Brecha de seguridad en el correo electrónico institucional y su impacto en la infraestructura crítica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre en el año 2022.

Arias Peña, Cristian Fernando y Dávila Mejía, Nelson Xavier

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Defensa y Seguridad

Trabajo de titulación, previo a la obtención del título de Magíster en Defensa y Seguridad mención Estrategia Militar

Muñoz Morales, Bethy Andrea Mgtr.

16 de noviembre del 2023

Copyleaks

Plagiarism report

REVISION_FINAL_TESIS_ARIAS_DAVILA...

Scan details

Scan time:	Total Pages:	Total Words:
September 11th, 2023 at 22:39 UTC	111	27718

Plagiarism Detection

7.2%

Types of plagiarism		Words
Identical	6.9%	1907
Minor Changes	0%	0
Paraphrased	0%	0
Omitted Words	4.5%	1246

AI Content Detection

N/A

Text coverage

- AI text
- Human text

Sangolquí, 16 de noviembre de 2023

Firmado electrónicamente por:
BETHY ANDREA MUÑOZ MORALES

.....

Muñoz Morales Bethy Andrea

Director

C.C: 1714086236

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación: "**Brecha de seguridad en el correo electrónico institucional y su impacto en la infraestructura crítica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre en el año 2022.**" fue realizado por los señores **Arias Peña Cristian Fernando y Dávila Mejía Nelson Xavier;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 16 de noviembre de 2023

Firmado electrónicamente por:
BETHY ANDREA MUÑOZ MORALES

Muñoz Morales Bethy Andrea

Director

C.C: 1714086236

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de autoría

Nosotros, **Arias Peña Cristian Fernando y Dávila Mejía Nelson Xavier**, con cédulas de ciudadanía N° 1900241702 y 1714014733, declaramos que el contenido, ideas y criterios del trabajo de titulación*:* "**Brecha de seguridad en el correo electrónico institucional y su impacto en la infraestructura crítica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre en el año 2022.**" es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 16 de noviembre de 2023

CRISTIAN FERNANDO ARIAS PEÑA
Firmado digitalmente por CRISTIAN FERNANDO ARIAS PEÑA
Fecha: 2023.11.20 16:11:09 -05'00'

.....
Arias Peña Cristian Fernando
C.C: 1900241702

Firmado electrónicamente por:
NELSON XAVIER DAVILA MEJIA

.....
Dávila Mejía Nelson Xavier
C.C: 1714014733

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Autorización de Publicación

Nosotros, **Arias Peña Cristian Fernando y Dávila Mejía Nelson Xavier**, con cédulas de ciudadanía N° 1900241702 y 1714014733, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación:*:* "**Brecha de seguridad en el correo electrónico institucional y su impacto en la infraestructura crítica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre en el año 2022.**" en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 16 de noviembre de 2023

CRISTIAN FERNANDO ARIAS PEÑA
Firmado digitalmente por CRISTIAN FERNANDO ARIAS PEÑA
Fecha: 2023.11.20 16:11:23 -05'00'

.....
Arias Peña Cristian Fernando
C.C: 1900241702

Firmado electrónicamente por:
NELSON XAVIER DAVILA MEJIA

.....
Dávila Mejía Nelson Xavier
C.C: 1714014733

Dedicatoria

Muchas fueron las personas que me ayudaron enormemente durante todo este proceso de enseñanza aprendizaje dentro del curso de Estado Mayor CEMA74, para lograr escalar tanto profesional como técnicamente en mi carrera militar.

Dedico este trabajo a mis instructores de la Academia de Guerra del Ejército por darme las herramientas necesarias para desarrollar un pensamiento crítico y analítico dentro de un nuevo escenario VICA; a mis preciosas hijas, Shantal, Kristen, Natasha y mi amada esposa Lina, por su apoyo y comprensión en este proceso. Espero con este proyecto aportar con un grano de arena en el desarrollo de la institución que me ha dado todo.

(Arias Peña, Cristian Fernando)

Dedico con todo mi amor este trabajo de investigación, primeramente a Dios, por darme la vida y la oportunidad de haber llegado a realizar el Curso de Estado Mayor, a mi esposa Daniela, a mis hijos Danielle, Emiliano, a mi querida madrecita Amparito y a mi papito Nelson que está en el cielo, quien son y han sido parte integral de mi vida, siendo el soporte e inspiración para alcanzar esta meta académica, ya que, gracias a su amor, ternura y comprensión, he logrado conseguir los objetivos que me he propuesto.

A mi estimado amigo y compañero Cristian Arias, que con su confianza y apoyo ha permitido culminar con éxito esta etapa y reafirma el compromiso de seguir luchando por metas futuras.

(Dávila Mejía, Nelson Xavier)

Agradecimiento

Iniciaré agradeciendo a Dios por guiar mi camino, a mis abuelitos Florita y Víctor Hugo que desde el cielo me inspiran a conseguir mis objetivos, a mi Madre Martha que siempre me apoya incondicionalmente a la distancia, a mi Esposa Lina y a mis adorables Hijas quienes me han brindado su amor, cariño, comprensión y apoyo en todo momento. Mi éxito es el de ustedes, ¡las amo!

