios y ciclos. Se trata de un conjunto de normas y configuraciones utilizadas para garantizar la respetabilidad, la seguridad y la apertura de la organización y la información a través de la programación y la innovación de los equipos.

Todas las entidades, sin importar la estimación, la fundación o la industria, necesitan arreglos de protección de red ilimitados contra los peligros digitales y un gran número de asaltos en Internet. La ciberseguridad combina múltiples capas de defensa a nivel del perímetro y de la red. Cada capa de seguridad de la red implementa políticas y controles. Los usuarios autorizados pueden acceder a los recursos de la red, mientras que los usuarios malintencionados están bloqueados para evitar que ataquen vulnerabilidades y amenazas de seguridad. Se tiene muchos puntos a considerar cuando se habla de seguridad de redes de una organización, cualquier ataque de gran magnitud puede ocurrir en cualquier capa de seguridad de la red y la política, el método a seguir debe estar en condiciones de preparar y actuar con métodos para tratar cada área, por lo que se tiene tres diferentes tipos de seguridad:

Seguridad física en redes

Los controles de seguridad física tienen por objeto evitar que personas no autorizadas lleguen realmente a organizar partes como interruptores y armarios con cables. El control de acceso a las cerraduras, la información biométrica y otros dispositivos es fundamental para cualquier empresa

Seguridad técnica en redes

Los controles técnicos de seguridad garantizan la información guardada o comunicada en la organización, ya sea dentro o fuera de ella. Doble garantía: la

información y los marcos deben estar protegidos de ejercicios malignos por parte de personas y representantes no autorizados.

Seguridad administrativa en redes

Los controles de seguridad de la gestión comprenden los enfoques y ciclos de seguridad que controlan la conducta del cliente, por ejemplo, cómo los clientes verifican, los niveles de acceso y cómo los trabajadores de la innovación de datos (TI) llevan a cabo cambios en la fundación.

Hay varias formas de asegurar su organización y varios tipos de controles de seguridad de la organización:

Control de acceso a red

Deben ejecutarse enfoques integrales de control de acceso de clientes y aparatos para evitar que los probables agresores entren en la organización. El control de acceso a la red (NAC) puede diseñarse a un nivel mínimo. Por ejemplo, se puede permitir a un jefe la admisión completa a la organización, negar la admisión a sobres misteriosos específicos o impedir que los gadgets individuales se unan a la organización.

Software antivirus y antimalware

a programación anti-malware y contra el malware protege a su organización de un surtido de malware, por ejemplo, infecciones, ransomware, gusanos y troyanos. La mejor programación comprueba los documentos cuando usted está en la web, pero además continuamente salidas y pantallas de sus registros.

Protección de firewall

Un cortafuegos, como su nombre indica, actúa como un obstáculo entre una red exterior no fiable y una organización interna de confianza. Los directores suelen diseñar conjuntos de directrices explícitas para impedir o permitir el tráfico de la red

Redes privadas virtuales

Una VPN se asocia con su organización desde otro punto final o sitio. Por ejemplo, los clientes que trabajan a distancia suelen conectarse con la organización

corporativa a través de una VPN. La información se codifica entre los dos lugares y el cliente debe ser verificado para permitir la correspondencia entre el aparato y la organización.

**Indicador 3: Seguridad en Internet**

La sensacion de confianza en Internet es un conjunto de precauciones que se toman para proteger todos los elementos de la red, como la infraestructura y la información, que se ven más afectados por el ciberdelito.

La seguridad informática es responsable de establecer métodos, procedimientos y estándares capaces de identificar y eliminar las debilidades en la información y los dispositivos físicos, como los diferentes tipos de computadoras y todos los dispositivos eléctricos.

Este tipo de seguridad incluye bases de datos, archivos y dispositivos que evitan que información importante caiga en las manos equivocadas.

Una de las mejores formas de mantenerse protegido en Internet es utilizar software antivirus; para comprenderlo mejor, realice nuestro curso sobre virus informáticos y software antivirus.

Los peligros más normales que influyen en los clientes y los sitios son: Robo de datos: bancarios, privados, etc…

Virus

Phishing (robo de identidad)

Ataques DDoS: un asalto DDoS realiza innumerables solicitudes a un sitio en un breve periodo de tiempo para derribarlo.

Spam

Medidas de privacidad y seguridad en internet

Antivirus:

El principal esfuerzo de seguridad fundamental en Internet es un programa antivirus. Son la mejor posibilidad para contrarrestar el peligro y tienen una extraordinaria disposición gratuita. Los antivirus son necesarios para todos los gadgets asociados, incluyendo tabletas y teléfonos móviles.

Contraseñas:

Las contraseñas son otra apertura de seguridad a comprobar. Por poner algunos ejemplos de las administraciones más conocidas, seguro que tienes una cuenta de Google, Facebook o Twitter. Sin embargo, para utilizar constantemente una frase secreta similar por comodidad, reconsidere, ya que esto es algo contrario a lo que sugieren los especialistas en seguridad de PC. Además, todo el mundo tiene varias contraseñas. Debería ser suficiente y difícil de averiguar.

Seguridad de la información:

Cuando se trabaja en un centro, se debe garantizar que los datos de los pacientes son totalmente privados. Center Cloud, un programa basado en la nube, no sólo facilita el manejo de la historia clínica de los pacientes, sino que también garantiza el cumplimiento de las normas de la LOPD.

Navegación:

La inseguridad en Internet es básicamente una cuestión inteligente. Una orientación típica es mantenerse alejado de los sitios dudosos (la mayoría de los programas antivirus distinguen esta infección). Los sitios seguros tienen declaraciones SSL. Es decir, la URL de su sitio contiene https en lugar de http. En lo que respecta a la seguridad en Internet, hay algunas opciones para navegar por la red de una manera más segura y sólida.

1. Revelar los datos individuales de forma restringida y experta.

Su jefe o cliente potencial no tiene por qué saber su estado civil o su número de calle. Todo lo que necesitan saber son datos sobre tu visión del trabajo, tus habilidades y tus opciones de contacto. No des datos rigurosamente cercanos a las personas de fuera, así que no los des a un gran número de individuos en la web.

2. Deje la configuración de protección habilitada

Al igual que los programadores, los anunciantes necesitan tener un conocimiento profundo de usted. Pueden obtener toneladas de conocimiento útil sobre tus propensiones a la lectura y cómo utilizas las organizaciones interpersonales. Sea como fuere, usted puede ocuparse de sus datos. Como el sitio Lifehacker trae a colación, los navegadores de Internet y los marcos de trabajo portátiles tienen ajustes para garantizar su seguridad en Internet. Los ajustes de mejora de la seguridad son igualmente accesibles en sitios enormes como Facebook. Estos indicadores pueden ser difíciles de rastrear (a propósito) a la luz del hecho de que las organizaciones necesitan información individual para promover la estima. Asegúrese de que esta estrategia de seguridad está habilitada y déjela habilitada.

3. Manejar una navegación segura

No te conectes a Internet en un lugar peligroso ya que no decides pasear por un lugar arriesgado. Los ciberdelincuentes se alimentan de sustancias sorprendentes. Se dan cuenta de que, ocasionalmente, los individuos se sienten atraídos por la sustancia dudosa y podrían tener cuidado al experimentarla. La "gran parte del mundo" de Internet ha tenido siempre el probable problema de los chasquidos salvajes que descubren los datos individuales y el malware que daña los aparatos. Suponiendo que el programador se oponga a la seducción, no encontrará la oportunidad.

4. Comprobar una conexión a Internet segura

Al iniciar sesión en un área pública, por ejemplo, una asociación pública de Wi-Fi, PCMag confirma que no tiene ningún mando inmediato sobre la seguridad. Los

especialistas en protección en línea se fijan en los "puntos finales" en los que las organizaciones privadas se asocian con el resto del mundo. El punto final sin poder es una asociación de Internet de barrio. Asegúrese de que su gadget es seguro y, si todo lo demás falla, espere a que se produzca una asociación aún más ideal (es decir, que se conecte con una organización Wi-Fi segura) antes de dar datos, por ejemplo, su número de saldo financiero.

5. Ten cuidado con lo que descargas

Uno de los primordiales metas a llegar de los ciberdelincuentes es engañarlo para que descargue malware. Este malware puede adoptar la apariencia de cualquier cosa, desde juegos ordinarios hasta aplicaciones de comprobación del tráfico o del clima. Como sugiere PCWorld, no descargues aplicaciones que creas que son dudosas o de sitios no confiables

6. Elija una palabra secreta sólida

Las contraseñas son probablemente el mayor defecto de toda la estructura de seguridad de Internet, aunque es básicamente imposible sortearlas. El problema con las contraseñas es que las personas suelen elegir contraseñas que no son difíciles de recordar (por ejemplo, "clave secreta" y "123456") y palabras que no son difíciles de averiguar. Elija una frase secreta sólida que sea difícil de descifrar para los agresores. Con nuestro director de claves secretas, puedes tratar con varias contraseñas para que las recuerdes. Una clave secreta sólida es una palabra secreta extraordinaria y compleja de algo así como 15 caracteres, que contiene letras, números y caracteres únicos.

7. Compre en línea en sitios seguros

En cualquier momento que compre en la web, se le pedirá que dé los datos de la tarjeta de crédito o del saldo financiero que más necesitan los ciberdelincuentes. Sólo dé estos datos a destinos que den intercambios seguros y codificados. Según ha

comprobado la Universidad de Boston, puede reconocer los locales seguros buscando direcciones que empiecen por https: (la S representa la palabra segura) en lugar de direcciones que empiecen por http. Asimismo, puede incorporar un símbolo de candado cerca de la barra de ubicación.

8. Sé precavido a la hora de publicar.

Es casi seguro que algunas fotografías o grabaciones de contenidos transferidos a la red o a Internet permanecerán en Internet durante toda la eternidad. Esto se debe a que borrar la primera (por ejemplo, de Twitter) no elimina las copias que puedan tener otros. No puedes "borrar" ningún comentario que prefieras no compartir, ni borrar los humillantes selfie que te hiciste en la fiesta. No publiques nada en la red que no sea necesario para las madres o los observadores.

9. Ten cuidado con quien conoces online

Las personas que conoces en línea no siempre son lo que dicen ser. De hecho, puede que no sea real. Como señaló InfoWorld, los perfiles falsos en las redes sociales son una forma común en que los piratas informáticos atraen a los usuarios de Internet desprevenidos y les roban sus billeteras en línea. Debe ser tan cuidadoso e inteligente en su vida social en línea como lo es en su vida social cara a cara.

10. Mantén actualizado el programa antivirus

El software de seguridad de Internet no puede protegerlo de todas las amenazas, pero detectará y eliminará la mayoría del malware, aunque debe asegurarse de que esté actualizado. Asegúrese de mantenerse al día con las actualizaciones del sistema operativo y las actualizaciones de las aplicaciones que utiliza. Proporcionan un importante nivel de seguridad.

**Indicador 4: Protección de las Infraestructuras críticas para la información**

Los ciberataques no solo están dirigidos a las empresas, organizaciones y personas con datos valiosos y sensibles, sino también a las infraestructuras críticas de las ciudades como plantas de tratamiento de agua, presas hidroeléctricas, centrales nucleares, oleoductos, gasoductos, entre otros.

Esto genera serias preocupaciones para los gobiernos y organizaciones responsables de administrar este tipo de infraestructura crítica, porque con un ataque bien organizado, los ciberdelincuentes pueden convertirse en ciberterroristas, causando daños y pérdidas a gran escala.

Ataques recientes a infraestructuras críticas

En 2019, los duchos de Eset archivaron un feroz desastre hacia la petrolera estatal mexicana PEMEX la cual daño al 5% de las computadoras, afectando el honor de la empresa más aún que su fama o materialmente hablando.

Finalizando febrero de 2021, los duchos en el tema dieron a conocer de otro ataque a infraestructura crítica que abarca e incluye información en la ciudad de Florida, EE. UU., En la cual algunos ciber terrorista trataron de intoxicar el suministro de agua potable con hidróxido de sodio.

A medida que paso el tiempo hicieron rápido su trabajo y ubicaron el punto centro del ataque o desastre que estaban ocasionando, por consecuencia y buena suerte han podido evitar lo cual pudo ser llamado "ciber terrorismo", ya que dicho desastre pudo haberse llamado como una de las mayores tragedias y desastres, si es que no se preparaban y atendían en el debido tiempo. Aparece en el momento adecuado.

Hace muy poco tiempo, en mayo del 2021, un ataque de ransomware afectó el suministro de combustible en toda la costa este de Estados Unidos, ocasionando fuertes montos de pérdidas a lo largo del desastre que estaba ocurriendo y asi mismo degrado la confianza que se tenía con la compañía hacia otras.

El alcance de este ataque es tan grande que llevó a que la Administración Federal de Seguridad de Auto transportistas (FMCSA, por sus siglas en inglés) declarara la emergencia regional en Alabama y muchas otras ciudades.

Medidas de protección para infraestructuras críticas

Las empresas, los ciudadanos y la infraestructura crítica se enfrentan ahora a cualquier tipo de ciberataque.

Los más comunes se encuentran en forma de ransomware (robo de información mediante cifrado), phishing (robo de identidad) y botnets (botnets que controlan dispositivos de forma remota, que han prosperado debido a la seguridad limitada que las empresas brindan al Internet de las cosas). Sin embargo, para evitarlos, no basta con apagar los dispositivos no utilizados o restablecer las contraseñas. Es importante que vayamos más allá. Estas son algunas de las garantías clave que ofrecen los expertos.

