ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

La gestión de seguridad informática y el nivel de conocimiento de los trabajadores del simulador de vuelo en la aviación del ejército del Perú, 2022

Trabajo de Investigación

para optar el Grado a Nombre de la Nación de:

Maestro en

Gestión de Tecnologías de la Información

Autor:

Bach. Vizarreta Balbuena, Jose Carlos

Docente Guía:

Mtro. Valderrama Herrera, Roberto Marcel

TACNA – PERÚ

2023

Índice

Índice de tablas

Índice de ilustraciones

Dedicatoria

Este trabajo de investigación es dedicado a ustedes, quienes me han apoyado incondicionalmente en todo momento y han creído en mí desde el principio. Gracias por su amor y dedicación en todas las etapas de mi vida y por ser mis pilares de fuerza en momentos difíciles. Sin su apoyo y orientación, este logro no habría sido posible.

Resumen

La gestión de seguridad informática y el nivel de conocimiento de los trabajadores son factores críticos para proteger los sistemas y datos sensibles en un entorno de simulación de vuelo. La gestión de seguridad informática involucra la implementación de medidas adecuadas para proteger los sistemas y datos, mientras que el nivel de conocimiento de los trabajadores se refiere a la capacidad de los individuos para comprender y aplicar prácticas de seguridad informática. Una gestión de seguridad informática efectiva y un alto nivel de conocimiento de los trabajadores pueden minimizar los riesgos asociados con la interrupción de las operaciones y proteger adecuadamente los sistemas y datos sensibles.

Durante la descripción, identificación y evaluación final de la investigación se pudo concluir que el nivel de conocimiento de los trabajadores sobre seguridad informática en el simulador de vuelo de la aviación del ejército del Perú es insuficiente y necesita ser mejorado. Es esencial tomar medidas para mejorar la gestión de seguridad informática y proteger la información confidencial, así como asegurarse de que los trabajadores tengan los conocimientos y habilidades necesarios para desempeñar sus tareas de manera segura y efectiva.

Palabras claves: gestión, seguridad, informática, simulador.

Abstract

Information security management and the level of knowledge of workers are critical factors in protecting sensitive systems and data in a flight simulation environment. Information security management involves the implementation of adequate measures to protect systems and data, while the level of knowledge of workers refers to the ability of individuals to understand and apply information security practices. Effective IT security management and a high level of worker awareness can minimize the risks associated with business interruption and adequately protect sensitive systems and data.

During the description, identification and final evaluation of the investigation, it was possible to conclude that the level of knowledge of the workers about computer security in the Peruvian army aviation flight simulator is insufficient and needs to be improved. It is essential to take steps to improve IT security management and protect confidential information, as well as to ensure that workers have the necessary knowledge and skills to perform their tasks safely and effectively.

Keywords: management, security, computing, simulator

INTRODUCCIÓN

La gestión de seguridad informática y el nivel de conocimiento de los trabajadores son dos aspectos críticos en la protección de los sistemas y datos sensibles en un entorno como el simulador de vuelo en la aviación. La gestión de seguridad informática involucra la implementación de medidas de seguridad adecuadas para proteger los sistemas y datos, mientras que el nivel de conocimiento de los trabajadores se refiere a la capacidad de los individuos para comprender y aplicar prácticas de seguridad informática. Es esencial garantizar que ambos aspectos sean considerados y abordados de manera efectiva para asegurar la protección adecuada de los sistemas y datos sensibles en un entorno de simulación de vuelo.

Además, la gestión de seguridad informática y el nivel de conocimiento de los trabajadores también pueden afectar la eficiencia y la continuidad de las operaciones en un simulador de vuelo. Una gestión de seguridad informática efectiva puede minimizar los riesgos de interrupción del sistema y los costos asociados con la recuperación de datos perdidos. Por otro lado, un nivel alto de conocimiento de los trabajadores sobre prácticas de seguridad informática puede ayudar a garantizar que se cumplan las políticas de seguridad y se eviten errores humanos que puedan poner en peligro la seguridad de los sistemas y datos.

Por lo tanto, la gestión de seguridad informática y el nivel de conocimiento de los trabajadores son dos factores cruciales en la protección de los sistemas y datos sensibles en un entorno de simulación de vuelo. Que por su importancia han sido abordados de manera efectiva para garantizar una protección adecuada y minimizar los riesgos asociados con la interrupción de las operaciones.

CAPITULO I: ANTECEDENTES DE ESTUDIO

1.1. Título del Tema

¨La gestión de seguridad informática y el nivel de conocimiento de los trabajadores del simulador de vuelo en la aviación del ejército del Perú, 2022¨

1.2. Planteamiento del Problema

Con la modernización de las tecnologías emergentes, cada vez más las compañías privadas y públicas crean, procesan, transmiten y almacenan su información utilizando las ventajas de las Tecnologías de Información y Comunicaciones (TIC). Sumado a esto y al gran número de crecientes amenazas informáticas es de vital importancia mantener y asegurar la disponibilidad, confidencialidad e integridad de los datos e información de las empresas e instituciones del estado, convirtiéndose esta, en un aspecto más importante en el cual centrar e invertir para minimizar la pérdida, alteración o destrucción de los activos informáticos.

¨La seguridad informática busca proteger los sistemas informáticos y garantizar la integridad y confidencialidad de la información que contienen. Esto significa tomar medidas técnicas para mantener la infraestructura y las comunicaciones que respaldan las operaciones de su empresa, el hardware y el software que utiliza su empresa¨ (ISOTools Excellence, 2017).

Los simuladores de vuelo, o dispositivos de entrenamiento de vuelo, se utilizan para entrenar a los pilotos y desarrollar sus habilidades para navegar, pilotear y mantener los sistemas de aeronaves. Utilizado tanto por militares como por civiles en todo el mundo, desarrollando nueva tecnología y nuevo software.

El simulador de vuelo para los helicópteros de transporte y combate Mi-171Sh-P y el aula computarizada de entrenamiento de la Aviación del Ejército del Perú fue

entregado, por Rosoboronexport, en el marco del convenio de Offset Nº 6 ¨Suministro de un Simulador Integral de Vuelo en Helicópteros sin movilidad para las Tripulaciones de Helicópteros de la aviación del ejército, por un valor en 22,9 millones de dólares, de conformidad con lo aprobado el 23 de diciembre del 2015 por el Ministerio de Defensa (MINDEF). Este sistema de simulación de vuelo y el Aula de Entrenamiento, desembarcaron del Buque Carguero Kapitan Mironov en el Puerto del Callao el 31 de agosto del 2019 y se ubica actualmente en el destacamento de la Aviación del Ejército en Chorrillos, colindante con la Base Aérea Las Palmas.

Motivo por el cual la aviación del ejército del Perú creo para la administración y control de este bien, al departamento de simulador de vuelo (DESIV), adscrita a la jefatura de estado mayor operativo desde el año 2019, donde se ha venido capacitando al personal de pilotos, copilotos e ingenieros de vuelo de las tripulaciones de helicópteros de MI 171 ShP en las técnicas tácticas y procedimientos de vuelo, aterrizaje, despegue, maniobras y operación de vuelo, vuelo por instrumentos y navegación, empleo simulado de armamento, y procedimientos anormales y emergencias de vuelo.

Al ser un activo critico de vital importancia para la capacitación y entrenamiento de las tripulaciones de vuelo es necesario conocer el nivel de conocimiento en la seguridad informática que posee el personal de trabajadores de este departamento a fin de tomar las medidas preventivas, predictivas y proactivas ante la pérdida del funcionamiento del simulador de vuelo frente a una mala gestión en la seguridad informática.

El departamento del simulador de vuelo pertenece a la aviación del ejército del Perú, y depende jerárquicamente del jefe del estado mayor operativo, por lo cual cuenta

para su administración y operatividad con 03 oficiales y 07 técnicos aeronáuticos, especialista en mantenimiento y operación de simulador de vuelo de MI 171 ShP, certificados por la empresa DINAMIKA desde el año 2019.

1.3. Objetivos de la Investigación

1.3.1. Objetivo General

Establecer lineamientos para mejorar la gestión de seguridad informática y el nivel de conocimiento de los trabajadores del simulador de vuelo en la aviación del ejército del Perú.

1.3.2. Objetivos Específicos

Objetivo específico 1

Describir el nivel de conocimiento de los trabajadores del simulador de vuelo en la aviación del ejército del Perú sobre seguridad informática.

Objetivo específico 2

Identificar las prácticas actuales de gestión de seguridad informática en el simulador de vuelo de la aviación del ejército del Perú

Objetivo específico 3

Evaluar la efectividad de las prácticas actuales de gestión de seguridad informática en el simulador de vuelo de la aviación del ejército del Perú.

1.4. Metodología

El siguiente trabajo de investigación es de enfoque cuantitativo ya que utilizaremos la medición de las variables en el análisis y tratamiento estadístico, para evaluar de forma medible el conocimiento sobre la gestión de seguridad informática que poseen los trabajadores del simulador de vuelo.

La investigación es de tipo aplicada y de nivel descriptivo debido a que en un primer momento se identificara la teoría científica de las variables para comprender una situación, así como para formular una manera de solucionarlo. Seguidamente se recopilará la información sobre las características de la población o el fenómeno y luego presentar los datos de manera clara y concisa sobre la gestión de seguridad informática y el nivel de conocimiento.

¨La investigación aplicada es aquella que tiene como objetivo resolver problemas concretos y prácticos de la sociedad o las empresas¨ (Arias E. R., 2020).

"La investigación descriptiva busca describir los aspectos relevantes de un fenómeno, situación o problema sin intentar explicar o predecir su comportamiento. Su objetivo principal es comprender y documentar la naturaleza de una población o fenómeno específico" (Robson, 2011).

De diseño no experimental ya que se hará sin la manipulación de las variables, solo observando y midiendo los fenómenos que se aprecien en el departamento de simulador de vuelo a fin de analizarlos.

Método de análisis de datos será por recolección de datos proporcionados por los instrumentos, para proceder con la comparación y validación de las herramientas de encuesta y guía de observación.

La técnica de investigación utilizada será la encuesta a fin de obtener la información de la población en estudio mediante un cuestionario de 8 preguntas validadas para medir relación entre la gestión de seguridad informática y su nivel de conocimiento. Y la guía de observación de 5 pasos para asegurar de que la información

sea clara y objetiva, y ya que el observador en un ente imparcial que garantiza la validez de las observaciones.