(Arias Peña, Cristian Fernando)

Mis más sinceros agradecimientos a mi carrera militar, al glorioso Ejército Ecuatoriano, al mejor instituto de pensamiento estratégico del Ecuador, que es la Academia de Guerra del Ejército y con ella a todos los oficiales directivos, docentes, personal de planta y personal administrativo, muchas gracias por sus conocimientos y servicios prestados, todos ellos han contribuido a formarme como oficial de Estado Mayor y culminar esta etapa de mi vida profesional ¡Muchas gracias!

(Dávila Mejía, Nelson Xavier)

Índice

Índice de Tablas

Índice de figuras

Resumen

El presente trabajo de investigación, busca analizar la situación actual de vulnerabilidad a la que está expuesta la infraestructura tecnológica digital de la Fuerza Terrestre a través de posibles brechas de seguridad físicas y lógicas en el servidor de correo electrónico institucional y el impacto que puede alcanzar en los aplicativos que mantiene en producción. Inicialmente se plantea el problema a resolver, luego se determina los objetivos de investigación. Se desarrolla una revisión bibliográfica respecto a la ciberseguridad y la ciberdefensa en el contexto militar a nivel mundial, regional y nacional mediante la utilización de fuentes primarias y datos estadísticos. La revisión exploratoria documental se desarrolla en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC FT). Se aplica el método científico con un enfoque cualitativo, planteando la hipótesis de investigación conjuntamente con las variables, posteriormente se aplica el método, técnicas e instrumentos de recolección de datos para su análisis e interpretación. Con los resultados y hallazgos se plantea implementar una propuesta de guía metodológica basada en la NORMA ISO/IEC 27001 y el Esquema Gubernamental de Seguridad de la Información (EGSI) en su última versión, lo cual permite evaluar la situación actual de vulnerabilidad, establecer una línea base para la implementación de políticas de seguridad que permitan incrementar la seguridad de la información que se almacena en los servidores de correo electrónico de la Fuerza Terrestre. La investigación ayuda a minimizar el impacto de los riesgos a través de conceptualizaciones doctrinarias, análisis de vulnerabilidades y concientización de los usuarios que administran y consumen la información disponible. Finalmente, la investigación concluye identificando las deficiencias tecnológicas, humanas y económicas que podrían ser causales de vulnerabilidad y de esta manera contribuir al fortalecimiento institucional y al desarrollo del país.

Palabras claves: vulnerabilidad, brechas de seguridad, servidor de correo electrónico, seguridad de la información

Abstract

This research work seeks to analyze the current situation of vulnerability to which the digital technological infrastructure of the Land Force is exposed through possible physical and logical security breaches in the institutional email server and the impact it can reach in the applications it maintains in production. A literature review regarding cybersecurity and cyber defense in the military context at global, regional and national levels is developed through the use of primary sources and statistical data. The exploratory documentary review is carried out in the Directorate of Information Technologies and Communications of the Land Force (DTIC FT). The scientific method is applied with a qualitative approach, raising the research hypothesis together with the variables, then the method, techniques and instruments of data collection are applied for analysis and interpretation. With the results and findings, it is proposed to implement a proposal for a methodological guide based on the ISO/IEC 27001 STANDARD AND THE GOVERNMENT INFORMATION SECURITY SCHEME (EGSI) in its latest version. Which allows to evaluate the current situation of vulnerability, establish a baseline for the implementation of security policies that allow to increase the security of the information that is stored in the email servers of the Ground Force. Finally, the research concludes by identifying the technological, human and economic deficiencies that could be causes of vulnerability and thus contribute to the institutional strengthening and development of the country.

Keywords: vulnerability, security gaps, email server, information security

.

Capítulo I

Planteamiento del problema

Planteamiento del Problema de Investigación

El gobierno ecuatoriano en su esfuerzo por minimizar los riesgos ante ciberataques ha desarrollado algunas políticas de seguridad en esta materia, para lo cual en el año 2012 implementó el *Centro de Respuesta a Incidentes Informáticos del Ecuador* (Ecucert) para mitigar incidentes informáticos en el País, también a partir del año 2013 se establecen políticas sustentables a largo plazo como es la emisión del Acuerdo Ministerial No 166 por parte de la Secretaria Nacional de la Administración Pública, en la cual decreta que todas las instituciones públicas que sean dependientes de la función ejecutiva, implementen de forma obligatoria el Esquema Gubernamental de Seguridad de la Información (EGSI) en sus instituciones (Borbúa, Herrera, & Reyes, 2017). A partir del año 2014, Fuerzas Armadas (FF. AA) del Ecuador implementó el Comando de Ciberdefensa (COCIBER) para contrarrestar ciberataques, ciberguerra y espionaje a entidades estratégicas del Estado que provengan de cualquier parte del mundo (Comercio, 2014). En marzo del año 2021 se asignan competencias específicas al COCIBER en temas de ciberseguridad, el cual dentro de sus procesos gobernantes tienen la capacidad de realizar exploración defensa y respuesta ante ciberataques que se presenten en la infraestructura tecnológica de las unidades militares que pertenecen al Comando Conjunto de Fuerzas Armadas (CC.FF. AA).

Terminado el año 2022 es importante determinar lo que ha sucedido en el campo de la ciberdefensa en Latinoamérica, decantando en el Ecuador y específicamente en su Fuerza Terrestre (FT), en ese sentido, es necesario determinar cómo se encuentra actualmente su infraestructura tecnológica digital, determinar las posibles vulnerabilidades informáticas a la que están expuestas los servidores de correo electrónico institucional, así mismo determinar si en base al presupuesto asignado para la seguridad de la información a la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC FT), dispone de

personal capacitado y herramientas tecnológicas que le permitan ser resiliente ante ciberataques, lo cual pueda ser una causa para dar paso a posibles brechas de seguridad tanto lógicas como físicas que afecten a la seguridad de la información de la Fuerza Terrestre (FT).