Realizar auditorías técnicas

Para establecer medidas de seguridad específicas, es necesario conocer el estado de la infraestructura y tomar acciones para abordar las vulnerabilidades.

Muchos expertos recomiendan utilizar soluciones de seguridad en la nube para garantizar la seguridad al conectarse a estos sistemas.

También recomiendan solicitar actualizaciones de confiabilidad y seguridad digital a proveedores de hardware y software.

Además, es necesario implementar un alto nivel de ciberseguridad en los sistemas SCADA (monitorización, control y adquisición de datos), que en algunos casos no se tiene en cuenta.

Vigilar las nuevas superficies de ataque

Las continuas innovaciones tecnológicas (como Internet de las cosas) traen nuevos desafíos en la seguridad de TI y la superficie de ataque se expande con cada innovación.

El vector de ataque de la "red" está en casi todas partes, y casi todos los tipos de dispositivos modernos se comunican con otros sistemas dentro y fuera de Internet para que los datos se puedan extraer utilizando Big data y analizarlos mediante el aprendizaje automático.

Además, la migración a la nube introduce nuevas vulnerabilidades de seguridad, ya que los ejecutivos de nivel C y otros niveles C creen que al pasar a la tecnología de nube estarán protegidos, pero no están interesados en proteger sus resultados. Conectividad de un extremo a otro, como terminales y empleados a una instancia en la nube y toda la infraestructura asociada.

Cambio de mentalidad

Una encuesta reciente de nuestro socio Fortinet muestra que, lamentablemente, las organizaciones van en la dirección equivocada en términos de resultados. Nueve de cada diez empresas están experimentando al menos un avance en tecnología operativa (OT) en 2020, un aumento del 19% con respecto a 2019. El porcentaje de organizaciones con tres o más avances aumentó del 47% al 65% en el mismo período. Los gerentes de TI en la infraestructura crítica deben comprender que deben cambiar el enfoque de sus estrategias de reactivo a proactivo, asegurando un sistema de seguridad cibernético integral que reduzca la superficie de ataque. Para asegurar una protección de este tipo, es necesario evaluar las soluciones de ciberseguridad centrándose en 5 vehículos de ataque a los que están expuestos todo tipo de sistemas informáticos: red, endpoint, aplicación web, mensajería y navegación web.

Contar con un aliado estratégico

En redes ópticas entendemos bien esta situación, por eso hemos desarrollado un conjunto de soluciones de ciberseguridad que se enfocan en cada uno de los cinco vectores de ataque con un enfoque proactivo.

De esta forma, podemos combinar diferentes soluciones para que se comuniquen entre sí y aprendan a través de la inteligencia artificial y el aprendizaje automático a identificar, mitigar, aislar y prevenir diferentes tipos de ataques informáticos antes de que sucedan. Causan más daños, especialmente a la infraestructura crítica.

### 2.2.2 Base teórica Variables dependiente y sus indicadores)

### Variable independiente: SISTEMAS INFORMÁTICOS

En redes ópticas entendemos bien esta situación, por eso hemos desarrollado un conjunto de soluciones de ciberseguridad que se enfocan en cada uno de los cinco vectores de ataque con un enfoque proactivo.

De esta forma, podemos combinar diferentes soluciones para que se comuniquen entre sí y aprendan a través de la inteligencia artificial y el aprendizaje automático a identificar, mitigar, aislar y prevenir diferentes tipos de ataques informáticos antes de que sucedan. Causan más daños, especialmente a la infraestructura crítica.

Las partes de un sistema informático son:

• Componente físico: está formado por todos los aparatos electrónicos y mecánicos que realizan los cálculos y el manejo de la información.

• Componente lógico: se trata de las aplicaciones y los datos con los que trabajan los componentes físicos del sistema.

• Componente humano: está compuesto tanto por los usuarios que trabajan con los equipos como por aquellos que elaboran las aplicaciones.

Estructura de un sistema informático

Los sistemas informáticos suelen estructurarse en Subsistemas.

Subsistema físico: Asociado al hardware, Son todos aquellos componentes físicos del ordenador, es decir, todo lo que se puede ver y tocar. Incluye entre otros elementos la CPU, memoria principal, la placa base, periféricos de entrada y salida.

Subsistema lógico: Asociado al software, Son las instrucciones que el ordenador necesita para funcionar, no existen físicamente, o lo que es igual, no se pueden ver ni tocar.  y la arquitectura. Incluye al sistema operativo, el firmware, las aplicaciones y las bases de datos.

## Clasificación de sistemas informáticos

Los sistemas informáticos hoy en día se dividen en diferentes 6 clases, flexible y versátil de acuerdo al entorno en el cual se implementan. Estos son:

### Sistemas de apoyo a la toma de decisiones

Un Sistema informático de apoyo a la toma de decisiones, también conocido como "Sistema de soporte a la decisión" o DSS (Decision Support System) por sus siglas en inglés, básicamente es un sistema basado en computadoras diseñado con el propósito de ser usado por una gerencia o gerencia de área para ayudarlos en el proceso de tomar una decisión para resolver problemas y con ello poder diagramar las directrices para seleccionar la mejor opción o predecir los futuros escenarios para afrontar nuevos desafíos.

### Sistema de control de procesos de negocio

Los Sistemas de control de procesos de negocio, conocidas también como "BPM" del inglés "Business Process Management" son aquellos sistemas encargados de monitorizar, controlar y gestionar cualquier proceso de industrialización. En este tipo de sistema informático, se utilizan sensores electrónicos conectados a computadoras para poder hacer un monitoreo directo del proceso que la maquinaria está realizando, con el objetivo de controlar que el mismo se lleve a cabo con total eficacia.

### Sistemas de colaboración empresarial

Los sistemas ERP, por sus siglas en inglés "Enterprise resource planning" son uno de los más claros ejemplos de sistema informático. Los sistemas ERP, conocidos en español como "Sistemas de colaboración empresarial", son el tipo de sistema informático más utilizado por empresas alrededor del mundo, ya que le permiten a las compañías a gestionar la gran cantidad de información que circula dentro de la misma.

La particularidad del ERP es que es un sistema informático que no es de uso específico de un nivel puntual de una compañía, ya que pueden brindar servicios a un abanico importante de usuarios en muchas áreas de la empresa.

Sistemas de Información Ejecutiva

Los Sistemas de información ejecutiva o “Executive information system”, conocida también como EIS por sus siglas en inglés, es un sistema informático capaz de proporcionar acceso inmediato a toda la variedad de información crítica que produce la empresa, tanto de fuentes internas como externas, la cual se presenta en formas variadas, de acuerdo a la necesidad de profundizar que se tenga en esta información, siempre en un formato que pueda ser fácilmente visualizado y comprendido en una simple mirada.

Al igual que los sistemas de información ejecutiva, en el caso de los sistemas informáticos los mismos han sido desarrollados con el objetivo de generar todo tipo de datos e información, la cual se caracteriza por ser lo suficientemente compacta, es decir en una versión simplificada la cual presenta toda la operación de la empresa, y de esta forma pueda ser analizada de forma rápida, pero a la vez confiable. Tiene como meta brindarles todos los datos necesarios a los altos directivos de la compañía a través de dicho sistema informático, para que de esta manera puedan tomar decisiones estratégicas correctas.

Sistemas de procesamiento de transacciones

Los Sistemas de Procesamiento de Transacciones, o "Sistemas de Procesamiento de Transacciones" o "TPS" se utilizan para aumentar todo lo relacionado con el estado operativo a nivel organizacional, que son sistemas informáticos con puntos adicionales complementarios que es la profesión básica.

Básicamente, un sistema de procesamiento de transacciones es un sistema informático que registra, evalúa y desarrolla transacciones que ocurren durante el día y es necesario para el funcionamiento normal de cualquier negocio. Estos tipos de sistemas de TI se encuentran en la parte inferior de la jerarquía relacionada con una organización y son en sí mismos la base de un sistema de TI para las operaciones diarias de la empresa.

Sistemas de Información de Gestión

Un sistema de información de gestión, también conocido en inglés como "Sistema de información de gestión", abreviado como "MIS", es un sistema informático capaz de recopilar y valorar datos de muchos estados con el fin de obtener una visión más amplia y aún más clara al hacer negocios. decisiones. decisiones. La característica más importante de un sistema informático de este tipo es la capacidad de generar informes, lo que es muy útil para la gestión de operaciones, y el control total de todas las actividades de procesamiento de transacciones realizadas a niveles de gestión.

Significa que un sistema de gestión computarizado es un tipo de sistema que proporciona datos internos y cuyo principal objetivo es procesar y agregar toda esta información en informes que luego serán utilizados para apoyar las actividades de gestión y toma de decisiones en la empresa.

¿Cómo funcionan los sistemas informáticos? En un sistema informático, los datos se ingresan a través de dispositivos de entrada (por ejemplo, un teclado), los datos se emiten o se recuperan a través de dispositivos de salida (por ejemplo, monitores) y también hay un dispositivo de entrada / salida, que se utiliza para ingresar y borrar datos en una computadora (por ejemplo, un enrutador).

**Indicador 1: Red informática**

Se cree que es por una red informática, una red de comunicación de datos o una red informática con varios sistemas informáticos interconectados por una serie de dispositivos cableados o inalámbricos a través de los cuales pueden compartir información. Información en paquetes de datos, transmitida por pulsos eléctricos, electromagnéticos, ondas o cualquier otro medio físico.

Elementos de una red informática Normalmente, una red informática presenta los siguientes elementos:

Servidor. En una red, las computadoras no siempre tienen la misma jerarquía o las mismas funciones. Los servidores son máquinas que procesan flujos de datos, sirven

a todos los demás ordenadores de la red ("les sirven", de ahí el nombre) y controlan de forma centralizada la red.

Cliente o estación de trabajo. Es el nombre que se le da a los equipos que no son servidores, pero que forman parte de una red, y permiten que los usuarios accedan a ellos, utilizando recursos administrados por el servidor.

Medios de transmisión. Este es el nombre que se le da al cableado eléctrico u ondas electromagnéticas que, en su caso, permiten transmitir información.

Factores materiales. Partes que permiten la interconexión física, como la tarjeta de red en cada computadora, módems y enrutadores que soportan la transmisión de datos, o antenas repetidoras que extienden la conexión (en el caso de las inalámbricas).

Elementos de software. Finalmente, están los programas necesarios para administrar y operar el hardware de comunicación, y esto incluye el Sistema Operativo de Red (NOS), que además de hacerse cargo del funcionamiento de la red, también brinda soporte antivirus-desenchufar y firewall; y protocolos de comunicación (como TCP e IP) que permiten que las máquinas "hablen" el mismo idioma. Las redes informáticas se clasifican según su tamaño en:

LAN. Un acrónimo de Local Area Network (en inglés: "Local Area Network"), estas son las redes más pequeñas, como las que existen en una cabina telefónica, un café de la red o un apartamento.

Red MAN. El acrónimo Metropolitan Area Network ("Metropolitan Area Network") se refiere a redes de tamaño medio, como las que se utilizan en los campus universitarios o en bibliotecas o grandes empresas, que conectan diferentes regiones distantes entre sí.

WAN. El acrónimo de Wide Area Network (en inglés: "Wide Area Network"), se refiere a redes de mayor alcance y alcance, como la red global, Internet. También suelen clasificarse según la tecnología a la que están conectadas las computadoras, de la siguiente manera:

Redes de medios guiadas. Las computadoras se entrelazan entre computadoras a través de un sistema de cableado físico, como un par trenzado, coaxial o cable de fibra óptica.

Las redes multimedia no son compatibles. Conectan sus computadoras a través de medios ampliamente distribuidos y distribuidos, como ondas de radio, infrarrojos o microondas.

Indicador 2: Aplicativos

Siempre será preciso alguna introducción para comenzar a hablar de aplicativos, el medio para sacar todo el jugo a las capacidades funcionales del PC (personal computer).

Las aplicaciones de consumo, productividad y entretenimiento han atravesado una metamorfosis a medida que los sistemas operativos han evolucionado, se han adaptado a las capacidades de cada ecosistema y están limitados por la ingeniería de software. El sistema de escritorio está dominado por código (MSDOS), a través de un sistema de iconos (MS Windows y Mac OS X), y termina con los sistemas operativos móviles (Android, Windows Phone, IOS). Las aplicaciones han mejorado con el tiempo, acumulando más funciones y aumentando la productividad, todo lo cual conduce a una mejor vida laboral y personal para las personas.

sistemas operativos para PC o dispositivos móviles: el tamaño de un archivo digital se expresa en bytes de números, y generalmente se trata de kilobytes, megabytes, gigabytes o terabytes.

Desde el punto de vista de la programación, cada archivo es parte del dispositivo y ejecución de un juego o programa, cada uno de los cuales cumple una función específica a lo largo del proceso. Como resultado, todos los archivos no desempeñarán la misma función y proporcionarán la misma información en la salida final y general de un programa: la extensión del archivo, precedida por un "punto", determinará su función.

Los archivos son elementos que forman parte del mundo digital más amplio, algunos más visibles que otros, pero todos

**Indicador 3: Información**

La Información es importante cuando se habla de la función informática y generalmente se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente. Por lo cual, hay que saber lo que muchas veces es complicado dentro de la función informática, de forma especial y primordial cuando su maniobrabilidad está basada en tecnología moderna, para esto, se debe conocer que la información esta almacenada y procesada en computadoras, que puede ser confidencial para algunas personas o a escala institucional, que puede ser mal utilizada o divulgada y que puede estar sujeta a robos, sabotaje o fraudes. Los sistemas de información están cambiando en la actualidad la forma en que operan las organizaciones. Mediante su uso se obtienen grandes mejoras, ya que automatizan los procesos operativos que se pueden llevar a cabo en toda empresa, proporcionan información de apoyo al proceso de tomas de decisiones y facilitan el logro de ventajas competitivas a través de su implantación dentro de la organización. Los sistemas de información han llegado para quedarse por su gran utilidad como herramienta complementaria en diferentes áreas, ya sea en lo personal, empresarial (gestión de recursos humanos, procesamiento de transacciones, gerencial o administrativas, toma de decisiones) y comunicacional, entre otros.