Las encuestas son una herramienta que sirve para conocer las características específicas de un grupo de personas de una población. Para tratar y evaluar las variables tanto de una investigación cuantitativa como cualitativa (Bernal torres, 2010).

"La guía de observación es un instrumento valioso para la recolección de datos en investigaciones descriptivas y explicativas, especialmente en el contexto de estudios de campo y en el análisis de comportamientos y acciones concretas" (López, 2017).

1.5. Justificación

En lo teórico, la investigación servirá como aporte de vital importancia en el sustento de la estructura de la gestión de la seguridad informática, que afecta en el nivel de conocimiento del personal de trabajadores del departamento de simulador de vuelo para ser integrado en la corriente de doctrina del simulador de vuelo.

Metodológicamente la investigación es adecuada debido a que se utilizarán los instrumentos y métodos científicos en la recolección de los datos de las variables de gestión de seguridad informática y el nivel de conocimiento, que serán de importante valor y ayuda, para demostrar la confiabilidad y validez de los datos que servirán en la mejora de la gestión del simulador de vuelo de helicópteros.

Práctico, la investigación se realiza porque se ha apreciado la necesidad de evaluar los datos obtenidos en la investigación para poder mejorar las técnicas y tácticas y procedimientos vigentes en el departamento de simulador de vuelo a fin de mantener operativo el activo crítico del simulador de vuelo.

1.6. Principales definiciones

Incidente de seguridad

¨Se refiere a cualquier suceso relacionado con la seguridad desfavorable, como ataques de denegación de servicio (DoS), robo de información, espionaje y obtención de acceso a la información sin autorización. ¨ (Silva Coelho y otros, 2018).

Activo

¨Todo componente que tiene valor para la organización y su negocio. Algunos ejemplos incluyen bases de datos, software, hardware (como computadoras y portátiles), servidores, dispositivos de red (como enrutadores y conmutadores), personas, procesos y servicios. ¨ (Silva Coelho y otros, 2018).

Amenaza

¨ cualquier cosa que explote vulnerabilidades. Posible causa de un incidente no intencionado que podría dañar un sistema u organización ¨ (Silva Coelho y otros, 2018).

Simuladores de vuelo completo (FFS)

¨Estos simuladores de vuelo entran en la categoría de los mejores por su locomoción y características visuales. Sin el sistema de vuelo real, es el más exigente. El nivel de validación del simulador FFS garantiza la aerodinámica, las características de vuelo y los controles para marcas de aeronaves específicas¨ (Bernard, 2012).

Dispositivos de entrenamiento de vuelo (FTD)

¨Son dispositivos destinados a representar una configuración de aeronave particular y pueden rodear la cabina y las pantallas. Estos sistemas no siempre están en funcionamiento, pero son lo suficientemente maduros para ser capacitados y certificados. Estos dispositivos se pueden observar en centros educativos y universidades y son muy

utilizados para la enseñanza y el conocimiento de las nuevas tecnologías. ¨ (Bernard, 2012).

Vulnerabilidad

¨Vulnerabilidades que pueden explotarse para comprometer la seguridad del sistema y de los datos. Una vulnerabilidad en un activo o grupo de activos que puede ser explotada por una o más amenazas. Una vulnerabilidad es una falla que puede manifestarse como una falla en la seguridad general de una computadora o red. ¨ (Silva Coelho y otros, 2018).

Riesgo

¨Combinación de la probabilidad de que ocurra un evento y sus consecuencias para la organización. Algo que puede ocurrir y sus efectos sobre los objetivos de la organización¨ (Silva Coelho y otros, 2018).

Ataque

¨Cualquier acción que comprometa la seguridad de una organización¨ (Silva Coelho y otros, 2018).

Impacto

¨Resultado evaluado de un evento en particular¨ (Silva Coelho y otros, 2018).

Simulador de vuelo

¨Un dispositivo que reproduce el entorno de vuelo, ya sea en movimiento o no. Generalmente surgen de movimientos repetitivos de la aeronave tales como sonido, movimiento, control de vuelo y reacción a factores externos (turbulencias, viento, tormentas, nubes, etc.). Se utilizan para capacitación, diseño u otras aplicaciones. ¨ (Administration., 2014).

1.7. Alcances y limitaciones

Alcance

La presente investigación explorara los conocimientos que tienen los trabajadores del departamento de simulador de vuelo de helicóptero del ejército del Perú, en gestión de la seguridad informática, la cual se realizara en las instalaciones de la Aviación del Ejército del Perú – Chorrillos, colindante con el Comando de Educación y Doctrina del Ejército (COEDE), con la información y datos de las encuestas a los trabajadores del departamento de simulador de vuelo, de una población de 15 trabajadores entre oficiales, técnicos y suboficiales.

Limitaciones

Teóricas. La investigación probablemente no cuente con la suficiente información y apoyo de los encargados por ser información sensible y de carácter confidencial.

Gestión o de entorno. La investigación se enfocará únicamente en el departamento del simulador de vuelo, dejando de lado al personal de dicentes, que asisten al simulador a realizar su entrenamiento que también son vectores de ataques cibernéticos.

Metodológicos. La investigación será válida, en el periodo de tiempo en el que este se realice por lo que lo más importante en esta clase de metodología usada, motivo a que el muestreo o el uso del cuestionario generan errores y desviaciones.

CAPITULO II: MARCO TEÓRICO

2.1. Conceptualización de las variables y/o tópicos

La gestión de la seguridad informática

La seguridad informática se refiere al conjunto de actividades orientadas a proteger la información digital de una organización mediante el establecimiento de medidas de seguridad y la gestión de riesgos. El objetivo principal de la seguridad informática es proteger la confidencialidad, integridad y disponibilidad de la información almacenada en los sistemas informáticos de la organización (Whitman & Mattord, 2016).

Con esto se puede comprender que la implementación de controles definidos en la Seguridad de la Información sobre los componentes de las infraestructuras tecnológicas de las empresas y demás necesidades que permitan gestionar la operación normal y adecuada de los servicios informáticos empresariales y termina con el monitoreo, que permite establecer la adecuada y eficaz operación de los controles instalados.

Según (Romero Castro, Martha Irene; Figueroa Moràn, Grace Liliana ; Vera Navarrete, Denisse Soraya;, 2018) ¨La seguridad de la información se puede definir como la disciplina responsable de desarrollar estándares, procedimientos, métodos y técnicas para garantizar que un sistema de información sea confiable, seguro y, lo más importante, disponible.¨.

Es el objetivo principal de una buena gestión en la seguridad informática convertir a la organización en un ente seguro y libre de amenazas.

Gestión preventiva

¨Consiste en una serie de revisiones periódicas, algunos cambios o mejoras en varios aspectos que pueden involucrar hardware, software o cualquier otro componente involucrado en los sistemas y procesos. Como resultado, cada revisión depende de su propio conjunto de procesos comerciales¨ (Romero Castro, Martha Irene; Figueroa Moràn, Grace Liliana ; Vera Navarrete, Denisse Soraya;, 2018).

En gran porcentaje los ataques informáticos se pueden evitar o por lo menos mitigar el impacto, si se al menos se hubieran utilizado procedimientos o mecanismos preventivos, los errores y falla en los sistemas y demás problemas podrían localizarse, evitarse y resolver con ayuda de un buen trabajo en esta etapa.

Utilizar herramientas como respaldo de información, control de medios, comprensión de la información son de vital importancia para lograr una gestión preventiva de informática eficiente dentro de la institución.

Gestión correctiva

Según (Romero Castro, Martha Irene; Figueroa Moràn, Grace Liliana ; Vera Navarrete, Denisse Soraya;, 2018) Los mecanismos correctivos se diferencian significativamente de los mecanismos preventivos en que se aplican después de que ha ocurrido un evento y su objetivo principal es reparar las consecuencias. Y con tendencia a ser bastante caro económicamente.

El alto valor de estos mecanismos de la gestión correctiva es que normalmente se debe de contratar a empresas externas que solucionen el problema que uno tiene ya encima y que demorar más tiempo afectaría la productividad de la empresa.

Para una buena agestión correctiva es necesario ya tener una catalogación de la asignación de probables problemas que puedan dañar los activos críticos de la empresa, así como un análisis adecuado del problema a solucionar, con la documentación sustentatoria que de respaldo al proceso de la gestión correctiva de la seguridad informática.

Gestión proactiva

¨Son los más difíciles y necesitan el mayor nivel de conocimiento técnico dependiendo del tema que se trate. ¨ (Romero Castro, Martha Irene; Figueroa Moràn, Grace Liliana ; Vera Navarrete, Denisse Soraya;, 2018)**.**

La gestión proactiva de la seguridad informática utiliza los mecanismos de información que tiene la premisa de trabajar como si uno fuera el atacante y buscar la las vulnerabilidades de la empresa a fin de solucionarse en etapas de la gestión posteriores.

Teniendo siempre como objetivo detectar el vector de ataque por donde se realizará el ataque a la institución, para así, si es posible mitigar o limitar este posible ataque. Y detectar la actividad sospechosa, reconocerla para saber al menos que sucedió, a fin de tomar las medidas correctivas.

Seguridad física

Aunque la seguridad física tradicionalmente se ha centrado en proteger las instalaciones y bienes materiales de una organización, en la era digital, también se hace referencia a la seguridad física en el contexto de la seguridad informática. En este ámbito, la seguridad física se refiere a la protección física de los equipos y dispositivos de almacenamiento que contienen información sensible, así como a la protección de las

instalaciones que albergan los centros de datos y servidores. La seguridad física en el ámbito de la seguridad informática incluye medidas tales como la seguridad de la sala de servidores, el control de acceso a los equipos, la protección contra incendios y desastres naturales, y la vigilancia de los sistemas y equipos críticos.

Dentro de las amenazas contra la seguridad física se encuentran los desastres naturales (incendios, inundaciones, hundimientos, terremotos). Para lo cual tenemos que tener en cuenta a la hora de colocar el centro de proceso de datos (CPD), o donde ubicaremos los servidores de la empresa. Además de tener un sistema de extinción de fuego se debe de planear un segundo centro de proceso de datos lo que nos daría resiliencia ante cualquier catástrofe.