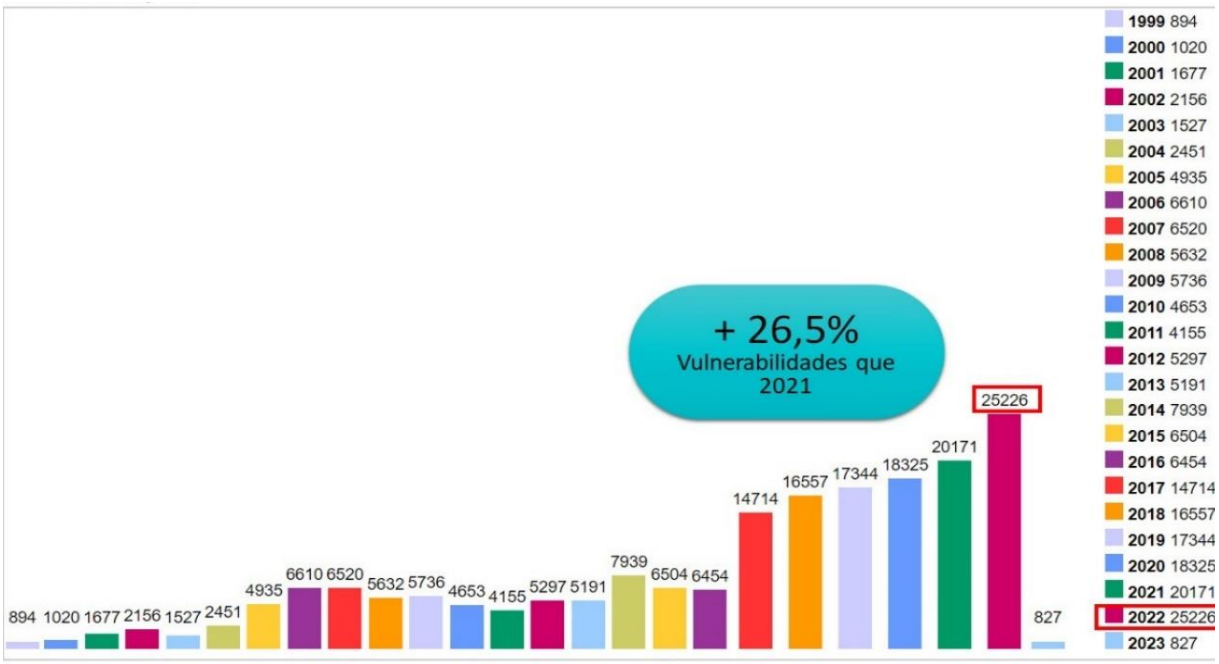
En el mes de junio de 2022, el Ministerio de Telecomunicaciones (MINTEL) publica la Política Nacional de Ciberseguridad para garantizar los derechos digitales de los ecuatorianos en el ciberespacio la cual está sustentada en siete pilares:

1. Gobernanza de ciberseguridad.
2. Sistemas de información y gestión de incidentes.
3. Protección de servicios e infraestructuras críticas digitales.
4. Soberanía y defensa.
5. Seguridad pública y ciudadana.
6. Diplomacia en el ciberespacio y cooperación internacional.
7. Cultura y educación de ciberseguridad.

Actualmente, existe un raudo crecimiento de ataques y vulneraciones informáticas a la infraestructura tecnológica de las instituciones tanto públicas como también las privadas, mismas que en su mayoría son detectadas a nivel mundial y en diferentes sistemas operativos, servidores, aplicativos, dispositivos, etc., evidenciando la exposición a la que se enfrentan a diario estas instituciones y los nuevos escenarios a los que se enfrentan al descuidar la seguridad informática (CVE Details). A continuación, en la figura 1 se puede visualizar el incremento exponencial de vulnerabilidades reportadas en Latinoamérica en el año 2022, alcanzando un pico histórico con 25226 vulnerabilidades, lo cual representa un crecimiento del 26,5% que han sido reportadas, esto representa a un equivalente de unas 70 vulnerabilidades por día.

Figura 1

Vulnerabilidades por año desde 1999.



Nota. La figura muestra el incremento de vulnerabilidades informáticas en el año 2022 en un 26,5% respecto al año 2021. Tomado de (CVE Details, 2023).

Es muy importante considerar dentro de la seguridad de la información el incremento de ciberataques que sufren a diario las instituciones privadas y públicas del Ecuador, según el informe presentado por (ESET, 2022) se registran detecciones informáticas maliciosas en las empresas ecuatorianas llegando a ocupar un quinto puesto dentro de los 17 países latinoamericanos que han sido evaluados. El país con más detecciones es Perú con un 18%, seguido por México 17%, Colombia 12%, Argentina 11% y Ecuador 9%.