Los sistemas de información abarcan: equipos (hardware) y programas informáticos (Software), telecomunicaciones, bases de datos, recursos humanos y procedimientos. (García Bravo, 2000). Los equipos que hoy en día se usan con más frecuencia en las empresas por lo general son los ordenadores personales o PC.; los programas informáticos son de dos (2) tipos: del sistema que administran los recursos del sistema computarizado y simplifican la programación y las aplicaciones que ayudan directamente al usuario final a hacer su trabajo, un ejemplo sería programas de hoja de cálculo o procesadores de texto; las telecomunicaciones son medio de transmisión electrónica de información a largas distancias y computadoras conectadas en redes; el

recurso humano se distingue entre personas especialistas en sistemas de información (analistas de sistemas, programadores y operadores) y usuarios finales que son la mayoría de personas de una organización que utilizan los sistemas de información que generan los especialistas. Un ejemplo sería el que ejecuta el programa de pago de nómina y el que está autorizado para ejecutarlo y que tiene acceso a los informes producidos. Los sistemas de información son desarrollados en las empresas para ayudar en el desempeño de las tareas que se prevén realizar. Así, podemos encontrar un sistema de registros médicos en un hospital, un sistema de registros criminales en las comisarías, un sistema de pago de nóminas en todas las empresas, sistemas de inventarios en los auto mercados, sistemas de automatización de oficinas, sistemas de automatización de bibliotecas, sistemas de automatización de la gestión jurídica, entre otros.

**Marco Conceptual (glosario de términos)**

**Información. -** son datos procesados que engloban un mensaje que habilita un nuevo conocimiento a la persona o sistema que reciba dicho mensaje.

**Datos. -** son hechos que han sido registrados de manera cuantitativa o cualitativa.

**Seguridad. -** es una característica de alguna persona o máquina que esta con ausencia de peligro.

**Sistema. -** es un conjunto de medidas o procedimientos que guían el correcto funcionamiento de un grupo.

**Estándar. -** es aquel que sirve de patrón, punto de referencia para medir la valoración de cosas, organizaciones de la misma especie.

**Organización. -** es un ajuste sistemático entre personas que desean alcanzar algún propósito en común.

**Ciberataque. -** es una maniobra ofensiva hecha por individuos u organizaciones con el fin de dañar los diferentes tipos de sistemas informáticos.

**Ciberespacio. -** es aquel espacio virtual creado por medios cibernéticos con el propósito que transportemos información a través de las redes.

**Cibercrimen. -** es un crimen que se realiza a través de línea o de redes cibernéticas y logra afectar computadores o cualquier dispositivo red que se asocie con informática.

**Gestión de riesgos. -** proceso para la determinación de medidas necesarias para la protección de algún servicio.

**Infraestructuras críticas. -** sistemas físicos o virtuales que dan facilidad de funciones y servicios primordiales para ayudar a los sistemas básicos.

**Ciberdelincuentes. -** persona que realiza acciones delictivas mediante el medio de internet.

# CAPÍTULO III: HIPÓTESIS Y VARIABLES

## 3.1 Formulación de Hipótesis

### 3.1.1 Hipótesis general

Los Estándares de Ciberseguridad de los Sistemas Informáticos en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2021 es importante porque mejora significativamente la seguridad y confianza a cada usuario que forma parte de la Institución al tener un grado superior de protección en su Ciberseguridad.

### 3.1.2 Hipótesis especificas

Los Estándares de Ciberseguridad ayuda al usuario a comprender las diferentes amenazas que existe en la red de los Sistemas Informáticos en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2021.

Los Estándares de Ciberseguridad al formar parte de la institución favorece la determinación de fallos técnicos que existe en las aplicaciones de los Sistemas Informáticos en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2021.

Los Estándares de Ciberseguridad mejora la exclusividad que pueda tener la información de los Sistemas Informáticos en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2021.

### 3.2 Definición conceptual y operacional de las variables

| VARIABLES | INDICADORES | DEFINICIÓN CONCEPTUAL |
|---|---|---|
| Variable 1<br><br>Estándares de Ciberseguridad | Seguridad de la información | Encargada de asegurar las redes informáticas de los ciber terroristas |
| | | Por lo cual se adopta medidas preventivas y reactivas que puedan proteger o proteger la información almacenada en esta red. |
| | Seguridad de las redes | Es aquel que gestiona el acceso a la red |
| | Seguridad de internet | Es un conjunto de precauciones que se adoptan para proteger todos los elementos de la red, como la infraestructura y la información, que se ven más afectados por el ciberdelito. |
| | Protección de las infraestructuras críticas de la información | Las infraestructuras críticas de las ciudades como plantas de tratamiento de agua, presas hidroeléctricas, centrales nucleares, oleoductos, gasoductos, entre otros. |
| **Variable 2** | Red Informática | Se le dice por redes informáticas, redes de comunicaciones de datos o redes de computadoras a un número de sistemas informáticos conectados entre sí |

| VARIABLES | INDICADORES | DEFINICIÓN CONCEPTUAL |
|---|---|---|
| Sistemas Informáticos | | mediante una serie de dispositivos alámbricos o inalámbricos |
| | | Por lo que se puede compartir información en paquetes de datos, transmitidos mediante impulsos eléctricos, ondas electromagnéticas o cualquier otro medio físico. |
| | Aplicativos | Las aplicaciones representan realizar una actividad y obtener un beneficio de ello. |
| | | Las aplicaciones son las herramientas que hacen que nosotros mismos impulsemos y vayamos más allá de nuestra imaginación y creatividad. |
| | Información | Es de gran importancia cuando se habla de la función informática y muchas veces se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente. |
| | | Los sistemas de información engloban: equipos (hardware) y programas informáticos (Software), telecomunicaciones, bases de datos, recursos humanos y procedimientos. |

### 3.3 Cuadro de operacionalización de variables

| Variables | | Indicadores |
|---|---|---|
| Variable Independiente | Estándares de ciberseguridad | Seguridad de la información |
| | | Seguridad de las redes |
| | | Seguridad de la información |

| Variables | | Indicadores |
|---|---|---|
| | | Protección de las infraestructuras críticas de la información. |
| Variable Dependiente | Sistemas informáticos | Red informática |
| | | Aplicativos |
| | | Información |

## CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

### 4.1 Método de estudio

(Iberico Collazos, 2019) "Se encarga de buscar el porqué de los hechos mediante el establecimiento de relaciones causa-efecto". (p. 67)

(Iberico Collazos, 2019) "En este sentido, los estudios explicativos pueden ocuparse tanto de la determinación de las causas (investigación postfacto), como de los efectos (investigación experimental), mediante la prueba de hipótesis. Sus resultados y conclusiones constituyen el nivel más profundo de conocimientos". (p. 68)

### 4.2 Enfoque de la Investigación

El tipo de Investigación es cuantitativa, porque es preponderante el estudio de los datos se basa en la cuantificación y cálculo de los mismos.

(Iván & Toro , 2005) "Dicen que la investigación Cuantitativa tiene una concepción lineal, es decir que haya claridad entre los elementos que conforman el problema, que tenga definición, limitarlos y saber con exactitud donde se inicia el problema y qué tipo de incidencia existe entre sus elementos". (p. 1)

## 4.3 Tipo de Investigación

El Tipo de Investigación es Básica

## 4.4 Nivel y Diseño de la Investigación

(CUBA, 2019) "El diseño que se utilizará en la Investigación será el No experimental, el cual se define como un diseño de un solo grupo cuyo grado de control es mínimo." (p. 68)

(CUBA, 2019) "Generalmente es útil como primer acercamiento al problema de investigación. También se utiliza el diseño de medición de pre prueba / pos prueba con un único grupo, ya que se aplica una prueba previa al estímulo, luego se administra tratamiento para finalizar con la prueba posterior al estímulo; tomando el nivel de referencia que tenía inicialmente el grupo de estudio". (p. 69)

## 4.5 Técnicas e Instrumentos para la recolección de datos

### Técnica

- Encuesta: Puede definirse como un conjunto de técnicas destinadas a reunir, de manera sistemática, datos sobre determinado tema o temas relativos a una población, a través de contactos directos o indirectos con los individuos o grupos de individuos que integran la población (Zapata, 2005, p.189).
- (Palella, 2012) "La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones interesan al investigador. A diferencia de la entrevista, se utiliza un listado de preguntas que se entregan a los sujetos quienes, en forma anónima, las responden por escrito." (p. 17).

- Es una técnica aplicable a sectores amplios del universo, de manera mucho más económica que mediante entrevistas individuales

**Instrumento**

El cuestionario es un instrumento de investigación que forma parte de la técnica de la encuesta. Es fácil de usar, popular y con resultados directos. El cuestionario, tanto en su forma como en su contenido, debe ser sencillo de contestar. Las preguntas han de estar formuladas de manera clara y concisa; pueden ser cerradas, abiertas o semi abiertas, procurando que la respuesta no sea ambigua. Como parte integrante del cuestionario o en documento separado, se recomienda incluir unas instrucciones breves, claras y precisas, para facilitar su solución. Seguidamente se presenta y resumen de las dificultades más frecuentes en la elaboración de cuestionarios".

## 4.6 Población y Muestra

### 4.6.1 Población

"Totalidad de unidades de análisis del conjunto a estudiar, conjunto de individuos, objetos, elementos o fenómenos en los cuales puede presentarse determinada característica susceptible de ser estudiada"

Entonces cuando hablamos de población comprendemos que se refiere a la totalidad del objeto a estudiar. La población del presente trabajo de investigación estuvo conformada por los cadetes del arma de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

### 4.6.2 Muestra

Se tiene como muestra censal a los 64 cadetes de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

# CAPÍTULO V: INTERPRETACIÓN, ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

## 5.1 Análisis descriptivo

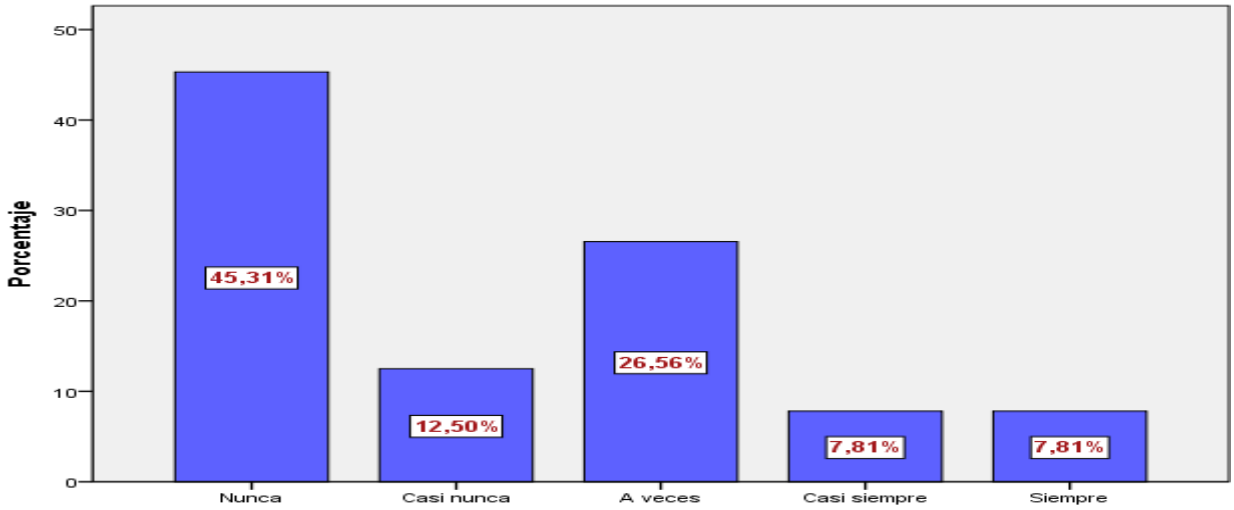
*¿Considera usted que los sistemas informáticos en la EMCH están seguros y funcionan en forma adecuada?*

**Tabla 011: Pregunta 1: ¿Considera usted que los sistemas informáticos en la EMCH están seguros y funcionan en forma adecuada?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 29 | 45,3 | 45,3 | 45,3 |
| | Casi nunca | 8 | 12,5 | 12,5 | 57,8 |
| | A veces | 17 | 26,6 | 26,6 | 84,4 |
| | Casi siempre | 5 | 7,8 | 7,8 | 92,2 |
| | Siempre | 5 | 7,8 | 7,8 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

### Interpretación Análisis descriptivo

En cuanto a la interrogante si considera usted que los sistemas informáticos en la EMCH están seguros y funcionan en forma adecuada; manifestaron que Nunca 45.3%; por su parte dijeron que A veces 26.6%; el 12.5% dijeron que Casi nunca; 7.8% manifestaron que Casi siempre y, por último, el 7.8% dijeron que Siempre.