Medidas de seguridad sobre robos tanto de equipos como de la información que contienen, la cual es valiosa para la empresa e individuos de la organización. Un área con equipo informático siempre de ser protegida físicamente tanto como vigilantes, tarjetas de acceso, identificación mediante usuario y contraseña, etc.

Los equipos electrónicos funcionan con corriente eléctrica, y un fallo con el suministro de los mismos puede afectar con el funcionamiento de la empresa y su comunicación con los clientes, para lo cual se deben considerar baterías o un grupo electrógeno por si fallara la corriente, una conexión auxiliar a Internet como línea de backup o incluso podemos optar por una solución inalámbrica para estar protegidos ante un corte.

Seguridad lógica

La seguridad lógica se refiere a una serie de estrategias, prácticas y técnicas que se utilizan en el contexto de las tecnologías de la información y la comunicación para

salvaguardar la información y los sistemas que la procesan. Su objetivo es prevenir, detectar y responder a las posibles amenazas de seguridad que puedan afectar los sistemas informáticos y las redes de comunicaciones. La seguridad lógica se considera un aspecto crucial de la seguridad de la información (Sanz, 2021).

La seguridad lógica de una empresa suele ser atacada por virus, caballos de Troya y malware. Al igual que el spam y el malware, es un software innecesario el que debe eliminarse.

La pérdida de datos, generalmente causada por errores o una configuración incorrecta del código fuente del software, puede provocar cambios inexplicables o la pérdida de datos almacenados. Para mitigar este riesgo, las empresas utilizan las aplicaciones antes de decidir utilizarlas y realizan copias de seguridad utilizando varios puntos de procesamiento de información para evitar perder la información almacenada.

Los ataques a los servidores de aplicaciones se llevan a cabo cuando los piratas informáticos intentan ingresar al sistema y recuperar datos a través de vulnerabilidades en la aplicación o el sistema operativo.

Confidencialidad, disponibilidad, integridad y no repudio

La confidencialidad es garantizar que solo las personas o máquinas autorizadas puedan utilizar la información. Para garantizar la confidencialidad, necesitamos implementar tres mecanismos.

La verificación de que una máquina o persona es quien dice ser y que estamos hablando con otra entidad.

Una vez que nos hayamos autenticado, los usuarios de los datos tendrán diferentes privilegios sobre la Autorización. Básicamente, son solo lectura o lectura y escritura.

El objetivo principal de la integridad es que las informaciones queden almacenados y guardadas tal y como espera el usuario lo dejo en el momento de cárgalo es decir no sufra alteraciones sin su consentimiento.

La disponibilidad trata lograr que los usuarios logren acceder a sus servicios en el horario permitido. Para lo cual se trata en sobredimensionar los recursos informáticos de la empresa.

El no repudio es cuando, dos partes ante una relación, intentan evitar que cualquiera de ellas logre negar que participe en dicha relación.

Buenas prácticas de la seguridad informática

Es muy difícil la tarea de seguridad informática en una empresa grande tanto para el encargado como para los usuarios: hay muchos datos de información que hay que proteger y un sinfín de puertas por donde ser víctimas de intrusiones. Quien administra la seguridad de la informática de una empresa debe como funciones principales localizar los activos que hay que cuidar: aplicaciones, equipos, comunicaciones y datos.

Además de revisar la política de copias de seguridad: qué, cuándo y dónde lo copiamos, sin olvidar el dónde lo guardamos de forma muy segura las copias de los dispositivos, así como verificar que la copia se ha hecho de forma correcta. Redactar y revisar regularmente los planes de contingencia ante catástrofes es otra función a la cual se le debe dar una prioridad, analizando todas las posibilidades: ataque intencionado, arranque parcial de servicios, desastre natural. No instalar ningún software que no sea

estrictamente necesario, y revisar todas las configuraciones de las aplicaciones y sistemas y si estamos entregando más permisos de los necesarios.

Además, existen muchas otras actividades que se consideran mejores prácticas para ayudar a las empresas con la seguridad informática. B. Actualizar todos los informes de seguridad generados. Esto requiere suscribirse a la lista de correo de aprobación de seguridad y suscribirse al proveedor para recibir actualizaciones directamente.

Habilite el procedimiento de actualización automática para el sistema instalado. Los creadores de este software generalmente lanzan actualizaciones que no causan errores, excepto para sistemas sensibles. Anime a los usuarios a usar la seguridad y véala como una ayuda en lugar de un obstáculo. Al verificar constantemente los registros de su sistema, puede recopilar archivos de registro y aplicar rápidamente muchos patrones. Además, puede ser muy difícil detectar conceptos erróneos por su cuenta, ya que puede pagar una auditoría externa para verificar los conceptos erróneos.

Verifique la lista de computadoras conectadas y usuarios conectados que están en la red del empleado o corporativa, o verifique si los permisos han caducado o no coinciden con el perfil del usuario. Finalmente, la configuración de notificación por correo electrónico o SMS le alerta sobre cualquier problema. En caso de falla del sistema de batería o del proceso del servidor.

Gestión de Riesgos

Es el proceso iterativo e interactivo basado en evaluar, conocer y manejar los riesgos e impactos, a fin de mejorar la toma de decisiones dentro de la institución (Silva Coelho, Segadas de Araújo, & Kowask Bezerra, 2018).

La gestión de riesgos es aplicable en toda situación que sean oportunidades para la consideración de mejoras de la empresa dentro de la gestión de factores, seguridad, políticas implementadas y manuales de usuario para evitar daños a nivel de toda la empresa en relación a la planificación administrativa, comercial, financiera y de sistemas que exista.

El uso de los estándares ISO 27001 relacionados con la seguridad informática y la gestión de riesgos es una tarea importante para detallar proyectos e iniciativas importantes para mejorar la seguridad de la información en toda la organización. El objetivo final es exigir un análisis de riesgo para que la exposición de la empresa al riesgo pueda reducirse a un nivel óptimo para un análisis inicial de la situación.

Plan de Gestión de Seguridad Informática

Un Plan de Gestión de Seguridad Informática es un registro de las directrices y procedimientos para salvaguardar los sistemas informáticos y la información de una organización. Su finalidad es establecer medidas de control que aseguren la confidencialidad, integridad y disponibilidad de la información, gestionar los riesgos y proporcionar una estructura de referencia para la administración de la seguridad informática (ISO 27001,2020) .

En pocas palabras, un plan de gestión de seguridad de la información establece los principios organizacionales y funcionales de la empresa relacionados con la seguridad de la información, resume las políticas de seguridad y las responsabilidades de los miembros del proceso de información y proporciona una base para permitir la prevención y detección. documento. y reaccionar ante amenazas que perjudiquen a la empresa.

Sistemas de Gestión de la Seguridad de la Información (SGSI)

"Los Sistemas de Gestión de la Seguridad de la Información (SGSI) son un conjunto de políticas, procedimientos y controles que se implementan en una organización para proteger la confidencialidad, integridad y disponibilidad de la información, al tiempo que se gestionan los riesgos de seguridad informática. Los SGSI establecen un marco sistemático y estructurado para la gestión de la seguridad informática, y pueden ser certificados por terceros para demostrar el cumplimiento de estándares y normativas de seguridad" parafraseado.

El modelo de gestión de riesgos incluye a todos los empleados, procesos externos, procesos internos y sistemas controlados por el departamento de tecnologías de la información.

La implementación de un sistema de gestión de seguridad de la información siempre ayudará a todas las empresas a mantener seguros sus activos de información, lo que les permitirá ganar credibilidad frente a sus competidores.

Nivel de conocimiento

En la gestión del conocimiento hay dos procesos fundamentales, uno es la creación de conocimiento y el otro, la transmisión de conocimiento. La transmisión se da de muchas maneras y puntos de vista, incluido en el tiempo y espacio (Zambrano Burbano, 2018).

Cuando colocamos de forma explícita el conocimiento en una base de datos, en el fondo lo que hacemos, es ponerlo allí, para que más adelante alguien pueda recogerlo; en cierta medida mejorarlo, a fin de trascender el conocimiento en el tiempo. Y al utilizar las herramientas de comunicación lo que hacemos es tratar de transmitir el conocimiento.

¨Los primeros científicos valoraron la sistematización de tales manifestaciones experienciales trascendentales para la humanidad al tiempo que establecieron los fundamentos teóricos de la ciencia a través de una interacción dialógica entre el conocimiento sensorial y el lógico ¨ (Rojas, 2013).

Una de las habilidades humanas más cruciales es el conocimiento, ya que nos permite comprender la naturaleza de cómo funcionan las cosas que nos rodean y sus características y relaciones a través del razonamiento.

¨ Conocer las cosas es comprender sus propiedades y relaciones para reconocer lo que son y lo que no son ¨ (Díaz, 2003).

Nivel de conocimiento sensible o sensorial

El conocimiento sensible es aquel conocimiento que nos permite conocer y aprender un objeto mediante los sentidos, tales como son las imágenes percibidas por la vista.

¨ El conocimiento sensorial es el que resulta de la actividad de nuestros sentidos. Incluye sentimientos, percepciones y representaciones. ¨ (Bermúdez, 2013).

Con estos sentidos, en gran mayoría gracias al de la vista es posible acumular en la mente bastante información relacionada y entrelazada con dimensiones, imágenes, colores y estructuras, que forman nuestros recuerdos y experiencias de vida y aprendizaje, creando así a nuestra realidad privada, interna o personal. Gracias también a la audición podemos procesar y entender el habla, así como para transmitir los saberes. En conclusión, la vista y la audición son los sentidos más utilizados en el aprendizaje para el ser humano.

Nivel de conocimiento conceptual

El nivel de conocimiento conceptual se refiere al conocimiento teórico y abstracto que una persona tiene sobre un tema determinado. Se trata de la comprensión de los conceptos, principios y fundamentos teóricos que sustentan una disciplina o práctica, y que permiten a la persona aplicar ese conocimiento en situaciones concretas.

Este nivel de conocimiento se considera fundamental para el aprendizaje profundo y la resolución de problemas complejos en una determinada área del conocimiento

Es decir, con este tipo de conocimiento, cuando se reciben estímulos de los sentidos, los individuos los clasifican, etiquetan, clasifican, cuentan o interpretan con las mismas palabras o frases descriptivas que se relacionan con precisión con su realidad conocida.