La Fuerza Terrestre del Ecuador tiene varios servicios y aplicativos expuestos a la Internet, entre los que constan: Virtual Private Network (VPN), Correo Electrónico Corporativo (Zimbra), Portales Web, SIFTE, entre otros; adicional como parte la seguridad que brinda a su infraestructura digital dentro de su estructura informática cuenta con equipos de seguridad perimetral distribuidos en todo el territorio nacional, estos equipos disponen de varios módulos

(antivirus, antispam, antimalware, firewall, entre otros); también disponen de una plataforma de antivirus corporativa para los equipos informáticos utilizados en la parte administrativa, estas seguridades implementadas en su infraestructura digital tienen como objetivo principal bloquear posibles intentos de intrusión que se realizan de manera automática mediante herramientas de software que se los conoce como Bots[1] , los módulos implementados no garantizan la seguridad de los equipos finales al interior del sistema informático de la institución, por lo que existe la posibilidad de encontrar fallas o huecos de seguridad y que pueden ser aprovechados por personas inescrupulosas para extraer información. Para realizar la gestión ante incidentes y vulneraciones informáticas a la infraestructura digital de la FT, se necesita contar con personal técnico especializado en la detección y mitigación de vulnerabilidades, así también es indispensable contar con herramientas informáticas que permitan prevenir y estar en la capacidad de enfrentar la resiliencia ante la vulneración de la seguridad de la información y su impacto en su aplicativos, evitando que la infraestructura tecnológica disponible sea afectado por ciberataques relacionados con hacktivismo[2] entre otros.

Formulación del Problema de Investigación

¿Cuál fue el impacto de la brecha de seguridad en el correo electrónico institucional en la infraestructura crítica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre durante el año 2022, y cómo se puede diseñar una guía metodológica que permita implementar controles de seguridad efectivos en respuesta a dicha brecha?

Subproblemas o Preguntas de Investigación

¿Cuál es la percepción de los usuarios de la Fuerza Terrestre sobre el estado de seguridad en el correo electrónico institucional?

[1] Bots (robot): Programas que realizan tareas predefinidas y automatizadas.

[2] Hacktivismo: Forma de protesta social con fines reivindicativos realizada por personal con conocimientos de informática (hackers), aprovechando los fallos de seguridad de las entidades o sistemas gubernamentales.

¿Cómo se describe la situación actual de seguridad de la información implementada en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre en relación con el correo electrónico institucional?

¿Cuál es el impacto de la brecha de seguridad en el correo electrónico institucional en la infraestructura crítica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre?

¿Qué debe contener una guía metodológica basada en la NORMA ISO/IEC 27001 y el EGSI en su última versión, para implementar controles de seguridad en el servidor de correo electrónico institucional de la DTIC FT?

Justificación e Importancia

El presente proyecto está anclado a la Ciberdefensa y Protección de las Infraestructuras Críticas del Estado, enfocado en un análisis de vulnerabilidades y a la brecha de seguridad de la información que se pudiese ocasionar en el servidor de correo electrónico institucional y que afecte a los aplicativos que mantiene en producción la DTIC FT, en la cual se pretende proteger la confidencialidad, integridad y disponibilidad de la información que se almacena de forma digital en sus servidores, empleando personal técnico especialista, así como el uso de herramientas de análisis de vulnerabilidades que permiten detectar y gestionar incidentes o fallos. A través de la gestión de las vulnerabilidades contribuimos a la seguridad en la infraestructura crítica digital de la FT y por ende coadyuva a la seguridad del Estado.

Objetivos de Estudio

Objetivo General

- Analizar el impacto de la brecha de seguridad en el correo electrónico institucional en la infraestructura crítica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre en el año 2022, con el fin de diseñar una guía metodológica que permita implementar controles de seguridad.

Objetivos Específicos

- Diagnosticar el estado de seguridad en el correo electrónico institucional desde la percepción de los usuarios de la Fuerza Terrestre y, evaluar la situación de seguridad de la información implementada en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre para determinar la brecha de seguridad en el correo electrónico institucional.
- Medir el impacto de la brecha de seguridad en el correo electrónico institucional en la infraestructura critica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre.
- Diseñar una guía metodológica que permita implementar controles de seguridad en la DTIC FT (servidor de correo electrónico institucional), basado en la NORMA ISO/IEC 27001 y el EGSI en su última versión.

Capítulo II:

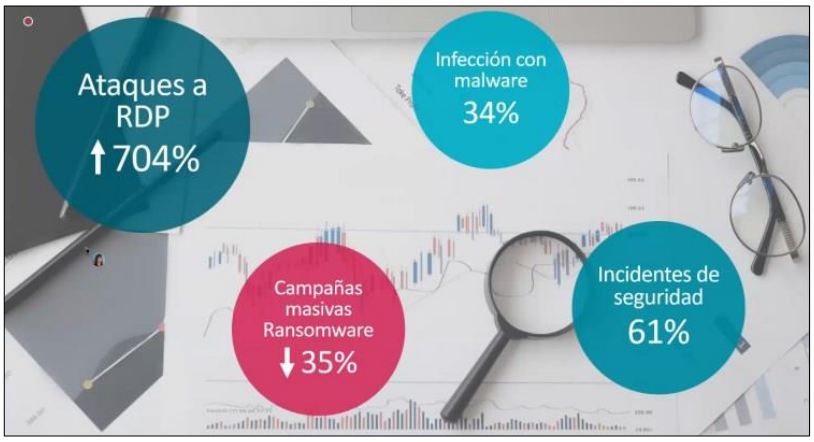
Marco teórico

Estado del arte

En Latinoamérica, en el año 2020 hubo un incremento del 704% en ataques de escritorio remoto (RDP[3]) por ciberdelincuentes en diferentes modalidades, las campañas masivas de ransomware disminuyeron en un 35%. El 61% de las empresas reportaron al menos un incidente de seguridad, el 39% no tuvieron incidentes o no se dieron cuenta que lo habían tenido. Un 34% de las empresas sufrieron infecciones con malware, del 20% de las empresas una de cada cinco reportó ataques con ingeniería social, 10% explotación de vulnerabilidades y el 9% incidentes de ransomware (Report Eset, 2021). En la figura 2 se puede obtener un resumen de los ataques informáticos en el año 2020.