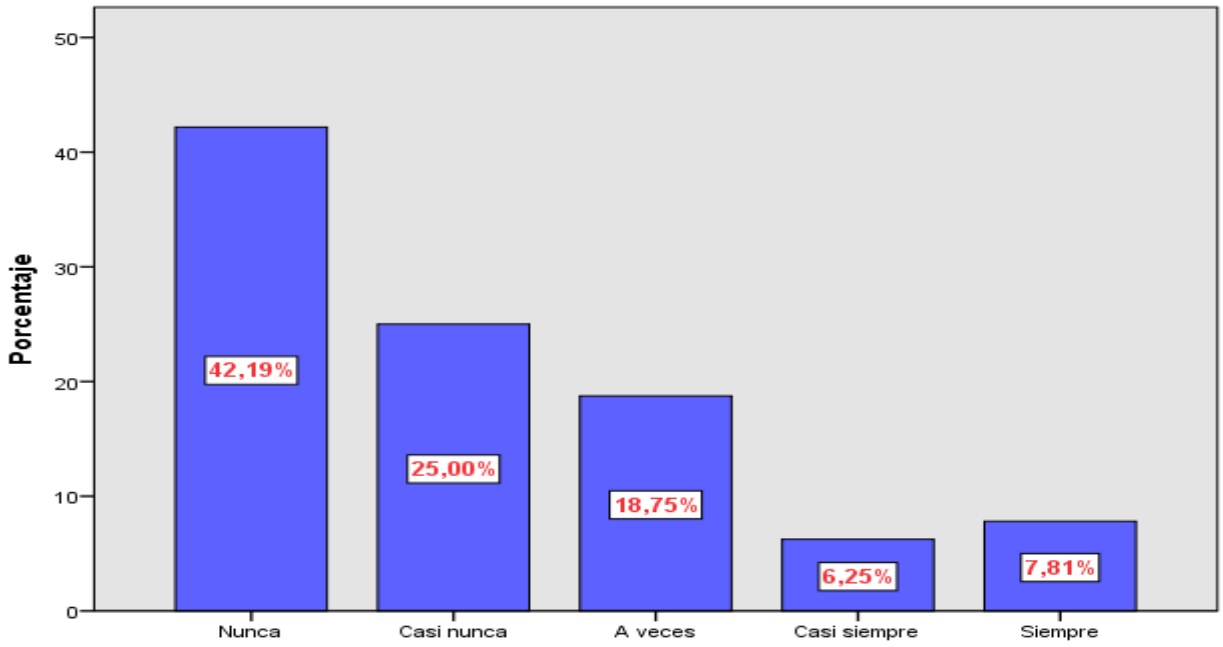
¿Consideras que los cadetes extreman medidas de Ciberseguridad en los Sistemas Informáticos?

**Tabla 022: Pregunta 2:¿Consideras que los cadetes extreman medidas de Ciberseguridad en los Sistemas Informáticos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 27 | 42,2 | 42,2 | 42,2 |
| | Casi nunca | 16 | 25,0 | 25,0 | 67,2 |
| | A veces | 12 | 18,8 | 18,8 | 85,9 |
| | Casi siempre | 4 | 6,3 | 6,3 | 92,2 |
| | Siempre | 5 | 7,8 | 7,8 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si considera usted que los cadetes extreman medidas de Ciberseguridad en los Sistemas Informáticos; manifestaron que Nunca el 42.2%; por otra parte, dijeron que Casi nunca el 25%; el 18.8% dijeron que A veces; 6.3% manifestaron que Casi siempre; por último, el 7.8% dijeron que Siempre.



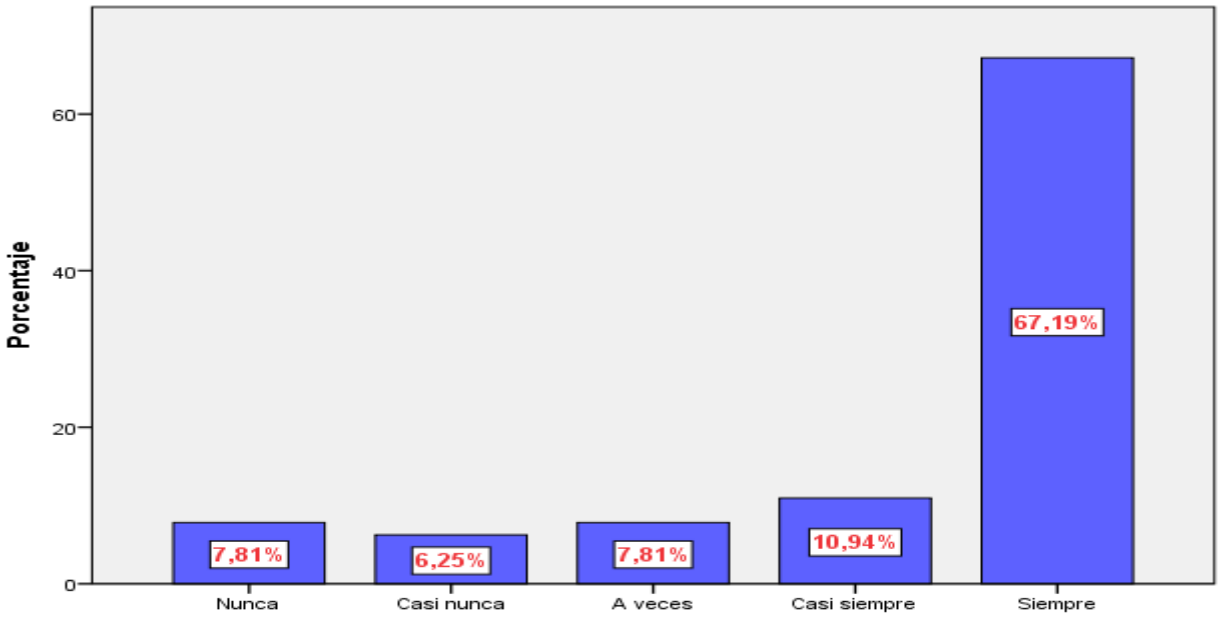
1. ¿Considera usted importante la seguridad de las redes en la EMCH “CFB”?

**Tabla 033: Pregunta 3:¿Considera usted importante la seguridad de las redes en la EMCH "CFB"?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 5 | 7,8 | 7,8 | 7,8 |
| | Casi nunca | 4 | 6,3 | 6,3 | 14,1 |
| | A veces | 5 | 7,8 | 7,8 | 21,9 |
| | Casi siempre | 7 | 10,9 | 10,9 | 32,8 |
| | Siempre | 43 | 67,2 | 67,2 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

Se aprecia que en la interrogante si considera usted importante la seguridad de las redes en la EMCH “CFB”, el 67.2% de los encuestados manifestaron que Siempre; el 7.8% dijeron que A veces, 10.9% manifestaron que Casi siempre; dijeron que Casi nunca el 6.3% de los encuestados y el 7.8% de los encuestados manifestaron que Nunca.



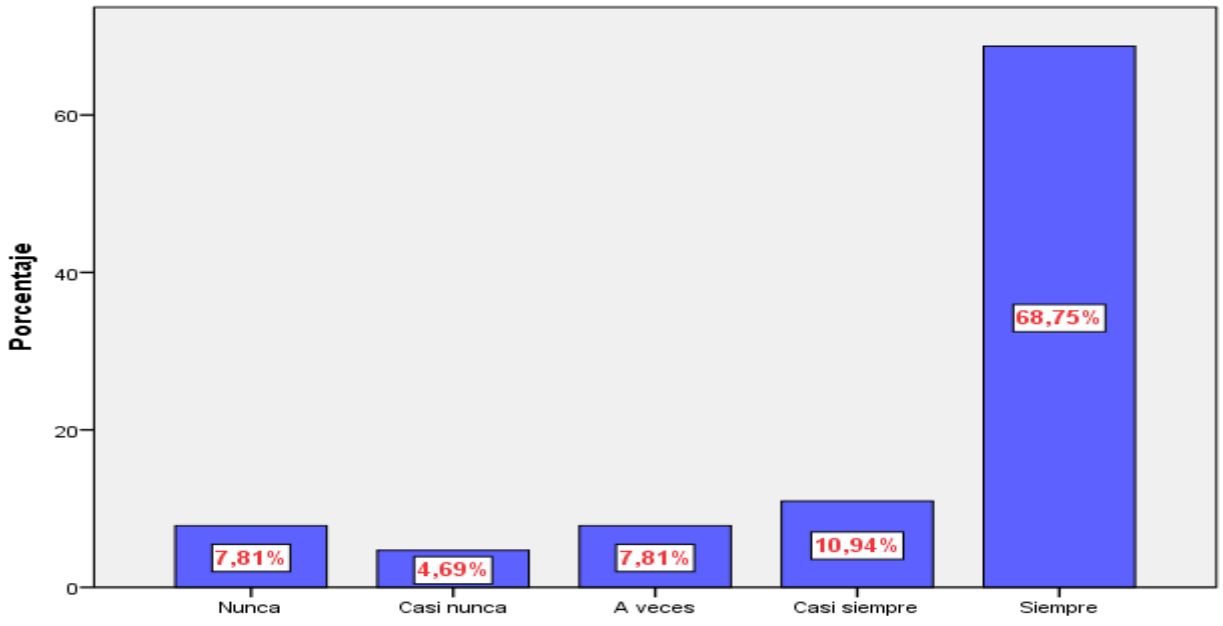
4. ¿Considera usted importante la seguridad de la información en la EMCH “CFB”?

**Tabla 044: Pregunta 4:¿Considera usted importante la seguridad de la información en la EMCH "CFB"?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 5 | 7,8 | 7,8 | 7,8 |
| | Casi nunca | 3 | 4,7 | 4,7 | 12,5 |
| | A veces | 5 | 7,8 | 7,8 | 20,3 |
| | Casi siempre | 7 | 10,9 | 10,9 | 31,3 |
| | Siempre | 44 | 68,8 | 68,8 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

Se aprecia que en la interrogante si considera usted importante la seguridad de la información en la EMCH “CFB”, el 68.8% de los encuestados manifestaron que Siempre; el 10.9% dijeron que Casi siempre; el 7.8% dijeron que Nunca, otro 7.8% dijeron que A veces y el 4.7% de encuestados manifestaron que Casi nunca.



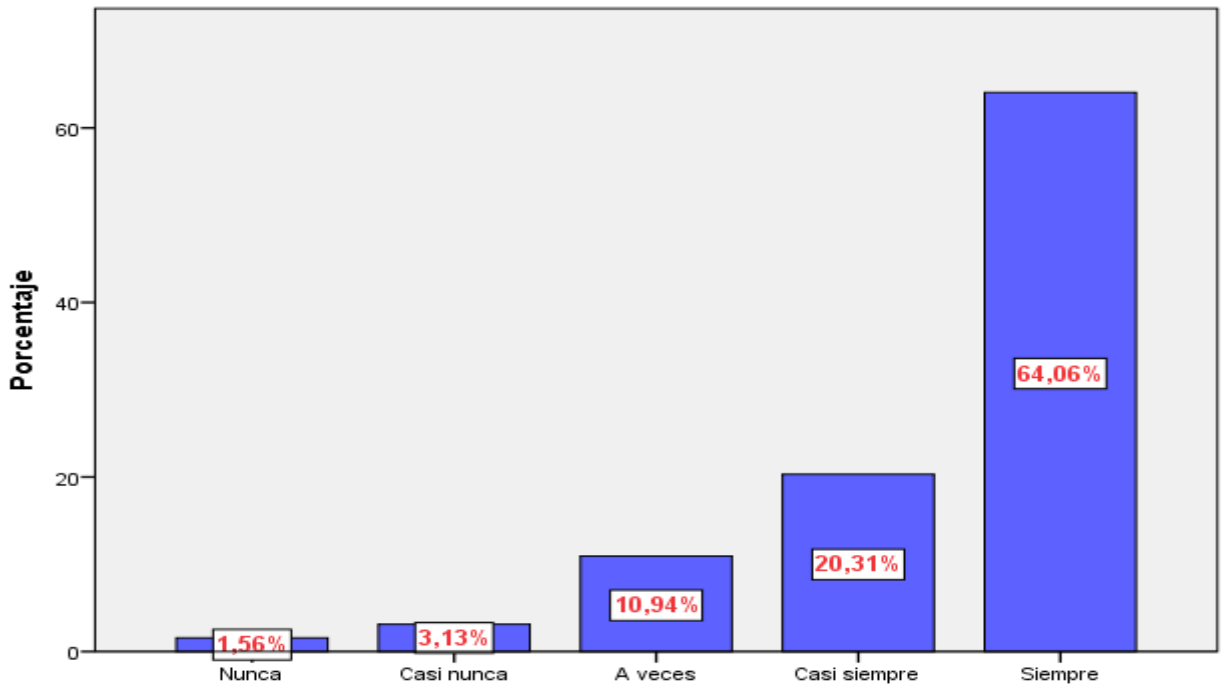
5. ¿Considera usted importante la seguridad de internet en la EMCH “CFB”?

**Tabla 055: Pregunta 5: ¿Considera usted importante la seguridad de internet en la EMCH "CFB"?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 1 | 1,6 | 1,6 | 1,6 |
| | Casi nunca | 2 | 3,1 | 3,1 | 4,7 |
| | A veces | 7 | 10,9 | 10,9 | 15,6 |
| | Casi siempre | 13 | 20,3 | 20,3 | 35,9 |
| | Siempre | 41 | 64,1 | 64,1 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si considera usted importante la seguridad de internet en la EMCH “CFB”, el 64.1% de los encuestados manifestaron que Siempre; el 20.3% dijeron que Casi siempre; el 1.6% dijeron que Nunca, otro 10.9% dijeron que A veces y el 3.1% de encuestados manifestaron que Casi nunca.