Nivel de conocimiento holístico

el nivel de conocimiento holístico en la informática se refiere al conocimiento y comprensión completa de los sistemas, aplicaciones y tecnologías informáticas en su conjunto, en lugar de centrarse solo en aspectos específicos o fragmentados.

Así que, para lograr entender los hechos relacionada a una perspectiva de múltiples interacciones, que se caracteriza por ser un nivel de conocimiento con una actitud integradora y explicativa de la teoría, orientada a comprender el total de los de los sujetos, procesos, y objetos en cada uno de sus contextos. Haciendo referencia a la forma de interpretar, ver, entender a las cosas en su complejidad y totalidad, ya que de esta manera se pueden apreciar sus procesos, interacciones y características.

Conocimiento empírico-no científico

¨Es el conocimiento del tipo de conocimiento común, real y espontáneo, en el que se construye a partir de la vida cotidiana sin buscarlo, estudiándolo, aplicando métodos, sin pensar en ello¨ (Tamayo y Tamayo, 2012).

Es un lugar común, popular, empírico, vulgar o de sentido común. Esto se debe a que el conocimiento se deriva del sentido común de un individuo, es visto como impreciso y sus juicios no están debidamente justificados, es decir, el lenguaje se presenta como ambiguo y los métodos de adquisición del conocimiento se caracterizan principalmente por el hecho de que hay escasez de método para obtener el conocimiento.

Conocimiento científico

¨Más bien, consiste principalmente en entender la investigación como conocimiento práctico, y la docencia investigativa como transferencia de habilidades, más que en saber hacer¨ (Sánchez, 2014).

Este conocimiento tiene el propósito básico y primario de descubrir y comprender los procesos o leyes que regulan la naturaleza, y modificarlos y transformarlos en beneficio de la sociedad. En este nivel, el conocimiento se profundiza. Es comprender las causas o razones de los fenómenos o hechos mediante la verificación o demostración sistemática. El conocimiento científico siempre es reemplazado por el conocimiento empírico. Siempre generalice sobre los objetos y siempre busque formas de resolver problemas.

Conocimiento filosófico

¨Busca el porqué de los fenómenos y se basa fundamentalmente en la reflexión sistemática para descubrir y explicar¨ (Nieto, 2010).

El conocimiento filosófico es en sí un saber que se logra tras la recopilación de la información escrita, una vez es analizada y corroborada en la práctica del ser humano. Por tanto, este conocimiento se utiliza como medio para crear y ejercer conocimientos de herramientas como la crítica y el análisis.

2.2. Análisis comparativo de las bases teóricas

En la tabla 1 se realiza el análisis comparativo de las bases teóricas de seguridad informática, donde se evalúan sus similitudes y diferencias.

Tabla 1 Análisis comparativo de gestión de seguridad informática.

Autor	Definición	Comentario
(Aguilera, 2011)	¨La seguridad informática como la disciplina encargada de proponer y diseñar estándares, procedimientos, métodos y técnicas para garantizar que los sistemas de información sean seguros, confiables y sobre todo disponibles¨	Estas tres citas tienen en común que todas tratan sobre la seguridad informática y su objetivo principal: proteger la información y los sistemas de una organización. La primera cita destaca el diseño de estándares, procedimientos y técnicas para garantizar la seguridad de los sistemas de información, mientras que la segunda cita se enfoca en el uso de herramientas y métodos para proteger los activos críticos de una organización. La tercera cita hace hincapié en que la gestión de riesgos es fundamental en la seguridad informática, y que siempre es posible tomar medidas preventivas para evitar situaciones de riesgo. En resumen, todas las citas resaltan la importancia de
(Aguirre, 2014)	¨ La seguridad informática se puede definir como un conjunto de métodos y diversas herramientas para proteger las principales propiedades. de una organización, como la información y los sistemas, frente a amenazas potenciales¨	
(Romero Castro, Martha Irene; Figueroa Moràn, Grace Liliana ; Vera Navarrete, Denisse Soraya;, 2018)	¨La seguridad siempre exige una gestión de riesgos. En otras palabras, siempre hay una manera de evitar o prevenir los riesgos, y se pueden tomar ciertas acciones para evitar estas situaciones¨	

		la seguridad informática para proteger los sistemas y la información, aunque desde diferentes perspectivas.

Fuente propia

En la tabla 2 se realiza el análisis comparativo de las bases teóricas de nivel de conocimiento, donde se evalúan sus similitudes y diferencias.

Tabla 2 Análisis comparativo de niveles de conocimiento de los trabajadores.

Autor	Definición	Comentario
(Britto, 2013)	¨Son de carácter general o conceptual, aplicables a una gran serie de casos y fenómenos que comparten ciertos rasgos y características comunes, y no se refieren únicamente a hechos singulares o individuales. Este conocimiento debe ser obtenido o verificado usando métodos conocidos y aceptados en el campo, sujeto a repetición y verificación por otros investigadores¨	Estas citas abordan diferentes aspectos del conocimiento. La primera cita se refiere al conocimiento conceptual o general, que es aplicable a diferentes situaciones y debe ser obtenido y verificado a través de métodos conocidos y aceptados. La segunda cita se refiere al proceso cognitivo a través del cual se obtiene el conocimiento, transformando la realidad en conceptos y representaciones. La tercera cita se refiere a las características del conocimiento como racional, objetivo e inteligente, basado en la búsqueda de la verdad objetiva y representando fielmente la realidad. En resumen, estas citas abordan diferentes aspectos del
(Arias F. , 2012)	¨ Como el acto de cognición, el proceso que surge en la cognición de la realidad. transformados en conceptos, imágenes y representaciones de esa realidad como producto o resultado de ese proceso¨	
(Pérez, 2012)	¨Es racional porque el conocimiento proviene de las actividades superiores dadas solo a los humanos. Es objetivo porque su finalidad es la búsqueda de la verdad objetiva. Por lo tanto, el logro del conocimiento debe representar fielmente la realidad sin alterar o distorsionar el objeto de investigación. Es inteligente porque es un proceso lógico que se basa en la sensación, la percepción y la	

	representación para conceptualizar el conocimiento.¨.	conocimiento y su adquisición, procesamiento y uso en la comprensión de la realidad.

Fuente propia.

2.3. Análisis crítico de las bases teóricas.

Analizando la información presentada sobre la variable de gestión de seguridad informática se puede apreciar que los conceptos de las bases doctrinales se relacionan y expresan directamente un concepto en los siguientes puntos:

- La gestión de seguridad informática es un factor importante en el desarrollo y continuidad de cualquier empresa pública y privada.
- Para un eficaz desarrollo de la seguridad informática se debe de realizar actividades antes, durante y después de cada actividad de la empresa, lo que resultara en una mayor resiliencia y capacidad de enfrentar cualquier amenaza.
- Son necesarias para la seguridad informática la capacitación tanto del administrador de la seguridad informática como de los usuarios, ya que en el nivel informático cualquier individuo es un vector de ataque para dañar los activos críticos de la empresa.

En la variable de los niveles de conocimiento de los trabajadores, los autores expresan en su gran mayoría una sinergia sobre el conocimiento humano y como este se obtiene:

- El conocimiento humano es universal, tuene sus propias particularidades, pero tienen validez en todo lugar del mundo y para todo tipo de personas.

- El conocimiento es organizado y uniforme en el principio de sus concepciones que desarrolla el ser humano durante su aprendizaje.
- El conocimiento es un proceso lógico y abstracto que se fundamenta y se obtiene a través de la sensación, percepción y representación a fin de cimentar un conocimiento.

CAPITULO III: MARCO REFERENCIAL

3.1. Reseña histórica

El simulador de vuelo de helicópteros de transporte y combate Mi-171Sh-P y el aula computarizada de entrenamiento de la Aviación del Ejército del Perú entregado a la aviación del ejército por la federación Rusa en compensación por el convenio marco de Offset Nº 6 ¨Suministro de un Simulador Integral de Vuelo en Helicópteros sin movilidad para las Tripulaciones de Helicópteros Mi-171Sh-P y Aula de Estudios para Simulador¨ por motivo de la compra de 24 helicópteros de asalto de transportes realizada, por el estado peruano a fin mejorar la capacidad operativa del batallón de asalto y transporte Nº 811.

El sistema de simulación llego al Perú el 31 de agosto del 2019 y entregado a la aviación del ejercito el 24 de noviembre del mismo año, valorado por un monto de 22,9 millones de dólares y colocado en las nuevas instalaciones construidas en la base de la aviación de ejercito – Destacamento chorrillos.

Para lo cual la aviación del ejército del Perú creo para la administración y control de este bien, al departamento de simulador de vuelo (DESIV), adscrita a la jefatura de estado mayor operativo, donde se ha venido capacitando al personal de pilotos, copilotos e ingenieros de vuelo de las tripulaciones de helicópteros de MI 171 ShP en las técnicas tácticas y procedimientos de pre-vuelo, despegue, ascenso, maniobras y operación de vuelo, vuelo por instrumentos y navegación, empleo táctico de armamento, y procedimientos anormales y emergencias de vuelo.