Figura 2

Ataques informáticos el Latinoamérica en el año 2020



Nota. La figura muestra los ataques informáticos en Latinoamérica en el año 2020. Tomado de (Report Eset, 2021).

En el Ecuador , específicamente en sus Fuerzas Armadas, a partir del año 2013 se establecen políticas sustentables a largo plazo en lo referente a seguridad de la información, se puede considerar como hitos importantes en este tema, la emisión del Acuerdo Ministerial No

[3] RDP, por sus siglas en ingles Remote Desktop Protocol.

166 por parte de la Secretaria Nacional de la Administración Pública, para implementar de forma obligatoria el Esquema Gubernamental de Seguridad de la Información (EGSI) en sus instituciones; otro hito importante es la creación en el año 2014 del Comando de Ciberdefensa (COCIBER) en el Comando Conjunto de Fuerzas Armadas, para contrarrestar ciberataques y ciberguerra en las Fuerzas (Terrestre, Aérea y Naval) que la conforman, así también a las entidades estratégicas de Estado; siguiendo cronológicamente, en el mes de junio de 2022, el Ministerio de Telecomunicaciones (MINTEL) publica la Política Nacional de Ciberseguridad para garantizar los derechos digitales de los ecuatorianos en el ciberespacio.

En un mundo globalizado e interconectado, el uso y abuso del internet para realizar gestiones personales y de trabajo es indispensable, según (Marketing & Ecommerce, 2023) el número de usuarios de internet en el mundo crece en 1,9% y alcanza los 5.160 millones en el 2023, los usuarios de internet en dispositivos móviles alcanzó un 68% de la población, con 5.440 millones de personas, esto evidencia notablemente el crecimiento de usuarios que se conectan a internet en el mundo; hoy por hoy, todo equipo informático o dispositivo móvil con acceso a internet puede ser vulnerable de sufrir ataques informáticos. La Fuerza Terrestre para mantener la confidencialidad, integridad y disponibilidad de su información ha venido implementado varias normativas y protocolos como los que fueron descritos en el párrafo anterior.

Las nuevas Tecnologías de la Información y comunicaciones han evolucionado en los servicios y accesibilidad que ofrecen a los usuarios finales, así como también han implementado estrategias de seguridad para fortalecer la ciberseguridad y ciberdefensa en sus empresas, para proteger uno de los bienes más preciados como es la información, para ello se ha categorizado a la seguridad en diferentes frentes: físico, referente al alojamiento de la información; social, relacionado con el grado de discrecionalidad del personal que la manipula, y el lógico, que se refiere a sus niveles de accesibilidad y disposición (Monsalve, Aponte, & Chaves, 2014). Entre los servicios que ofrece la DTIC FT a sus usuarios, está el uso del correo

electrónico institucional, el cual dispone de un total de 23.000 cuentas asignadas al personal militar y civil que trabaja para la Fuerza Terrestre, considerándose uno de los pilares fundamentales para el flujo de información a través de este servicio.

A continuación, se relacionan algunos estudios que se tomaron como base para la presente investigación:

En el año 2020 se realizó un “Análisis de la Ciberdefensa en la Fuerza Terrestre” (Abad y Sandoval, 2020), en la cual los autores plantean una propuesta para mejorar la ciberdefensa en la Fuerza Terrestre, mediante un sistema de ciberdefensa. La investigación concluye identificando las deficiencias que imposibilitan el mantenimiento de la ciberdefensa en la Fuerza Terrestre.

En el año 2021 se realizó el “Análisis de las nuevas tecnologías en las TIC´s y el mando y control” (Saltos, 2021) en la cual el autor determina las falencias en la capacidad tecnológica de las TIC´s de la Fuerza Terrestre, enfocado por la obsolescencia tecnológica, otra falencia, es el respaldo técnico que no brinda la oportunidad real de aprovechamiento óptimo de la capacidad de algunas herramientas, otra es la falta de capacitación del personal responsable, dependencia de técnicos externos a la FT y el uso inadecuado de la tecnología existente de forma interna y externa constituyéndose en un riesgo latente a la seguridad de la información.

También se ha realizado artículos técnicos de: “La Protección de la Infraestructuras Críticas en el Ámbito de las Fuerzas Armadas” (Morillo y Duque, 2018). En el año 2021 se publica la Política de ciberseguridad en el Ecuador para fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población ecuatoriana en el ciberespacio.