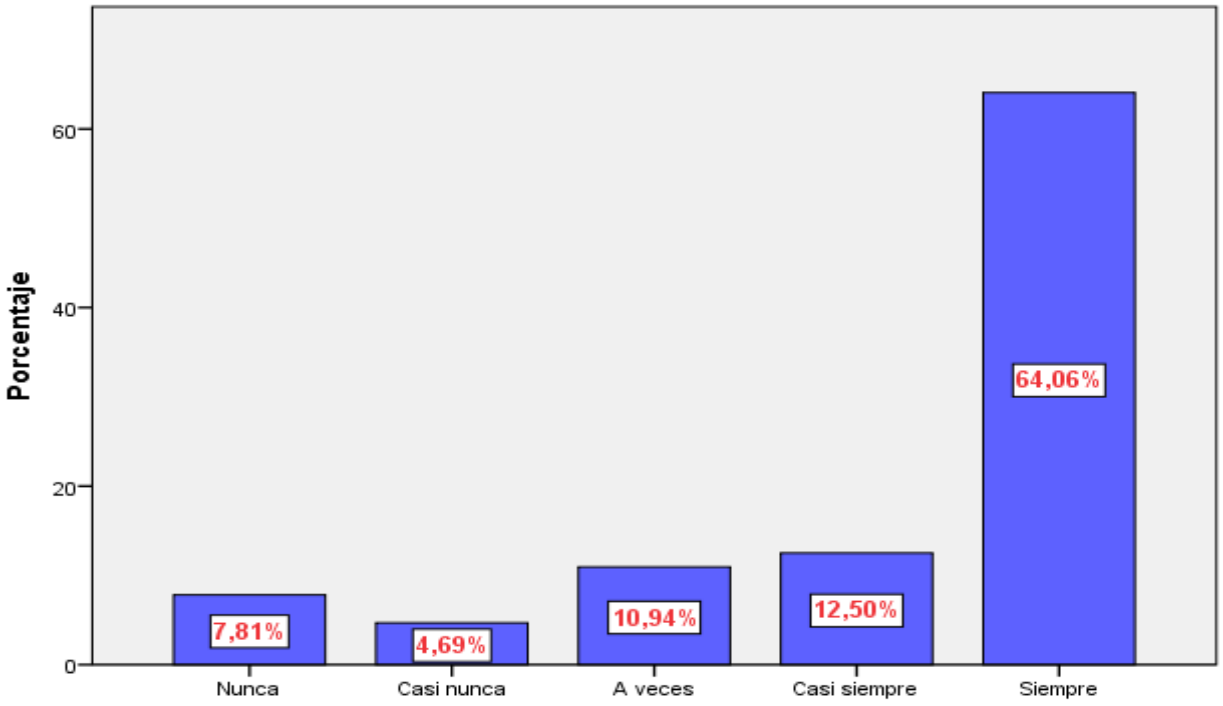


6. ¿Considera usted importante la protección de las infraestructuras críticas de la información?

**Tabla 066: Pregunta 6:¿Considera usted importante la protección de las infraestructuras críticas de la información?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 5 | 7,8 | 7,8 | 7,8 |
| | Casi nunca | 3 | 4,7 | 4,7 | 12,5 |
| | A veces | 7 | 10,9 | 10,9 | 23,4 |
| | Casi siempre | 8 | 12,5 | 12,5 | 35,9 |
| | Siempre | 41 | 64,1 | 64,1 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

En cuanto a la interrogante si considera usted importante la protección de las infraestructuras críticas de la información, el 64.1% de los encuestados manifestaron que Siempre; el 12.5% dijeron que Casi siempre; el 7.8% dijeron que Nunca, otro 10.9% dijeron que A veces y el 4.7% de encuestados manifestaron que Casi nunca.



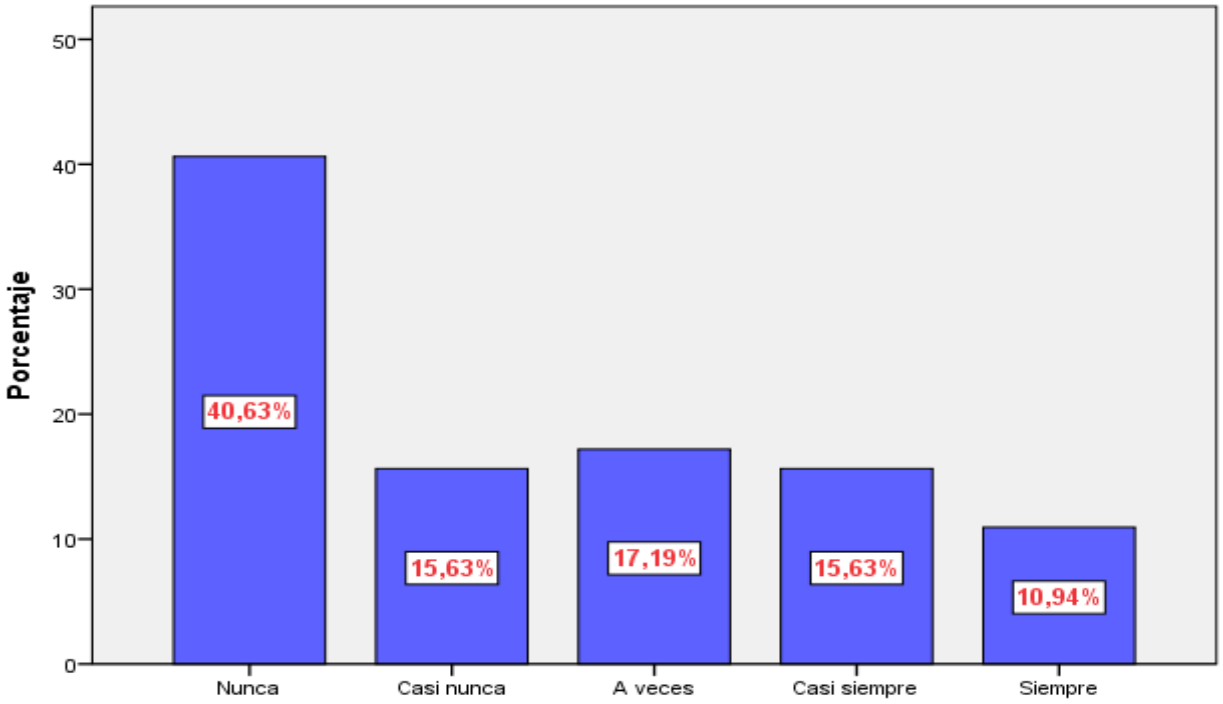
7. ¿Consideras que la EMCH “CFB” tiene la capacidad de combatir o evadir algún ciberataque?

**Tabla 077: Pregunta 7: ¿Consideras que la EMCH "CFB" tiene la capacidad de combatir o evadir algún ciberataque?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 26 | 40,6 | 40,6 | 40,6 |
| | Casi nunca | 10 | 15,6 | 15,6 | 56,3 |
| | A veces | 11 | 17,2 | 17,2 | 73,4 |
| | Casi siempre | 10 | 15,6 | 15,6 | 89,1 |
| | Siempre | 7 | 10,9 | 10,9 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si considera que la EMCH “CFB” tiene la capacidad de combatir o evadir algún ciberataque, el 10.9% de los encuestados manifestaron que Siempre; el 15.6% dijeron que Casi siempre; el 40.6% dijeron que Nunca, otro 17.2% dijeron que A veces y el 15.6% de encuestados manifestaron que Casi nunca.



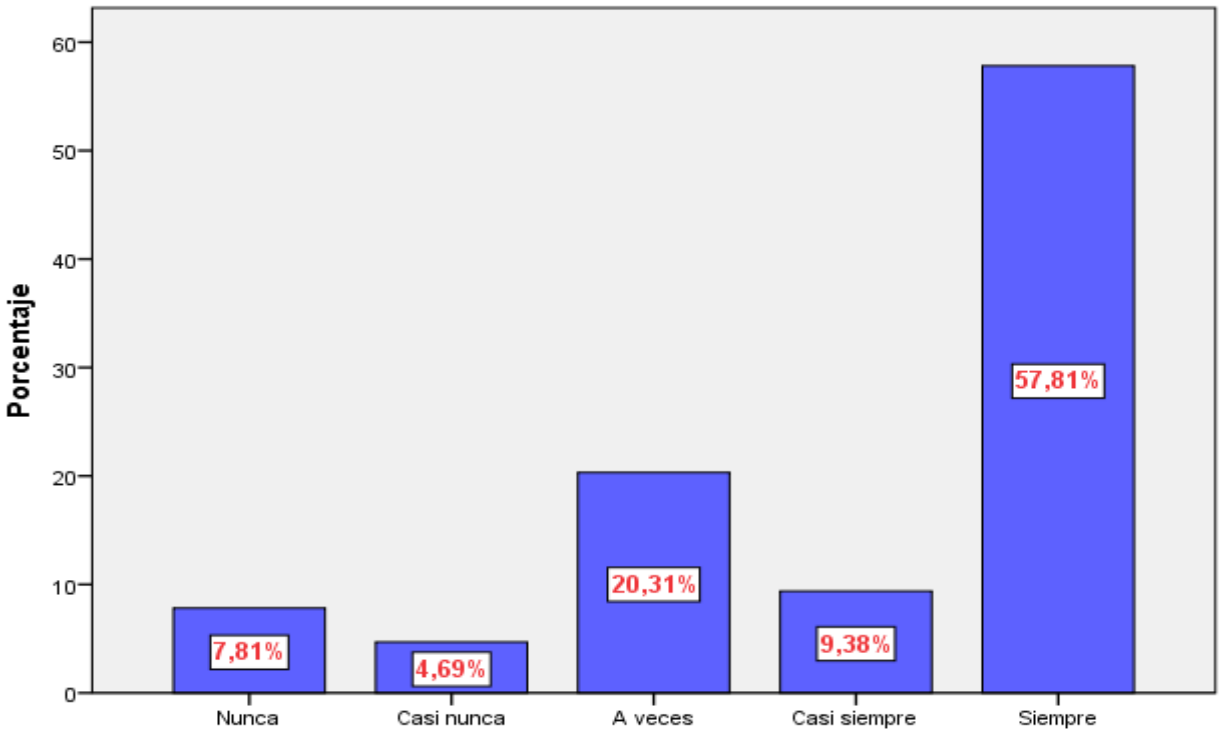
8. ¿Consideras importante tener experiencia en el ámbito de Ciberseguridad en los Sistemas Informáticos?

**Tabla 088: Pregunta 8:¿Consideras importante tener experiencia en el ámbito de Ciberseguridad en los Sistemas Informáticos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 5 | 7,8 | 7,8 | 7,8 |
| | Casi nunca | 3 | 4,7 | 4,7 | 12,5 |
| | A veces | 13 | 20,3 | 20,3 | 32,8 |
| | Casi siempre | 6 | 9,4 | 9,4 | 42,2 |
| | Siempre | 37 | 57,8 | 57,8 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si consideras importante tener experiencia en el ámbito de Ciberseguridad en los Sistemas Informáticos, el 57.8% de los encuestados manifestaron que Siempre; el 9.4% dijeron que Casi siempre; el 7.8% dijeron que Nunca, otro 20.3% dijeron que A veces y el 4.7% de encuestados manifestaron que Casi nunca.



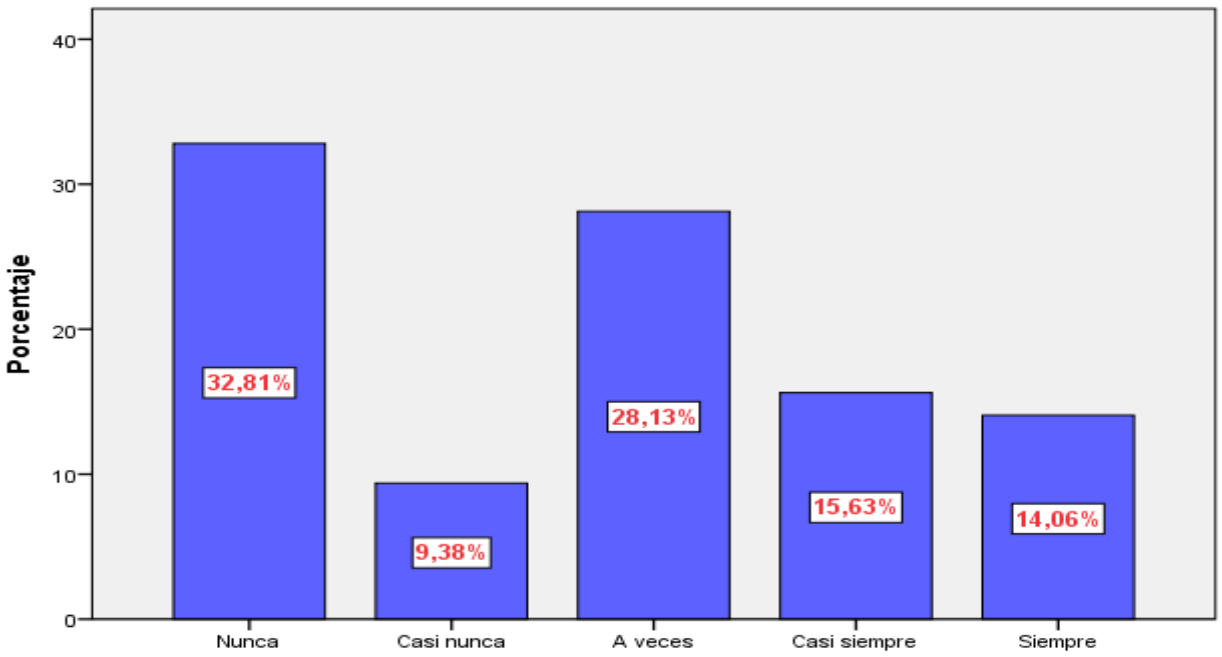
9. ¿Consideras que los aplicativos de los Sistemas Informáticos de la EMCH son seguros?