Ilustración 1 Aula computarizada de entrenamiento

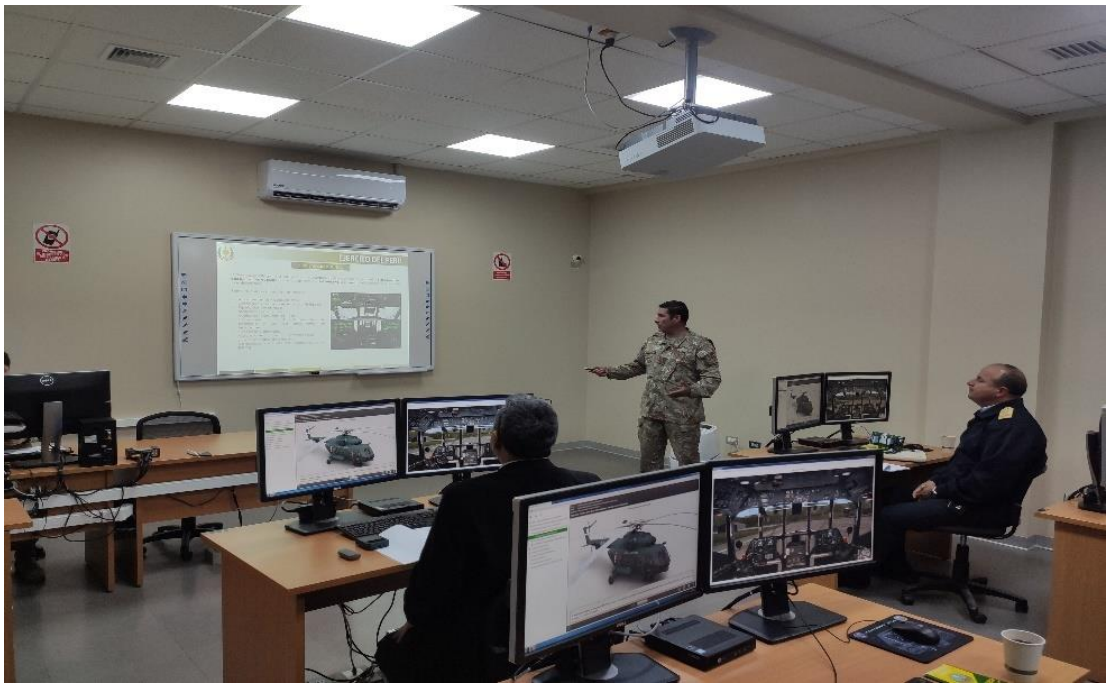


Ilustración 2 Entrenamiento en el simulador de vuelo

3.2. Filosofía organizacional

Misión

"El Simulador de Vuelo instruirá y entrenará al personal de pilotos, ingenieros de vuelo y especialistas aeronáuticos en los diferentes sistemas del helicóptero MI 171 SH y en situaciones de emergencia, haciendo énfasis en el profesionalismo para mantener la seguridad del vuelo en el ámbito operacional, tanto diurno como nocturno a través de la instrucción programada por el DIEDOC y DEPLANO" (Ejercito, 2022).

Visión

"Ser el Simulador de Vuelo de helicóptero para MI 171 Shp, líder en la región sudamericana con capacidades de entrenamiento para personal militar y civil avalado por la dirección general de aeronáutica civil. " (Ejercito, 2022).

Valores institucionales

- Disciplina.
- Vocación de servicio.
- Liderazgo.
- Identidad.
- Iniciativa.
- Superación

3.3. Diseño organizacional

Función General

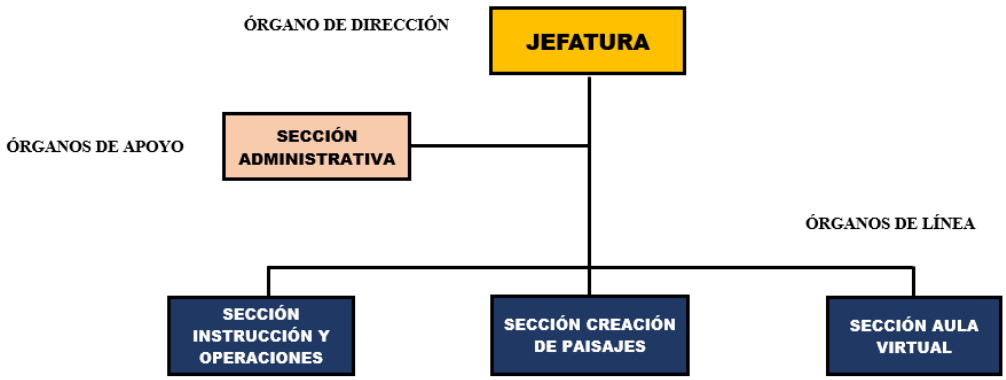
"El Simulador de vuelo capacitará, instruirá y entrenará al personal de pilotos, ingenieros de vuelo y especialistas aeronáuticos en los diferentes sistemas del helicóptero MI 171 SH y en situaciones de emergencia haciendo énfasis en el profesionalismo para mantener la seguridad del vuelo en el ámbito operacional, tanto

diurno como nocturno a través de la instrucción programada por el DIEDOC y DEPLANO" (Ejercito, 2022).

Línea de Autoridad.

"El Departamento Simulador de Vuelo es un Órgano de asesoramiento del comando de la Aviación del Ejército, depende directamente del comandante General de la AE; tendrá el mando cuatro secciones (Administrativa, Instrucción y operación, Creación de paisajes y Aula Virtual automatizada). El cargo estará representado por un Oficial Superior con el grado de teniente coronel" (Ejercito, 2022).

Ilustración 3 Organigrama estructural del departamento del simulador de vuelo



3.4. Productos y/o servicios

El departamento de simulador de vuelo como parte fundamental de la cadena de valor del proceso de entrenamiento de tripulaciones de la aviación del ejercito realiza varios servicios internos para la mejor capacitación y entrenamiento del personal aeronáutico del ejército en bienestar de dar a la sociedad un producto de servicio eficiente y moderno en apoyo a la población y al desarrollo nacional según requerimientos del estado y organismos gubernamentales. Además de:

Entrenar al personal de tripulante aéreo que no ha realizado operaciones aéreas durante un periodo de tres meses en coordinación con el SEPAE.

Crear y/o modificar los modelos visualizados de bases de paisajes del simulador integral del helicóptero MI-17 SH.

Participar en el curso de habilitación de 2do comandante de Aeronave de los Helicópteros MI 17 1b, MI-17 SHP y MI-17 SH dirigido a los Oficiales aviadores recientemente graduados de la Escuela de Aviación del Ejército.

Realizar instrucción teórica de los diferentes sistemas del helicóptero MI-17 SH en el aula virtual del Simulador de Vuelo.

3.5. Diagnóstico organizacional

Tabla 3 Análisis FODA

AMENAZAS	FORTALEZAS
• Falta de repuestos por la guerra rusa – ucraniana • Intención de otros institutos armados para administrar el simulador de vuelo.	• Infraestructura moderna • Infraestructura propia • Personal altamente capacitado • Certificación de la empresa
DEBILIDADES	**OPORTUNIDADES**
• Falta de presupuesto para mantenimiento y operatividad • Personal con pocos conocimientos en seguridad informática • Falta de certificación por la DGAC	• Único simulador de vuelo de helicóptero en el Perú • Segundo simulador en Sudamérica para capacitación en helicóptero. • Necesidad de entrenamiento de las tripulaciones de las otras fuerzas armadas

CAPÍTULO IV: RESULTADOS

4.1. Marco metodológico

Se realizará un estudio de tipo descriptivo transversal. Ya que será un tipo de investigación que tiene como objetivo describir o caracterizar un fenómeno o grupo de personas. En un estudio descriptivo, los investigadores recopilan información sobre las características de una población o un fenómeno y luego utilizan técnicas estadísticas para resumir y presentar los datos de manera clara y concisa

Y será transversal ya que que se miden las variables de interés en un solo momento en el tiempo. Por lo tanto, los investigadores recopilan información sobre la población o el fenómeno en un momento dado y analizan los datos para describir las características de la población en ese momento.

De diseño por combinación entre encuesta y guía de observación.

En este diseño de encuesta, los investigadores utilizan una encuesta o cuestionario para recopilar información sobre las características de la población o el fenómeno de interés. La encuesta puede ser en persona, por teléfono o en línea, y puede incluir preguntas abiertas o cerradas.

Y en la observación, los investigadores observan y registran las características de la población o el fenómeno de interés. La observación puede ser naturalista, participante o no participante. La observación naturalista implica observar un fenómeno en su entorno natural sin interferencia, mientras que la observación participante implica la participación activa del investigador en el fenómeno. La observación no participante implica la observación del fenómeno desde una perspectiva neutral sin participación activa.

La población es de 8 trabajadores que laboran en el departamento de simulador de vuelo de la aviación del ejército durante el AF 2022. Una población es el conjunto total de individuos, objetos o eventos que comparten características comunes y son relevantes para una pregunta de investigación específica.

En un estudio de investigación aplicada, la población puede ser un grupo de personas, una comunidad, un grupo de objetos, una industria, una organización, etc. que se encuentra en un contexto específico y que es relevante para la pregunta de investigación. Es importante definir la población claramente al inicio de la investigación para asegurarse de que los resultados sean relevantes y aplicables a la población de interés.

El estudio será con una muestra total o estudio poblacional. Esto significa que se incluye a todos los individuos o elementos de la población en la investigación, y no se realiza una selección de muestra.

Este tipo de diseño es adecuado cuando la población es pequeña y accesible, y cuando se dispone de los recursos necesarios para incluir a todos los individuos en la investigación. Sin embargo, también es importante tener en cuenta que un estudio con una muestra total puede ser más costoso y requerir más tiempo que un estudio con una muestra representativa.

Las herramientas utilizadas son la encuesta y la guía de observación.

Las encuestas pueden ser administradas en persona, por correo, por teléfono o en línea, y suelen incluir preguntas cerradas y abiertas sobre temas específicos.

La observación es otro tipo de instrumento de recolección de datos que se utiliza para registrar y describir las acciones y comportamientos de las personas, grupos o

eventos. La observación puede ser no participante, en la que el observador no interviene en la situación que está observando, o participante, en la que el observador se integra en la situación para obtener una perspectiva más cercana y detallada.

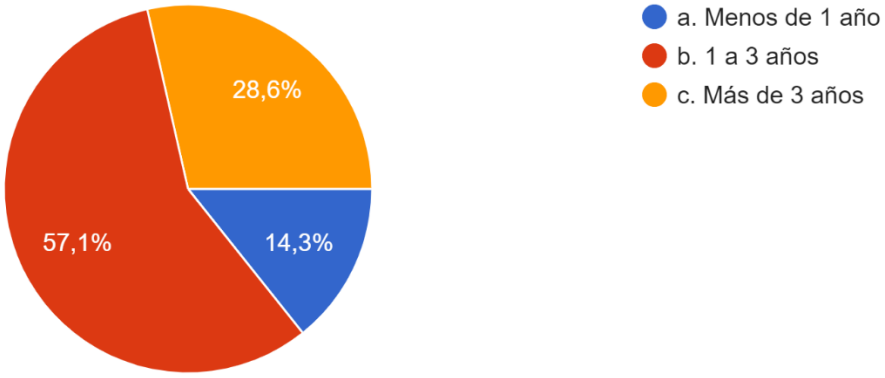
Ambos instrumentos son útiles en investigaciones descriptivas y fueron utilizadas juntos para complementar y validar la información obtenida.