Con el fin de estandarizar la seguridad de la información y su correcta gestión y organización existen las normas ISO 17799/ISO 27002 e ISO/IEC 27001 dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

Fundamentación Legal

Para desarrollar la presente investigación se necesita disponer una base legal acorde a la realidad nacional, regional y mundial. El presente trabajo de investigación tiene la siguiente fundamentación legal:

- Constitución de la República (CONSTITUCIÓN, 2008)
  - Artículo 66 numeral 19 reconoce y garantiza “El derecho a la protección de datos de carácter personal.
  - Artículo 227, “La Administración Pública constituye un servicio a la colectividad que se rige por principios de eficacia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación”.
- ISO 27000 y 27001 sobre seguridad de la información. (ISO, 2005)
- Norma NTE INEN-ISO/IEC 27002 “Código de Práctica para la Gestión de la Seguridad de la Información”. (INEN, 2015)
- Ley de Seguridad Pública y del Estado. (Nacional, 2017)
  - Artículo 2. Que describe la protección y control de los riesgos tecnológicos
  - Artículo 43. Que describe la protección de instalaciones e infraestructura
- Objetivos Estratégicos de la FT 2017-2021 (FT, 2017), Objetivo 4 numeral 3 “Fortalecer la capacidad de Ciberdefensa”
- Política Ecuador Digital (MINTEL, 2019)
- Esquema Gubernamental de Seguridad de la Información. (MINTEL, Esquema Gubernamental de Seguridad de la Información (EGSI), 2020)
- Estrategia Nacional de Ciberseguridad (MINTEL, 2022)

Fundamentación Conceptual

Dentro del tema de investigación que nos ataña, existen dos términos muy importantes que se usan con frecuencia, aunque son disímiles, persiguen el mismo objetivo en cada una de las instituciones que es el de crear estrategias y políticas para proteger la información, como son la ***Seguridad de la Información y la Seguridad Informática***, (Roba, Vento, & García, 2016).

Seguridad Informática

Según Canon citado por López Santoyo (2015) plantea que es la disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

Seguridad de la información

Es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

De los dos conceptos antes mencionados, se puede destacar que la principal diferencia es el enfoque que tienen cada uno de ellos, así también las metodologías que utilizan y las áreas específicas en donde se concentren; por ello, estas dos definiciones, aunque parezcan iguales, visiblemente se puede determinar que no lo son.

Correo electrónico

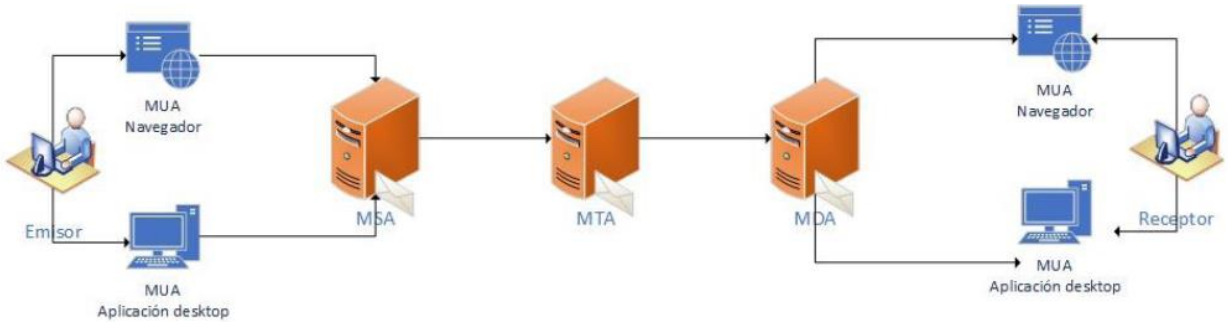
El correo electrónico con sus siglas en ingles e-mail, es un medio digital por cual fluye la información, la cual se genera desde un emisor y puede ser dirigido a uno o varios receptores a través de los diferentes protocolos y estándares que son parte del mismo.

Un correo electrónico consta de dos partes fundamentales: un agente usuario o Mailer y un programa de transporte. El agente de usuario, se utiliza para crear mensajes, leerlos, etc; El programa de transporte, entrega el correo tanto remoto como local cumpliendo con los protocolos de comunicaciones y demás. El usuario no interactúa con un programa de transporte, lo hace a través del agente de usuario (Pérez & Hernández, 2021).

A continuación, en la figura 3 se muestra el funcionamiento básico del correo electrónico.

Figura 3

Funcionamiento del correo electrónico.



Nota. La figura muestra una representación esquemática del funcionamiento de correo electrónico. Tomado de (Pérez & Hernández, 2021)

El servidor de correo electrónico se encarga de realizar la gestión del correo, el cual está en la capacidad de atender varias peticiones de cuentas de correo, además puede definir una cantidad ilimitada de receptores dentro de un mismo dominio, esto de acuerdo a la capacidad adquirida por cada uno de los clientes.

Agentes de correo

Dentro de los agentes de correo, se puede destacar tres clasificaciones, las cuales juegan un papel específico en el proceso de la administración de los mensajes generados en un servidor de correo electrónico, a continuación, se describen cada uno de ellos:

MTA (Mail Transfer Protocol, Agente de transferencia de correo): software que transfiere los mensajes de correo entre host usando SMTP[4].

MDA (Mali Delivery Agent, Agente de entrega de correo): Software que almacena mensajes para la recuperación por un cliente de correo electrónico MUA.

[4] SMTP: Simple Mail Transfer Protocol, Protocolo o conjunto de reglas de comunicación para enviar o recibir correos, usa el puerto 25 del servidor para comunicarse.

MUA (Mail user Agent, Agente de usuario de correo): Software que permite a los usuarios leer y redactar mensajes de correo, es decir es un cliente de correo electrónico, Ejemplo Zimbra, Gmail, Yahoo, etc.