**Tabla 099: Pregunta 9:¿Consideras que los aplicativos de los Sistemas Informáticos de la EMCH son seguros?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 21 | 32,8 | 32,8 | 32,8 |
| | Casi nunca | 6 | 9,4 | 9,4 | 42,2 |
| | A veces | 18 | 28,1 | 28,1 | 70,3 |
| | Casi siempre | 10 | 15,6 | 15,6 | 85,9 |
| | Siempre | 9 | 14,1 | 14,1 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si consideras que los aplicativos de los sistemas informáticos de la EMCH son seguros, el 14.1% de los encuestados manifestaron que Siempre; el 15.6% dijeron que Casi siempre; el 32.8% dijeron que Nunca, otro 28.1% dijeron que A veces y el 9.4% de encuestados manifestaron que Casi nunca.



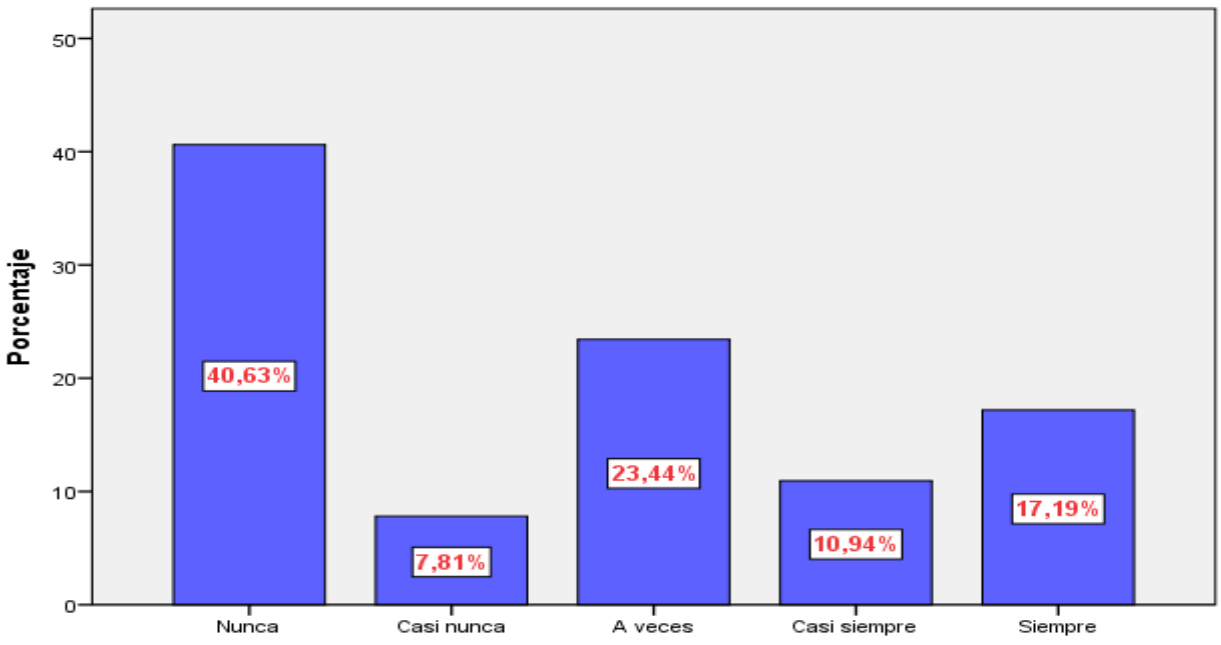
10. ¿Consideras que la red informática es la adecuada y confiable para los cadetes de la EMCH “CFB”?

**Tabla 1010: Pregunta 10:¿Consideras que la red informática es la adecuada y confiable para los cadetes de la EMCH "CFB"**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 26 | 40,6 | 40,6 | 40,6 |
| | Casi nunca | 5 | 7,8 | 7,8 | 48,4 |
| | A veces | 15 | 23,4 | 23,4 | 71,9 |
| | Casi siempre | 7 | 10,9 | 10,9 | 82,8 |
| | Siempre | 11 | 17,2 | 17,2 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si consideras que la red informática es la adecuada y confiable para los cadetes de la EMCH “CFB”, el 17.2% de los encuestados manifestaron que Siempre; el 10.9% dijeron que Casi siempre; el 40.6% dijeron que Nunca, otro 23.4% dijeron que A veces y el 7.8% de encuestados manifestaron que Casi nunca.



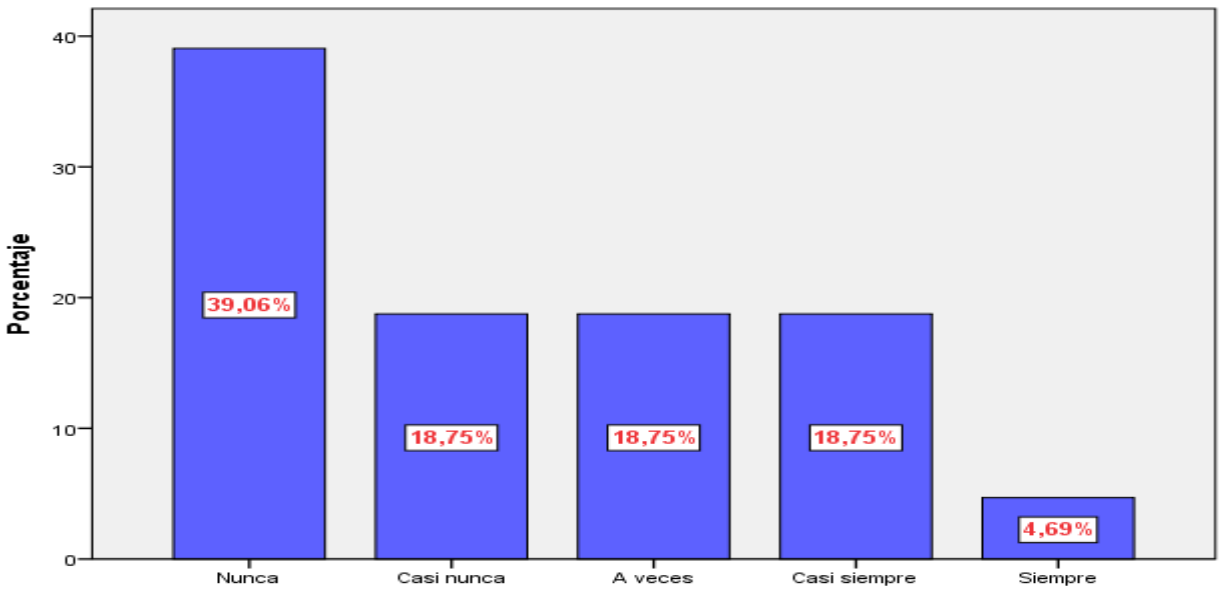
11. ¿Consideras que la información que guardas en tu ordenador está segura?

**Tabla 1111: Pregunta 11: ¿Consideras que la información que guardas en tu ordenador está segura?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 25 | 39,1 | 39,1 | 39,1 |
| | Casi nunca | 12 | 18,8 | 18,8 | 57,8 |
| | A veces | 12 | 18,8 | 18,8 | 76,6 |
| | Casi siempre | 12 | 18,8 | 18,8 | 95,3 |
| | Siempre | 3 | 4,7 | 4,7 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si consideras que la información que guardas en tu ordenador está segura, el 4.7% de los encuestados manifestaron que Siempre; el 18.8% dijeron que Casi siempre, A veces, Nunca y un 39.1% indicaron que Nunca.



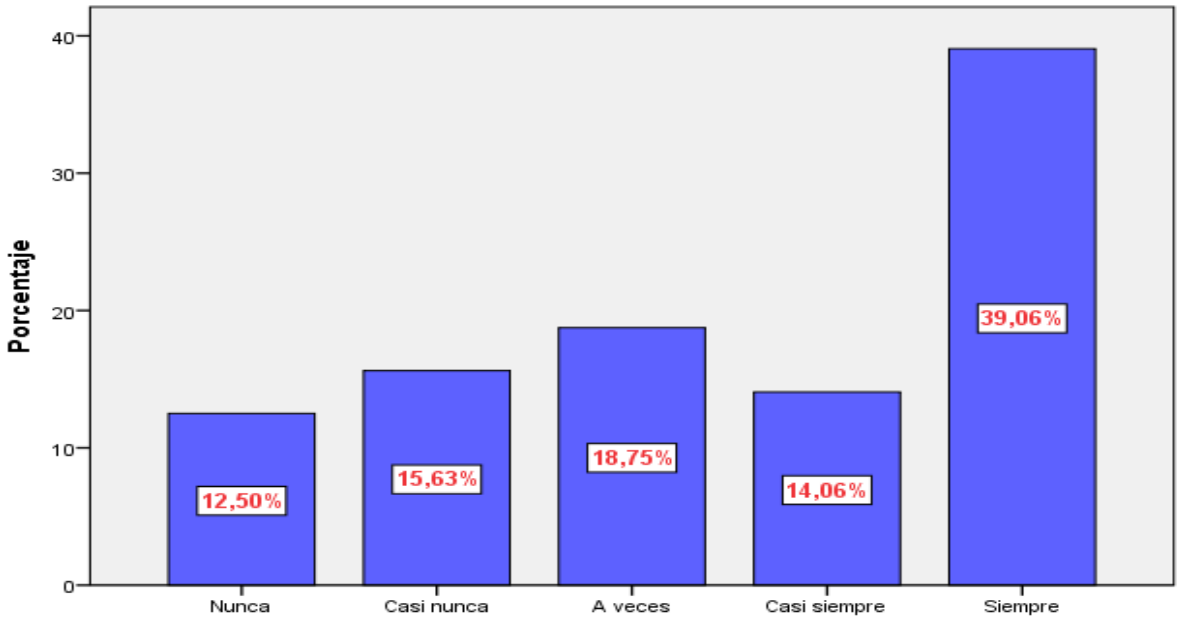
12. ¿Considera usted que un Estándar de Ciberseguridad ayudará a tener objetividad para identificar los riesgos en los Sistemas Informáticos?

**Tabla 1212: Pregunta 12: ¿Considera usted que un Estándar de Ciberseguridad ayudará a tener objetividad para identificar los riesgos en los Sistemas Informáticos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 8 | 12,5 | 12,5 | 12,5 |
| | Casi nunca | 10 | 15,6 | 15,6 | 28,1 |
| | A veces | 12 | 18,8 | 18,8 | 46,9 |
| | Casi siempre | 9 | 14,1 | 14,1 | 60,9 |
| | Siempre | 25 | 39,1 | 39,1 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si considera usted que un Estándar de Ciberseguridad ayudará a tener objetividad para identificar los riesgos en los Sistemas Informáticos, el 39.1% de los encuestados manifestaron que Siempre; el 14.1% dijeron que Casi siempre; el 12.5% dijeron que Nunca, otro 18.8% dijeron que A veces y el 15.6% de encuestados manifestaron que Casi nunca.



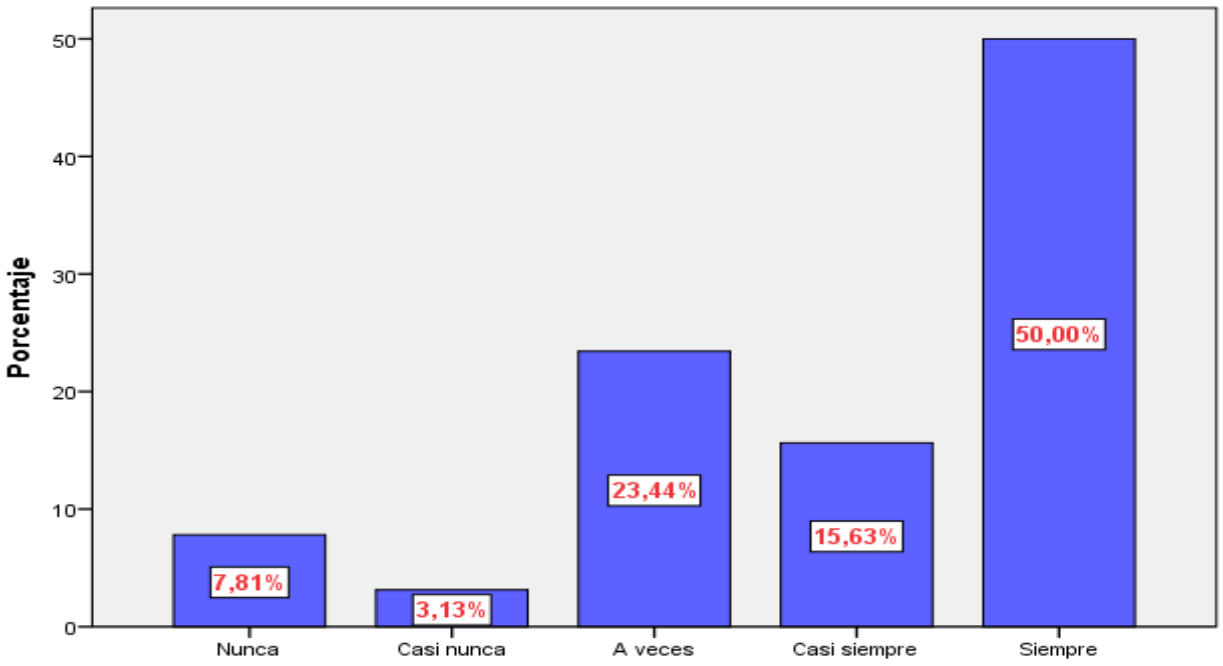
13. ¿Considera usted que las amenazas a la ciberseguridad son de riesgo para la EMCH “CFB”?