4.2. Resultados

Resultados de la encuesta.

De la pregunta N.º 1, sobre el tiempo laborando en el simulador de vuelo, se pudo identificar que un 57,1 % de trabajadores tienen de 1 a 3 años trabajando en el simulador de vuelo, un 28, 6 % mas de tres años y solo un 14, 3% menos de un año.

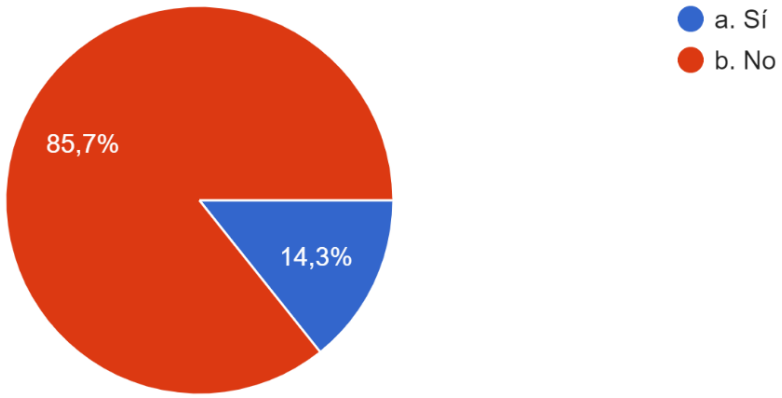
Ilustración 4. Tiempo trabajado en el simulador de vuelo.



Fuente propia

De la pregunta N.º 2, sobre si el personal ha recibido capacitación de seguridad informática en el simulador de vuelo un 85,7% del personal manifiesta ni haber recibió instrucción y solo un 14,3 % manifiesta no haberla recibido.

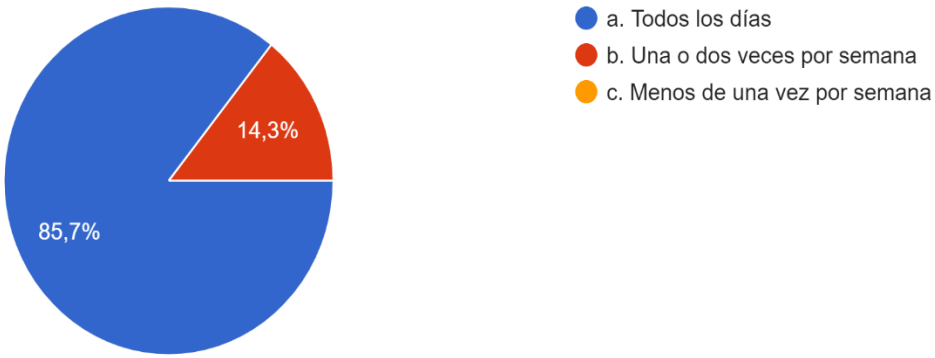
Ilustración 5 Personal que ah recibido capacitacion en gestion de seguridad informatica.



Fuente propia

De la pregunta N.º 3, sobre la utilización de dispositivos electrónicos en el simulador de vuelo el 85.7% manifiesta que utiliza todos los días los dispositivos electrónicos en el simulador de vuelo y solo un 14.3% utilizan uno o dos veces por semana.

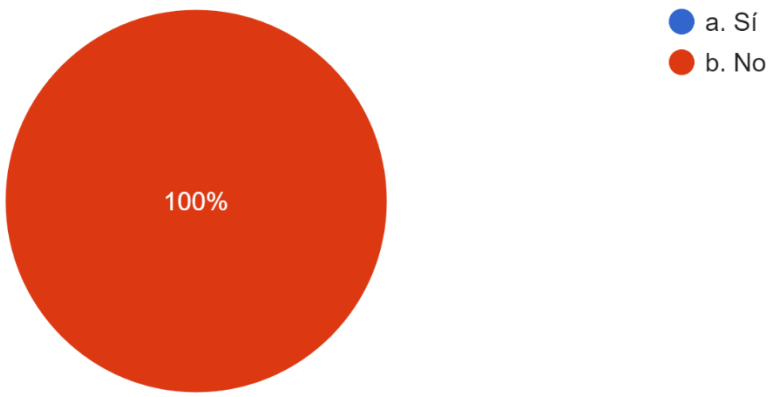
Ilustración 6 Temporalidad de dispositivos electrónicos en el simulador de vuelo.



Fuente propia

De la pregunta N.º 4, el 100% de los trabajadores del departamento del simulador de vuelo manifestaron no tener conocimientos sobre procedimientos de seguridad para dispositivos electrónicos.

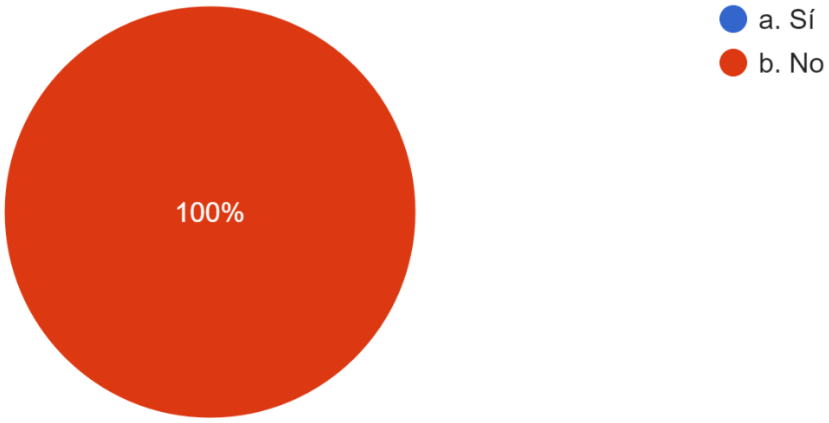
Ilustración 7 sobre el conocimiento en procedimientos de seguridad para dispositivos electrónicos.



Fuente propia

De la pregunta N.º 5, el 100 % de los trabajadores del departamento de simulador de vuelo manifiesta no haber recibido información sobre cómo proteger la información confidencial en el simulador de vuelo.

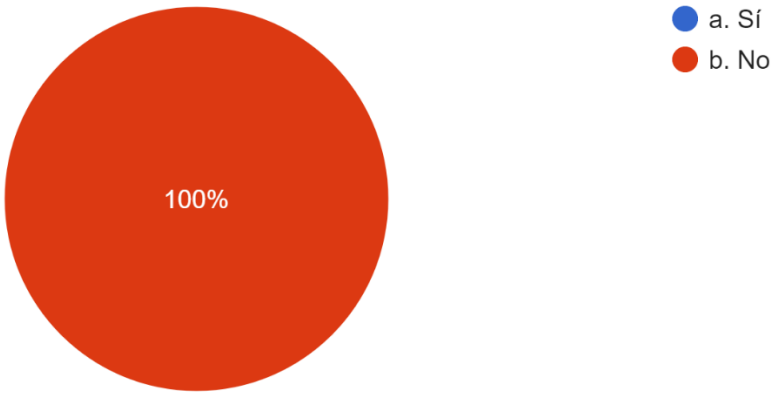
Ilustración 8 Conocimiento de información sobre cómo proteger la información confidencial



Fuente propia

De la pregunta N.º 6, el 100 % de los trabajadores del departamento de simulador de vuelo manifestaron no haber recibido información como identificar y prevenir el malware en el simulador de vuelo.

Ilustración 9 Conocimiento sobre información de como identificar y prevenir el malware.

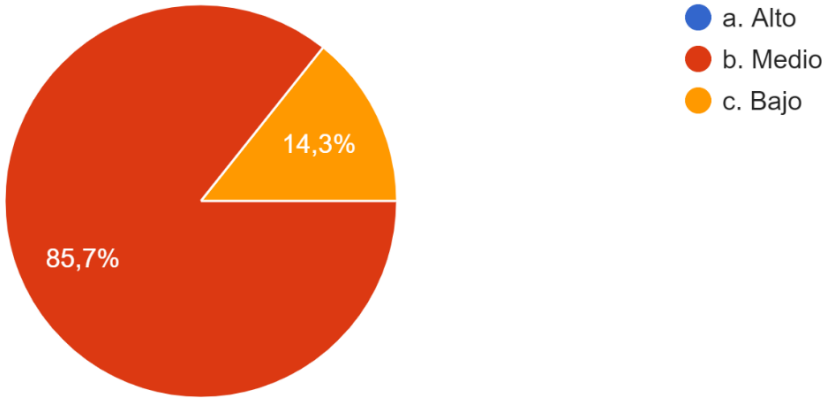


Fuente propia

De la pregunta N.º 7, el 85.7% de los trabajadores del simulador de vuelo manifestaron tener un conocimiento medio sobre seguridad informática y solo un 14.3 %

manifestaron tener un bajo conocimiento en seguridad informática en el simulador de vuelo.

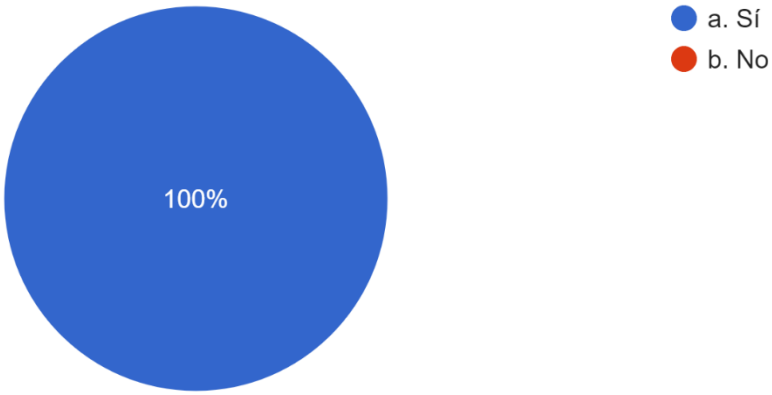
Ilustración 10 Nivel de conocimiento sobre seguridad informática en el simulador de vuelo.



Fuente propia

De la pregunta N.º 8, el 100% de los trabajadores del simulador de vuelo están dispuestos a recibir capacitación sobre seguridad informática.

Ilustración 11 Disposición a recibir capacitación sobre seguridad informática



Fuente propia

Al realizar la evaluación de las encuestas y guía de observación se pudieron determinar los siguientes datos:

Resultados de la ficha de observación.