MSA (Mail Submission Agent, Agente de recepción de correo): Software que se ejecuta en un servidor SMTP, recibe mensajes de un MUA, comprueba errores y lo remite a un MTA.

Protocolos de correo

Dentro de los protocolos más importantes podemos destacar los siguientes:

SMTP (Simple Mail Transfer Protocol, Protocolo simple de transferencia de correo): Protocolo o conjunto de reglas de comunicación para enviar o recibir correos, usa el puerto 25 del servidor para comunicarse.

POP (Post Office Protocol, Protocolo de oficina de correo): Se encarga de establecer una conexión entre un cliente y un servidor de correo electrónico, permite gestionar el envío de mensajes.

IMAP (Internet Message Acces Protocol, Protocolo de acceso a mensajes de internet): Permite acceder a los mensajes almacenados en un determinado servidor de correo, no permite enviar correos, únicamente permite el acceso a los mensajes almacenados.

Amenazas de seguridad al correo electrónico

Ningún servicio de correo electrónico es seguro, ya sea que estén expuestos al mundo a través del internet, o dentro de una organización por medio de una intranet, siempre estarán vulnerables a sufrir ciberataques o auto ataques dentro de la institución, que pretendan atentar contra la privacidad e integridad de la información disponible. A continuación, se describen algunas amenazas de seguridad informática que puedan afectar a la seguridad de la información a través del servidor de correo electrónico.

Malware: Programa o archivo malicioso que puede afectar la funcionabilidad de un dispositivo o causar daño a la data con su permiso, es muy peligroso para la seguridad del servidor de correo electrónico porque en sus paquetes insertados puede incluir virus, troyanos, gusanos y

spyware. Los ciberdelincuentes generalmente usan el correo electrónico para garantizar que llegue al objetivo, sin que sus víctimas sepan el origen del ataque y las consecuencias que puede alcanzar este tipo de ataque (Kaspersky, s.f.).

Spam: Correo no deseado o basura, el cual es enviado de forma masiva por un remitente desconocido, el cual puede ser en formato texto o con contenido HTML (ESET, 2020)

Pishing: Ataque realizado utilizando ingeniería social, con el objetivo de adquirir fraudulentamente información personal y/o confidencial de la víctima, como contraseñas o detalles de su tarjeta de crédito, cuentas de redes sociales, corporativas o de juegos en línea.

Ingeniería social: Conjunto de técnicas utilizadas para engañar a la víctima a través de una acción o conducta social (Eset, 2022).

Ransomware: Código malicioso usado para extorsionar a sus víctimas (Eset, 2022).

Spoofing: Conjunto de técnicas que permiten la falsificación de alguna característica de las partes intervinientes en una comunicación informática (Eset, 2022).

Análisis de vulnerabilidades

Hoy en día basta regresar a ver a nuestro alrededor, para ver que todos o casi todos tenemos un dispositivo como celular, ordenador, tablet, etc. y todas esas personas, utilizamos a diario redes sociales, correo, aplicaciones bancarias, aplicaciones de comunicación. Y justamente de toda esa información que los usuarios proporcionan es que nace las ciberamenazas, principalmente para el robo de información personal o empresarial.

Para tener un adecuado sistema de prevención y respuesta frente a estos ciberataques, es importante el análisis de vulnerabilidades. Existe dos métodos de escaneo (Ciberseguridad, 2019) para realizar un análisis de vulnerabilidades

- Caja blanca: Tiene una visión total de la red a analizar, así como, acceso a todos los equipos como súper usuario.
- Caja negra: Aquí se va a proporcionar a los analistas sólo información de acceso a red o al sistema, por ejemplo, una sola dirección IP, algún nombre de alguna empresa, etc. A

partir de aquí empieza como tal a buscar toda la información posible de dicha dirección IP y del resto de los equipos que se encuentran dentro de algún rango de direcciones IP asociado, solamente se detecta y se documenta la vulnerabilidad.

Actualmente, existe un raudo crecimiento de ataques y vulneraciones informáticas a la infraestructura tecnológica de las instituciones públicas y privadas, mismas que en su mayoría son afectadas en sus diferentes sistemas operativos, servidores, aplicativos, dispositivos, etc., evidenciando la exposición a la que se enfrentan a diario estas instituciones.

Según CVE Details (2022), podemos observar en la figura 4, las vulnerabilidades detectadas a nivel mundial desde el año 1999 hasta el 2021, que nos permite observar cómo cada vez van aumentando.

Figura 4

Vulnerabilidades por año desde el 1999 al 2021 (Cvedetails, 2022).

Nota. La figura muestra las vulnerabilidades totales reportadas por año. Tomado de Cvedetails (2022).

Test de intrusión

Consiste en realizar varios tipos de pruebas, aprovechando las vulnerabilidades encontradas y de esta manera comprometer los sistemas de la organización. Este tipo de auditorías de seguridad es más invasivo que el análisis de vulnerabilidades y puede ser dirigido a un solo objetivo.

Hacking ético

Intervenir en los sistemas electrónicos, así como también en los datos que contienen que pertenecen a una persona en específico, realizar un peritaje y servicio de seguridad de forma legal en una empresa (Vizueta, 2011).