**Tabla 1313: Pregunta 13: ¿Considera usted que las amenazas a la ciberseguridad son de riesgo para la EMCH "CFB"**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 5 | 7,8 | 7,8 | 7,8 |
| | Casi nunca | 2 | 3,1 | 3,1 | 10,9 |
| | A veces | 15 | 23,4 | 23,4 | 34,4 |
| | Casi siempre | 10 | 15,6 | 15,6 | 50,0 |
| | Siempre | 32 | 50,0 | 50,0 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si considera usted que las amenazas a la ciberseguridad son de riesgo para la EMCH “CFB”, el 50% de los encuestados manifestaron que Siempre; el 15.6% dijeron que Casi siempre; el 7.8% dijeron que Nunca, otro 23.4% dijeron que A veces y el 3.1% de encuestados manifestaron que Casi nunca.



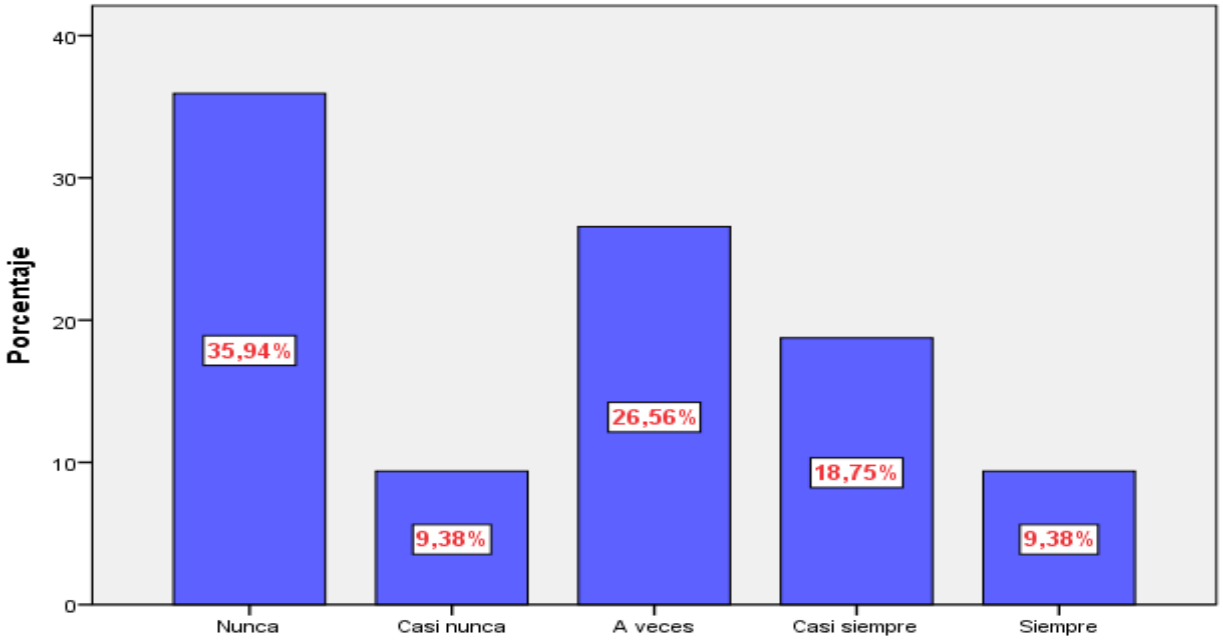
14. ¿Consideras que la EMCH “CFB” da importancia a la ciberseguridad en los Sistemas Informáticos?

**Tabla 1414: Pregunta 14: ¿Consideras que la EMCH "CFB" da importancia a la ciberseguridad en los Sistemas Informáticos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 23 | 35,9 | 35,9 | 35,9 |
| | Casi nunca | 6 | 9,4 | 9,4 | 45,3 |
| | A veces | 17 | 26,6 | 26,6 | 71,9 |
| | Casi siempre | 12 | 18,8 | 18,8 | 90,6 |
| | Siempre | 6 | 9,4 | 9,4 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si consideras que la EMCH “CFB” da importancia a la ciberseguridad en los Sistemas Informáticos, el 9.4% de los encuestados manifestaron que Siempre; el 18.8% dijeron que Casi siempre; el 35.9% dijeron que Nunca, otro 236.6% dijeron que A veces y el 9.4% de encuestados manifestaron que Casi nunca.



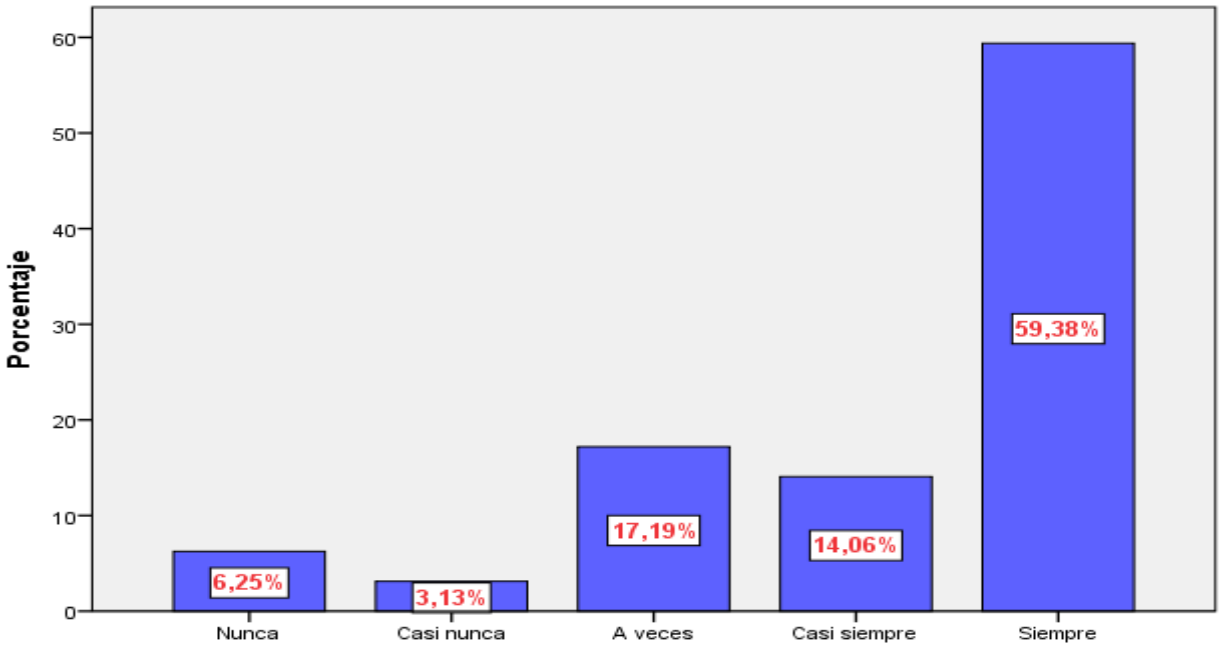
15. ¿Consideras adecuado que durante la formación de cadete se pueda aprender lo Básico-Intermedio acerca de la Ciberseguridad?

**Tabla 1515: Pregunta 15: ¿Consideras adecuado que durante la formación de cadete se pueda aprender lo Básico-Intermedio acerca de la Ciberseguridad?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 4 | 6,3 | 6,3 | 6,3 |
| | Casi nunca | 2 | 3,1 | 3,1 | 9,4 |
| | A veces | 11 | 17,2 | 17,2 | 26,6 |
| | Casi siempre | 9 | 14,1 | 14,1 | 40,6 |
| | Siempre | 38 | 59,4 | 59,4 | 100,0 |
| | Total | 64 | 100,0 | 100,0 | |

**Interpretación Análisis descriptivo**

En cuanto a la interrogante si consideras adecuado que durante la formación de cadete se pueda aprender lo Básico-Intermedio acerca de la Ciberseguridad, el 59.4% de los encuestados manifestaron que Siempre; el 14.1% dijeron que Casi siempre; el 6.3% dijeron que Nunca, otro




17.2% dijeron que A veces y el 3.1% de encuestados manifestaron que Casi nunca.

## 5.2 Análisis Inferencial

Durante las encuestas, el cual ha sido nuestro instrumento para poder comprobar nuestras hipótesis, por lo cual podemos decir que los integrantes de la Institución EMCH "CFB", los cadetes de comunicaciones, los cuales están al tanto de la situación de los problemas y bondades que pueda tener la Institución quisieran tener más protección en los Sistemas Informáticos, reducir las vulnerabilidades, riesgos que pueda tener dicha institución, el mismo usuario quisiera tener un mejor entendimiento del tema que abarca Ciberseguridad para asi poder mejorar la protección de los Sistemas Informáticos, lo cual si consideran que es de vasta importancia para la EMCH, ya que en el entorno se puede ver el descuido, la poca importancia que le dan al tema que abarca los Estándares de Ciberseguridad y entran en conciencia en que sí necesitan tener un conocimiento más amplio, para así ser más técnico, más capaz, al poder regular y minimizar riesgos.

**Tabla 1616:Resumen del procesamiento de los casos**

| | CASOS | | |
|---|---|---|---|
| | Válidos | | Total |
| | N | Porcentaje | 64 |
| VD | 64 | 100.0% | |
| VI | 64 | 100.0% | 64 |

Se procesaron 64 casos válidos, para todo el análisis inferencial de resultados.

Prueba de hipótesis de normalidad

H0: La muestra obtenida tiene una distribución normal (paramétrica)

H1: La muestra obtenida no tiene una distribución normal (no paramétrica)

Criterio de decisión:

$$\text{Si } p < 0.05, \text{ se rechaza la H0 y aceptamos Ha}$$

$$\text{Si } p >= 0.05, \text{ aceptamos la H0 y rechazamos la Ha}$$

En la siguiente tabla nos muestra los estadísticos de Kolmogorov Smirnov y de Shapiro Wilk, según las condiciones de los estadísticos nos mencionan que datos menores de 50 se

utiliza Shapiro Wilk y para datos mayores a 50 se utiliza Kolmogorov Smirnov. En nuestra investigación tenemos datos de 84 individuos estos son mayor a 50 por lo tanto tomaremos el criterio de Kolmogorov Smirnov.

**Tabla 17: Prueba de normalidad**

| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| VD | .359 | 64 | .000 | .794 | 64 | .000 |
| VI | .310 | 64 | .000 | .848 | 64 | .000 |

Para evaluar la hipótesis planteada se considerar el criterio de decisión, según el estadístico de Kolmogorov Smirnov se tiene 0 grados de libertad siendo menor a 0.05 por esta condición, rechazamos la hipótesis nula (H0) y aceptamos la hipótesis alterna (Ha); la hipótesis alterna nos dice que la muestra obtenida no tiene una distribución normal o es de tipo no paramétrica. Con este criterio asumiremos pruebas de correlación no paramétricas, para determinar el grado de relación entre la variable X e Y, para lo cual usaremos la Rho de Spearman.

Prueba de hipótesis de correlación

H0: No existe relación significativa entre la variable (X) y la variable (Y)

H1: Existe relación significativa entre la variable (X) y la variable (Y)

Criterio de decisión:

$$\text{Si } p < 0.05, \text{ se rechaza la H0 y aceptamos Ha}$$

$$\text{Si } p >= 0.05, \text{ aceptamos la H0 y rechazamos la Ha}$$

**Tabla 18: Correlación de Rho de Spearman**

| | | | VI | VD |
|---|---|---|---|---|
| Rho de Spearman | VI | Coeficiente de correlación | 1.000 | 0.771** |
| | | Sig. (bilateral) | . | 0.000 |
| | | N | 64 | 64 |
| | VD | Coeficiente de correlación | 0.771** | 1.000 |

| | | | |
|---|---|---|---|
| | Sig. (bilateral) | 0.000 | . |
| | N | 64 | 64 |

**. La correlación es significativa al nivel 0,01 (bilateral).

### 5.2.1 Prueba de Hipótesis General

Los Estándares de Ciberseguridad de los Sistemas Informáticos en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2021 es importante porque mejora significativamente la seguridad y confianza a cada usuario que forma parte de la Institución al tener un grado superior de protección en su Ciberseguridad, en la encuesta que hemos hecho se puede ver en la pregunta ¿Considera usted que un Estándar de Ciberseguridad ayudará a tener objetividad para identificar los riesgos en los Sistemas Informáticos?, el 39.1% dijeron siempre, lo cual nos indica que también los usuarios lo consideran de mucha importancia, le traerá más seguridad y confianza a cada uno que conforme la Institución y se puede reafirmar con la pregunta 15. ¿Consideras adecuado que durante la formación de cadete se pueda aprender lo Básico-Intermedio acerca de la Ciberseguridad?, el 59.4% consideraron que siempre, y es asi como se sabe que puede tener un grado superior de protección en su Ciberseguridad.

### 5.2.2 Prueba de Hipótesis específica 1

Los Estándares de Ciberseguridad ayuda al usuario a comprender las diferentes amenazas que existe en la red de los Sistemas Informáticos en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2021, en la encuesta que se ha dado a los cadetes de comunicaciones de la EMCH “CFB”, la pregunta 3, 4, 5, la cual pregunta acerca si es importante la seguridad de las redes, información e internet de la EMCH “CFB”, los encuestados afirmaron que siempre el 67.2%, 68.8%, 64.1%, sucesivamente, es por eso se dice que si debemos darle importancia a los Estándares de Ciberseguridad ya que esto abarca la seguridad en todos los Sistemas Informáticos de la EMCH “CFB”.