Tabla 4 tabal de resultados de la ficha de observación de seguridad informática

Nº	Actividad	Observación – Resultado
1	Identificación de la ubicación y los trabajadores: Anote el nombre y el cargo de los trabajadores que están utilizando dispositivos electrónicos en el simulador de vuelo.	El 100 % de los trabajadores utilizan dispositivos electrónicos en el simulador de vuelo durante el periodo laboral ya sea para cuestiones laborales o personales.
2	Observación de la utilización de dispositivos electrónicos: Observe cómo los trabajadores utilizan los dispositivos electrónicos en el simulador de vuelo, incluida la frecuencia de uso y el tipo de dispositivos utilizados.	Los trabajadore sen su mayoría utiliza laptops, computadoras, tables, celulares, pendrives además de los dispositivos propios del simulador en una carencia de 4 veces por hora.
3	Verificación de los procedimientos de seguridad: Observe si los trabajadores están siguiendo los procedimientos de seguridad para dispositivos electrónicos establecidos en el simulador de vuelo.	No hay normas claras o establecidas en el simulador de vuelo que puedan normar y restringir el desarrollo de utilización de dispositivos electrónicos dentro del simulador de vuelo.
4	Evaluación del conocimiento sobre seguridad informática: Observe si los	De las charlas y conversaciones con el personal que labora dentro del

	trabajadores demuestran un conocimiento adecuado sobre seguridad informática, incluido cómo proteger la información confidencial y cómo identificar y prevenir el malware.	simulador de vuelo se puede apreciar que el conocimiento es regular sobre medidas de seguridad informática, así como en la identificación y prevención de malware.
5	Anotación de las observaciones: Anote sus observaciones detalladas y objetivas sobre la gestión de seguridad informática y el nivel de conocimiento de los trabajadores en el simulador de vuelo.	Se realizaron observaciones detalladas sobre las deficiencias y factores críticos que puedan vulnerar los activos críticos del simulador de vuelo en lo referente a seguridad informática para la elaboración de un plan de gestión de riesgos de seguridad informática en el personal de simulador de vuelo.

Fuente Propia

Discusión de los resultados

Tabla 5. Cuadro de comparación de resultados.

Nº	Resultado de la encuesta	Resultado guía observación	Resultado de comparación
1	Sobre el tiempo laborando en el simulador de vuelo, se pudo identificar que un 57,1 % de trabajadores tienen de 1 a 3 años trabajando en el simulador de vuelo, un 28, 6 % más de tres años y solo un 14,	De la observación de los legajos personales del personal de trabajadores se puede determinar que la rotación del personal no es muy rápida por lo que el personal que labora son los únicos calificados para la	La conclusión que se puede obtener de estos dos resultados es que la mayoría de los trabajadores en el simulador de vuelo tienen de 1 a 3 años de experiencia, y una

	3% menos de un año.	operación y mantenimiento de los dispositivos del simulador de vuelo.	pequeña porción de ellos tienen menos de un año. Además, la rotación del personal es baja, lo que indica que el personal es estable y cualificado para el trabajo en el simulador de vuelo.
2	Sobre si el personal ha recibido capacitación de seguridad informática en el simulador de vuelo un 85,7% del personal manifiesta ni haber recibió instrucción y solo un 14,3 % manifiesta no haberla recibido.	Se pudo observar que no existe un programa ni plan de capacitación en seguridad informática para el personal de simulador de vuelo, y que sus conocimientos adquiridos son autodidactas.	La conclusión de estos dos resultados es que la mayoría del personal en el simulador de vuelo no ha recibido capacitación en seguridad informática, y que actualmente no existe un programa o plan para brindar esta capacitación. El conocimiento en seguridad informática de los trabajadores se adquiere de forma autónoma.
3	Sobre la utilización de dispositivos electrónicos en el simulador de vuelo el 85.7% manifiesta que utiliza todos los días los	Se puede evidenciar el uso en gran mayoría de dispositivos electrónicos durante las labores de mantenimiento y operación	La conclusión de estos dos resultados es que la mayoría del personal en el simulador de vuelo utiliza

	dispositivos electrónicos en el simulador de vuelo y solo un 14.3% utilizan uno o dos veces por semana.	del simulador de vuelo.	dispositivos electrónicos a diario en su trabajo, lo que indica una alta dependencia de estos dispositivos en las labores de mantenimiento y operación del simulador de vuelo. Solo un pequeño porcentaje de ellos utiliza dispositivos electrónicos una o dos veces por semana.
4	El 100% de los trabajadores del departamento del simulador de vuelo manifestaron no tener conocimientos sobre procedimientos de seguridad para dispositivos electrónicos.	Se pudo evidenciar el poco o escaso conocimiento en procedimientos de seguridad informática ni documento normativo que especifique estos procedimientos.	La conclusión de estos dos resultados es que no existe un conocimiento adecuado sobre procedimientos de seguridad informática en el departamento del simulador de vuelo, y que tampoco hay un documento normativo que especifique estos procedimientos. Además, todos los trabajadores del departamento afirman

			no tener conocimiento sobre procedimientos de seguridad para dispositivos electrónicos.
5	El 100 % de los trabajadores del departamento de simulador de vuelo manifiesta no haber recibido información sobre cómo proteger la información confidencial en el simulador de vuelo.	Se puede observar que el personal de trabajadores no ha recibido información escrita, pero si verbal sobre métodos para proteger la información confidencial.	La conclusión de estos dos resultados es que todos los trabajadores en el departamento del simulador de vuelo afirman no haber recibido información escrita sobre cómo proteger la información confidencial en el simulador de vuelo. Sin embargo, se ha dado información verbal sobre métodos para proteger la información confidencial. Esto indica una falta de medidas formales y escritas en cuanto a la protección de información confidencial en el simulador de vuelo.
6	El 100 % de los trabajadores del	Se puede observar que los trabajadores no han	La conclusión de estos dos resultados es que

	departamento de simulador de vuelo manifestaron no haber recibido información como identificar y prevenir el malware en el simulador de vuelo.	recibido información para prevenir e identificar malware.	todos los trabajadores en el departamento del simulador de vuelo afirman no haber recibido información sobre cómo identificar y prevenir el malware en el simulador de vuelo. Esto indica una falta de conocimiento y medidas para prevenir y detectar malware en el simulador de vuelo.
7	El 85.7% de los trabajadores del simulador de vuelo manifestaron tener un conocimiento medio sobre seguridad informática y solo un 14.3 % manifestaron tener un bajo conocimiento en seguridad informática en el simulador de vuelo.	Se pudo observar conocimientos empíricos sobre seguridad informática, adquiridos por auto preparación o debido a conocimientos impartidos en anteriores lugares laborales.	La conclusión de estos dos resultados es que la mayoría de los trabajadores en el departamento del simulador de vuelo tienen un conocimiento medio en seguridad informática, pero solo una minoría tiene un conocimiento bajo. Estos conocimientos han sido adquiridos por la auto preparación o por experiencias previas en otros lugares de trabajo.

			Esto indica que, aunque una parte de los trabajadores tiene un nivel de conocimiento medio en seguridad informática, puede ser insuficiente para garantizar una protección adecuada en el simulador de vuelo.
8	El 100% de los trabajadores del simulador de vuelo están dispuestos a recibir capacitación sobre seguridad informática.	Se puede observar la buena fe del personal de trabajadores para ser capacitados en seguridad informática, a fin de ser utilizados en las actividades del simulador.	Se puede concluir que existe una necesidad y disposición por parte del personal de trabajadores en el departamento del simulador de vuelo para recibir capacitación en seguridad informática, ya que todos están dispuestos a recibirla.

Fuente propia

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES O SUGERENCIAS

5.1. Conclusiones

El nivel de conocimiento de los trabajadores sobre seguridad informática en el simulador de vuelo de la aviación del ejército del Perú es insuficiente y necesita ser mejorado. Por lo que se proporciona lineamientos para mejorar la gestión de seguridad informática, esencialmente para tomar medidas de mejora en la gestión de seguridad informática y proteger la información confidencial, así como asegurarse de que los trabajadores tengan los conocimientos y habilidades necesarios para desempeñar sus tareas de manera segura y efectiva.

El nivel de conocimiento de los trabajadores del simulador de vuelo en la aviación del ejército del Perú es de un nivel medio o bajo de conocimiento en seguridad informática y no han recibido información o capacitación formal en este ámbito. Por lo tanto, es fundamental para el Ejército del Perú considerar la importancia de la seguridad informática y brindar capacitación al personal para garantizar la protección adecuada de la información confidencial en el simulador de vuelo.

Se ha identificado que las prácticas actuales de gestión de seguridad informática, actualmente en el simulador de vuelo de la aviación del ejército del Perú, mostrando una falta de conocimientos en seguridad informática y una carencia de prácticas actuales de gestión de seguridad informática. Es importante implementar un programa de capacitación para mejorar los conocimientos de los trabajadores y asegurar una adecuada gestión de la seguridad informática en el simulador de vuelo.

La efectividad de las prácticas actuales de gestión de seguridad informática en el simulador de vuelo de la aviación del ejército del Perú es incierta debido a la falta de

capacitación en seguridad informática y la falta de información sobre cómo identificar y prevenir el malware. Es necesario evaluar y fortalecer las prácticas actuales de gestión de seguridad informática para garantizar la protección de la información confidencial y prevenir riesgos de seguridad informática en el simulador de vuelo.

5.2. Recomendaciones o sugerencias

Es importante que la aviación del ejército del Perú proporcione capacitaciones regulares y actualizadas a sus trabajadores sobre seguridad informática en el simulador de vuelo. Además, se deben implementar políticas y procedimientos claros y específicos sobre seguridad informática, incluyendo cómo identificar y prevenir malware y cómo proteger la información confidencial.

El Ejército del Perú debe implementar un programa de capacitación y educación en seguridad informática para los trabajadores del simulador de vuelo, con el objetivo de mejorar su conocimiento y prevenir posibles riesgos en la seguridad de la información confidencial.

Implementar un diagnóstico de seguridad informática para los trabajadores y activos críticos del simulador de vuelo de la aviación del ejército del Perú, para asegurar un correcto manejo de la información y dispositivos electrónicos en el simulador de vuelo.

Implementar una evaluación exhaustiva de las prácticas actuales de gestión de seguridad informática en el simulador de vuelo de la aviación del ejército del Perú. Esta evaluación debería incluir una revisión de los procedimientos y políticas actuales, una evaluación de la implementación y aplicación de estos procedimientos y políticas, así como una evaluación de la efectividad de estos procedimientos y políticas en la

protección de la información confidencial y en la prevención de malware y otros riesgos de seguridad informática.

BIBLIOGRAFÍA

Administration., F. A. (2014). *Federal Aviation Administration.* AC 61-136A: https://www.faa.gov/search/?q=AC+61-136A+-+Federal

Aguilera, P. (2011). *Redes seguras (Seguridad informática).* Madrid: Editex.

Aguirre, J. R. (2014). *Libro electrónico de seguridad Informática y Criptografía.* Madrid: Universidad Politécnica de Madrid.

Alston, C. (29 de octubre de 2014). *Correlational Studies in Psychology: Examples, Advantages & Types.* https://study.com/academy/lesson/correlational-studies-in-psychology-examples-advantages-types.html

Arias, E. R. (10 de diciembre de 2020). *Economipedia.com*.

Arias, F. (2012). *El proyecto de investigación. Introducción a la metodología científica (6° Edición ed.) .* Caracas: Editorial Episteme.

Bermúdez, L. &. (2013). *Investigación en la gestión empresarial.* Bogotá: Ecoe Ediciones.

Bernal torres, C. A. (2010). *Metodología de la investigación. Administración, economía, humanidades y ciencias sociales.* colombia: Pearson.

Bernard, M. (2012). Real learning throught flight simulatión: The ABcs of ATDs. *FAA*, 8-10.

Briñez Bautista, M. L. (2017). *Diseño de un sistema de gestion de seguridad informatica.* La Jagua de Ibirico: Universidad nacional abierta y a distancia UNAD.

Britto, L. (2013). *La Ciencia: Fundamentos y Método.* Caracas: Ediciones de la Universidad Bolivariana de Venezuela.

Delgado Saavedra, M. M., & Vásquez Zevallos, J. L. (2019). *Diagnóstico de la seguridad informática de los.* Chiclayo: Universidad de Lambayeque.

Díaz, J. (2003). *Modelo de la gestión del conocimiento (GC) aplicado.* Lima: Universidad Nacional Mayor de San Marcos.

Ejercito, A. d. (2022). *Manual de organizacion y funciones.* Lima: Ejercito del Peru.

Guardia Tamara, R. V. (2020). *Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del instituto de educación superior tecnológico publico "Eleazar Guzmán Barrón"- Huaraz - 2018.* Huaraz: Universidad Nacional Santiago Antúnez de Máyalo.

Hernández, R. F. (2014). *Metodología de la investigación.* México D.F.: McGraw-Hill.

ISOTools Excellence. (26 de enero de 2017). *ISOTools Excellence*. https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Merino Rosas, A. A. (2020). *Diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa RANSA comercial S.A- Piura; 2020.* Piura: Universidad Católica los Ángeles de Chimbote.

Nieto, S. &. (2010). *Investigación y evaluación educativa en la sociedad del conocimiento.* Salamanca: Universidad de Salamanca.

López, M. (2017). Metodologías y técnicas de investigación social. Pearson.

Pareja, R. (2013). *El Hombre Multidimensional vive en la Realidad Multidimensional.* Bloomington: Palibrio.

Pérez, R. G. (2012). *Métodos y diseños de investigación en educación.* Madrid: Editorial UNED.

Querales, M., Ruiz, N., Rojas, S., & Espinoza, M. (2011). *Nivel de conocimiento sobre factores de riesgo cardiovascular en una comunidad de Naguanagua, Venezuel.* Naguanagua: Universidad de Carabobo.

Roa Buendía, J. F. (2013). *Seguridad Informatica.* Madrid: Mc Graw-Hill.

Robson, C. (2011). Real world research: A resource for social scientists and practitioner-researchers (3rd ed.). John Wiley & Sons.

Rojas, R. (2013). *Guía para realizar investigaciones sociales.* Mexico D.F.: Plaza y Valdés.

Romero Castro, Martha Irene; Figueroa Moràn, Grace Liliana ; Vera Navarrete, Denisse Soraya;. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Manabi: Editorial Área de Innovación y Desarrollo,S.L.

Sampieri, R. H., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la investigación.* México: Mc Graw Hill.

Sanz, M. (2021). Seguridad lógica de los sistemas informáticos y de comunicaciones. Ingeniería del Software y Tecnologías de la Información, 13(2), 43-55

Sánchez, R. (2014). *Enseñar a investigar. Una didáctica nueva de la investigación en ciencias sociales y humanas.* México D.F.: Universidad Nacional Autónoma de México.

Silva Coelho, F. E., Segadas de Araújo, L. G., & Kowask Bezerra, E. (2018). *Gestión de la seguridad de la informacion.* Ecuador: REDCEDIA.

Tamayo y Tamayo, M. (2012). *El Proceso De La Investigación Científica.* México, D.F.: Limusa.

Tigse Moposita, J. L. (2020). *“plan de gestión de seguridad informática basado en la norma ISO 27001 para el departamento de tecnología de la información en la empresa Plasticaucho industrial S.A.* Ambato: Universidad Técnica de Ambato.

Vázquez, A. (2011). *El cambio como constante histórica.* Alicante: Editorial Club Universitario.

Zambrano Burbano, R. M. (2018). *Estudio sobre el conocimiento y la aplicabilidad de la seguridad informática en las empresas médicas de Bogotá.* Bogotá: Universidad Nacional Abierta y a Distancia.

Whitman, M. E., & Mattord, H. J. (2016). Principles of information security. Cengage Learning.

ANEXOS

Instrumentos de recolección de datos

ENCUESTA

Buenos días/tardes, expresamos nuestro agradecimiento por el tiempo y la atención prestada para poder realizar esta encuesta, cuya información y comentarios proporcionados serán muy valiosos para profundizar la presente investigación

Entrevistados :		
Grado Académico:		
DNI :		
Lugar – fecha :		
Experiencia alcanzada:		
Título de la investigación: La gestión de seguridad informática y el nivel de conocimiento de los trabajadores del simulador de vuelo en la aviación del ejército del Perú, 2022		
N°	**ENCUESTA**	
01	**¿Cuánto tiempo has trabajado en el simulador de vuelo?**	
	Rpta	a. Menos de 1 año b. 1 a 3 años c. Más de 3 años
02	**¿Recibiste capacitación sobre seguridad informática en el simulador de vuelo?**	
	Rpta	a. Sí b. No
03	**¿Con qué frecuencia utiliza dispositivos electrónicos en el simulador de vuelo?**	
	Rpta	a. Todos los días b. Una o dos veces por semana c. Menos de una vez por semana
04	**¿Conoces los procedimientos de seguridad para dispositivos electrónicos en el simulador de vuelo?**	
	Rpta	a. Sí b. No
05	**¿Ha recibido información sobre cómo proteger la información confidencial en el simulador de vuelo?**	
	Rpta	a. Sí b. No
06	**¿Ha recibido información sobre cómo identificar y prevenir el malware en el simulador de vuelo?**	
	Rpta	a. Sí b. No
07	**¿Cómo describiría su nivel de conocimiento sobre seguridad informática en el simulador de vuelo?**	
	Rpta	a. Alto b. Medio c. Bajo
08	**¿Está dispuesto a recibir más capacitación sobre seguridad informática en el simulador de vuelo?**	
	Rpta	a. Sí b. No

GUÍA DE OBSERVACIÓN

Objetivo: Describir las acciones realizadas en gestión de seguridad informática y el nivel de conocimiento de los trabajadores del simulador de vuelo en la aviación del ejército del Perú, 2022.

N°	ASPECTOS A ANALIZAR	SI	NO	TAL VEZ	OBSERVACIONES
1	Identificación de la ubicación y los trabajadores: Anote el nombre y el cargo de los trabajadores que están utilizando dispositivos electrónicos en el simulador de vuelo.				
2	Observación de la utilización de dispositivos electrónicos: Observe cómo los trabajadores utilizan los dispositivos electrónicos en el simulador de vuelo, incluida la frecuencia de uso y el tipo de dispositivos utilizados.				
3	Verificación de los procedimientos de seguridad: Observe si los trabajadores están siguiendo los procedimientos de seguridad para dispositivos electrónicos establecidos en el simulador de vuelo.				
4	Evaluación del conocimiento sobre seguridad informática: Observe si los trabajadores demuestran un conocimiento adecuado sobre seguridad informática, incluido cómo proteger la información confidencial y cómo identificar y prevenir el malware.				
5	Anotación de las observaciones: Anote sus observaciones detalladas y objetivas sobre la gestión de seguridad informática y el nivel de conocimiento de los trabajadores en el simulador de vuelo.				

Lineamientos para mejorar la gestión de seguridad informática del simulador de vuelo de la aviación del ejército del Perú.

Estos lineamientos serán incluidos en el plan de seguridad informática del simulador de vuelo para ser desarrollados durante el plan anual, a fin de mejorar progresivamente la gestión de seguridad informática dentro del área.

1. Identificar las debilidades y fortalezas actuales de la gestión de seguridad informática en el simulador de vuelo y el nivel de conocimiento de los trabajadores.
2. Analizar las normativas y buenas prácticas existentes en el ámbito de la seguridad informática en simuladores de vuelo y en empresas similares.
3. Establecer objetivos claros y medibles para mejorar la gestión de seguridad informática y el nivel de conocimiento de los trabajadores.
4. Desarrollar un plan de acción para implementar los lineamientos, incluyendo actividades de capacitación, actualización de políticas y procedimientos, y mejora de la infraestructura tecnológica.
5. Asignar responsabilidades y recursos para la ejecución del plan de acción.
6. Evaluar regularmente los avances y resultados del plan de acción y hacer ajustes según sea necesario.
7. Realizar una investigación exhaustiva en el análisis de las amenazas y riesgos específicos asociados al uso del simulador de vuelo.
8. Identificación de los activos críticos y la definición de medidas específicas de seguridad para protegerlos.
9. Involucrar a expertos en seguridad informática en la planificación y ejecución de los lineamientos para garantizar que sean adecuados y efectivos.