### 5.2.3 Prueba de hipótesis específica 2

Los Estándares de Ciberseguridad al formar parte de la Institución favorece la determinación de fallos técnicos que existe en las aplicaciones de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021, tomando como referencia la encuesta que se realizó a los cadetes de comunicaciones de la EMCH "CFB", en la pregunta 9, 10 y 11 se hace referencia sobre qué tan seguros se encuentran los Sistemas Informáticos, red informática y ordenador del mismo usuario, y estos afirmaron que nunca en 32.8%, 40.6% y 39.1% sucesivamente, es por eso que basándonos en las bases teóricas se puede decir que tenemos que tener un Estándar de Ciberseguridad para así poder tener mayor objetividad en los fallos técnicos que pueda haber en los Sistemas Informáticos.

### 5.2.4 Prueba de hipótesis específica 3

Los Estándares de Ciberseguridad mejora la exclusividad que pueda tener la información de los Sistemas Informáticos en la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2021, basándonos en la encuesta que ha hecho a todos los cadetes de comunicaciones de la EMCH "CFB", nos acercamos a dar respuestas acerca de nuestra hipótesis, en la pregunta 13. ¿Considera usted que las amenazas a la ciberseguridad son de riesgo para la EMCH "CFB"? afirmaron que siempre un 50% de la población, y en la pregunta 14. ¿Consideras que la EMCH "CFB" da importancia a la ciberseguridad en los Sistemas Informáticos?, afirmaron que nunca un 35.9%, por la razón que se puede decir que hay demasiados riesgos, los cuales somos vulnerables a nivel Institución, y esta misma no le da importancia es por eso que sí se debe establecer un Estándar de Ciberseguridad para así mejorar la gran exclusividad que se tiene a los documentos confidenciales, los cuales hoy en día se maneja en el ciberespacio.

## 5.3 Discusión de Resultados

Una vez contrastado el resultado de la Hipótesis General y las Hipótesis Específicas el cual nos dicta la gran mejora que se puede dar hacia la Institución, la importancia que se le tiene que dar hacia la Ciberseguridad y los Sistemas Informáticos los cuales tienen vulnerabilidades, fallos

técnicos, y estos deberían tener exclusividad por la abundancia e importante información que almacena vía virtual, los mismos usuarios no están conforme con su capacidad intelectual que tienen acerca sobre este tema, el cual es muy amplio, si quieren y necesitan aprender sobre Ciberseguridad, ya que son conscientes de sus grandes descuidos que tienen, y su poca preparación ante algún ataque o dificultad, esto lo plasmamos con la realidad y vemos que en muchos países, han sido duramente atacados, empresas, instituciones muchos caídos, destruidos, es por eso que verdaderamente tomamos en consideración los Estándares de Ciberseguridad el cual ayuda a tener un mejor funcionamiento de la institución, dentro de las medidas y el Checklist que abarca esta, muy aparte del reconocimiento que pueda llegar a tener la Institución, la concientización estará en cada usuario de la EMCH "CFB".

## CONCLUSIONES

1. De acuerdo a la Hipótesis General que a la letra dice que, Estándares de Ciberseguridad y los Sistemas Informáticos en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, comparando con los resultados del instrumento que hemos usado el cual ha sido la Encuesta, se ha podido concluir lo cuan factible puede ser tener un Estándar de Ciberseguridad y la poca importancia que le dan hoy en día en alguna organización, y más aún deberemos darle importancia al ser una Institución castrense, con prestigio y muy querida por la población, es por eso que se concluye que la hipótesis es válida, ya que en la actualidad se ha visto lo significativo que puede ser que tengan conocimientos los usuarios sobre ciberseguridad y según lo investigado se ha visto los múltiples errores, caídas de empresas, instituciones por no tener un nivel de usuario y a nivel Organización, por otro lado se necesita ya que los Sistemas Informáticos de la EMCH son vulnerables y es por eso que ese cuidado debe aumentar a gran escala, y se puede concluir que si se necesita un Estándar de Ciberseguridad para tener un mejor grado intelectual sobre este tema y asi permita neutralizar cualquier incidente que puede ocurrir hacia los Sistemas Informáticos.

2. En un segundo plano se puede ver la gran importancia que tiene los Sistemas informáticos, a lo largo de los años se ha podido ver el sinfín de numerosos ataques informáticos los cuales siempre habrá ya que con el tiempo que pasa a paso agigantados en la tecnología asi como se descubre bondades para prevenir, los ciberdelincuentes provocan y ocasionan que se halle muchas más maldades para arrebatar, infiltrarse en la información asi como destruir la vida de una persona o institución en tan solo unos segundos, es por eso que se ve por conveniente y se asegura que es de vital importancia que cada uno de nosotros en la vida conozca de tema, asi mismo también que se desarrolle y expanda la información en la Institución, asi como también debe ser propicio asegurar la seguridad de cada uno de nosotros.

3. Por último, dentro del mundo de la informática se puede decir que para ser desarrollados y estar en listos y preparados para cualquier guerra por asi decirlo es adecuado y propicio tener base y como base fundamental tenemos a los Estándares de ciberseguridad 27032 el

cual ofrece gran mejoría a toda una Institución como la puede ser la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, en el cual se concluye que debemos y tenemos la necesidad de acoplarlo hacia nuestros medios para ser y estar más seguros de nosotros mismo para hacia otros medios u organizaciones.

## RECOMENDACIONES

1. Teniendo como objetivo los Estándares de Ciberseguridad y la mejora que pueda afectar a los Sistemas Informáticos, consideramos que la Ciberseguridad presenta objetivos, amenazas y tipos de ataques los cuales permiten analizar y estructurar los medios necesarios para prevenir y evitar los riesgos de hacking o diferentes vulnerabilidades que pueda tener los Sistemas Informáticos los cuales son de mucha importancia para la Institución, ya que es un ente militar y se tiene información confidencial la cual hoy en día se tiene y obtiene digitalmente, es recomendable que sí se tenga un Estándar de Ciberseguridad para tener un concepto más amplio, tener más conciencia y orientar al usuario para evitar cualquier amenaza, para así asegurar la neutralización y/o destrucción de todo lo que abarca nuestros Sistemas Informáticos de la EMCH "CFB".

2. Teniendo en consideración que los objetivos de la Ciberseguridad incluyen la infraestructura, el usuario y la información, los cuales permiten focalizar y orientar de una manera más directa el esfuerzo para prevenir y evitar los riesgos de ataques hacia los usuarios que conforma la Institución EMCH "CFB", es recomendable se establezca medidas de seguridad las cuales sean rigurosas para prevenir algún descuido que se pueda tener en la Ciberseguridad.

3. Tomando en consideración la Amenazas a la Ciberseguridad hacia la EMCH "CFB", incluyen el origen, el efecto y el medio utilizado por las mismas, los cuales se debe establecer en que forma específica debemos combatir y evitar nos tomen de sorpresa ya que es un factor decisivo, al tener un descuido y en el momento menos pensado, es ahí donde suelen atacar y los perjudicados será la misma Institución EMCH "CFB" y los usuarios que la conformen.

# Bibliografía

(s.f.).

Alcantára, F. J. (2015). *GUÍA DE IMPLEMENTACIÓN DE LA SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001, PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA COMISARIA DEL NORTE P.N.P EN LA CIUDAD DE CHICLAYO.* Chiclayo: UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO.

Alemán Carmona, A. M. (2020). La educación en línea y el coronavirus. La afectación de la salud mental de los estudiantes universitarios. En UNESCO, *Educación y panndemia. Una visión desde la universidad* (págs. 17-23).

Álvarez Álvarez, C. (2012). La relación teoría - práctica en los procesos de enseñanza - aprendizaje. *Educaatio Siglo XXI* , 383 - 402. Obtenido de file:///D:/Downloads/160871-Texto%20del%20art%C3%ADculo-593421-1-10-20121017.pdf

Álvarez, C. (2018). *LA GERENCIA Y EL PROBLEMA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES MODERNAS (CASO GANDALF COMUNICACIONES, C.A).* San Diego: Universidad Jose Antonio Paez.

América, e. E. (2 de 3 de 2021). *www.eleconomistaamerica.pe*. Obtenido de https://www.eleconomistaamerica.pe/empresas-eAm-peru/noticias/11081267/03/21/Mas-de-26-billones-de-intentos-de-ciberataques-afectaron-a-Peru-en-2020.html

B., A. N. (s.f.).

Bruderer, Vega, R. S. (2019). *DISEÑO DE UN MODELO DE CIBERSEGURIDAD PARA DISPOSITIVOS MÓVILES EN EL SECTOR EMPRESARIAL.* Lima: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.

CEPAL - UNESCO. (agosto de 2020). *La educación en tiempos de la pandemia de COVID 19*. Obtenido de https://www.cepal.org/sites/default/files/publication/files/45904/S2000510_es.pdf

Colén Riau, M., & Castro Gonzáles , L. (2017). El desarrollo de la relación teoría y práctica en el grado de maestro en educación primaria. . *Profesorado. Revista de Currículum y formación de profesorado*, 59 - 79.

CUBA, A. C. (2019). *INFLUENCIA DE UNA PMO PARA LA GESTIÓN DEPROYECTOS DE SISTEMAS DE INFORMACIÓN EN UNA EMPRESA DE TELECOMUNICACIONES EN EL PERÚ.* Lima: UNFV.

Ejército del Perú. (2015). *Preparación de Inteligencia del Campo de Batalla.* Lima: ME 1 - 132.

*GrupoACMSConsultores*. (s.f.). Obtenido de GrupoACMSConsultores: https://www.grupoacms.com/norma-iso-27032

Hermida, Alonso, J. Á., & Panizo, Alonso, L. (2018). *CIBERSEGURIDAD APLICADA A LA E-DEMOCRACIA: ANÁLISIS CRIPTOGRÁFICO Y DESARROLLO DE UNA METODOLOGÍA PRACTICA DE EVALUACIÓN PARA SISTEMAS DE VOTO ELECTRÓNICO REMOTO Y SU APLICACIÓN A LAS SOLUCIONES MÁS RELEVANTES - UNIVERSIDAD DE LEÓN- ESPAÑA 2018.* España: Universidad de León.

Huaura, M. M. (2019). *GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESAS DEL SECTOR TELECOMUNICACIONES.* Lima: UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS.

Iberico Collazos, J. (2019). *Influencia del agregado grueso según su formación geológica en.* lima: UNIVERSIDAD PERUANA UNIÓN.

Inoguchi, R. A., & Macha, M. E. (2016). *GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ, 2016,.* Lima: Universidad San Ignacio de Loyola.

Instituto de Democracia y Derechos Humanos . (02 de febrero de 2021). *Educación en tiempos de pandemia* . Obtenido de https://idehpucp.pucp.edu.pe/notas-informativas/educacion-en-tiempos-de-pandemia/

Iván , H., & Toro , J. (2005). *PARADIGMAS Y METODOS DE INVESTIGACION*. Carabobo: EPISTEME CONSULTORES ASOCIADOS C. A. .

*kaspersky*. (s.f.). Obtenido de kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Mansilla, P. D. (2020). *IMPLEMENTACIÓN DE PROGRAMAS DE CUMPLIMIENTO EN CIBERSEGURIDAD COMO UNA PRÁCTICA DE BUEN GOBIERNO CORPORATIVO EN LAS ENTIDADES QUE FORMAN PARTE DEL SISTEMA FINANCIERO PERUANO.* Lima: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.

Noguera, A. (2019). *IMPLEMENTACION DE UN SISTEMA DE DETECCIÓN DE INTRUSOS PARA VENEZOLANA DEL VIDRIO C.A.* Caracas: Universidad Central de Venezuela.

Nolasco, v. j. (2021). *Covid.* Lima: Univesidad Esan.

Palella, S. S. (2012). *Metodologia de la Investigacion Cuantitativa.* Caracas: Fedupel.

*Postgrado Universidad Catolica San Pablo*. (s.f.). Obtenido de Postgrado Universidad Catolica San Pablo: https://postgrado.ucsp.edu.pe/articulos/que-es-seguridad-redes/

Programa de las Naciones Unidades para el Desarrollo . (2012). *Conceptos generales sobre gestión del riesgo de desastre y contexto del país. Experiencias y herramientas de aplicación a nivel regional y local.* Obtenido de https://www.preventionweb.net/files/38050_38050conceptosbsicos.pdf

Programa de las Naciones Unidas para el Desarrollo . (2018). *Reducción del riesgo de desastres*. Obtenido de https://www.undp.org/content/undp/es/home/climate-and-disaster-resilience/disaster-risk-reduction.html

Roig Ferriol y Oltra Badenes, R. (1 de 6 de 2015). *Propuesta de modelo de evaluación de herramientas para la gestión del proceso de gestión de problemas de ITIL*. Obtenido de https://riunet.upv.es/handle/10251/94984

Romero, M. H. (2018). *CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL" INSTITUTO NACIONAL DE CIBERSEGURIDAD.* España: Instituto Nacional de Ciberseguridad.

Tibaquira, C. Y. (2015). *METODOLOGÍA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA.* Bogota: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.

Villafuerte, P. (19 de marzo de 2020). *Educación en tiempos de pandemia: COVID 19 y equidad en el aprendizaje*. Obtenido de https://observatorio.tec.mx/edu-news/educacion-en-tiempos-de-pandemia-covid19