Tipos de ataques en la seguridad

Dentro del proceso de comunicación existen dos tipos de ataques a la red de transmisión de datos, los cuales se los describe a continuación:

Ataques pasivos

Son aquellos que monitorean las transmisiones, el objetivo para realizar este tipo de ataque es para obtener información que se está transmitiendo, en este tipo de ataque se puede encontrar:

- Divulgación del contenido de un mensaje, el cual es un ataque en el cual el atacante se entera de la información transmitida al escuchar una llamada telefónica o leer un correo electrónico abierto.
- Análisis de tráfico, se realiza cuando el atacante puede determinar la localización e identidad de quienes se están comunicando y determinar el mensaje que está siendo transmitido aun cuando esté protegido por medio de cifrado (González, 2012, P.4).

Ataques activos

Suponen modificaciones de los datos o creación de flujos de datos falsos. Dentro de este tipo de ataques se puede encontrar:

- Enmascaramiento, tiene lugar cuando una entidad pretende suplantar a otra para obtener información confidencial
- Repetición, se realiza con la captura de unidades de datos que se vuelven a retransmitir para producir efectos no autorizados.
- Modificación de mensajes, se modifican los mensajes para producir efectos no autorizados en las víctimas.

- Denegación de servicios (DoS), previene o inhabilita el uso normal de las facilidades de comunicación, usualmente se hace para obtener un fin específico o para obtener perturbaciones sobre la red, desmejorando su rendimiento o incluso inhabilitando la misma (González, 2012, P.5).

Definición de Políticas De Seguridad

Para proteger un sistema, se debe realizar un análisis de las amenazas potenciales que este puede sufrir, las pérdidas que podrían generar y la probabilidad de su ocurrencia. Este estudio genera las políticas de seguridad que definen las responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se realicen. (Cifuentes, 2004, P.20).

Sistema de Gestión de Seguridad de la Información (SGSI)

Un sistema de Gestión de Seguridad de la Información, es un conjunto de políticas y procedimientos que se definen y ponen en práctica en cualquier organización pública o privada, con el fin de proteger su información, ya sea que afecte a la resiliencia de la organización, así como la información confidencial (INNEVO, 2022).

Norma IEC/ISO 27001 Seguridad de la información

Las normas ISO, son estándares de seguridad establecidas por la Organización Internacional de Estandarización (ISO) y la Comisión Electrónica Internacional (IEC), que se encargan de establecer estándares y guías relacionadas con sistemas de gestión y aplicables a cualquier tipo de organización internacional, con el fin de facilitar el intercambio de información y contribuir a la transferencia tecnológica.

Según la ISO/IEC 27001, referente a la seguridad de la información, tiene como base preservar la confidencialidad, integridad y disponibilidad de la información, así como la de los sistemas que se aplican para su tratamiento (MENTOR, s.f.).

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados

Integridad: mantener a la información completa y exacta cuando la requieran

Disponibilidad: que se garantice todo el tiempo el acceso y utilización de la información, y los sistemas de tratamiento por parte de individuos o procesos cuando lo requieran.

Mecanismos de seguridad

Los mecanismos de seguridad para implementar estas políticas, se utilizan lo que se conoce como mecanismos de seguridad. Los mecanismos de seguridad se dividen en tres grupos:

- Prevención: Aquellos que aumentan la seguridad de un sistema durante su funcionamiento normal.
- Detección: Aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.
- Recuperación: Aquellos que se aplican cuando el sistema ha sido atacado. (Cifuentes, 2004, P.21)

Elementos de seguridad

Los elementos de seguridad más importantes que se puede destacar en orden de jerarquía desde el más bajo se muestran a continuación:

- Política de Seguridad Corporativa
- Autenticación del Usuario
- Encriptación y Control de Acceso
- Auditoria y Administración

Responsabilidad

La empresa asigna responsabilidad a todo su personal, los Administradores implementan y hacen cumplir las políticas de seguridad y auditan la actividad de los usuarios, procurando señalar los problemas de seguridad, los cuales pueden incluir actividad ilícita de un empleado, un sistema con un nivel bajo de parches o un intruso fuera de la red. La

administración y los administradores seguridad deben de crear las políticas de seguridad corporativa porque esto provee los fundamentos para todas las actividades de la red.

La política de seguridad

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que la misma debe establecer un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

Elementos de una política de seguridad informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante. Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso. (Perpinan, 2011, P.29).

Parámetros para establecer políticas de seguridad

Es importante que, al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas. (Perpinan, 2011, P.30).

Ciberseguridad.

Podemos decir que la Ciberseguridad es la práctica para proteger la parte de hardware y la parte del software de posibles amenazas que alteren su correcto funcionamiento.

Ciberdefensa

La ciberdefensa son acciones y medidas que en conjunto logran garantizar la seguridad en el ciberespacio y evita las amenazas.

Podemos decir que tanto Ciberdefensa como Ciberseguridad lo que hacen es prevenir los ataques de posibles amenazas, de hecho, las dos deben trabajar coordinadamente, pero con la gran diferencia que la Ciberdefensa da respuesta a los ciberataques para dar más seguridad a la infraestructura digital.

Ciberataque

Son intentos de robar, alterar, dañar información mediante un acceso no autorizado a un sistema informático.

Ciberterrorismo

El FBI define de la siguiente manera “El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos”.

Ciberdelito

“Se refiere a cualquier actividad ilegal llevada a cabo mediante el uso de tecnología”. (AVAST, 2022)

Delimitación del estudio

El tema planteado es a nivel nacional y el área de influencia es la infraestructura crítica digital de la Fuerza Terrestre, con énfasis en el servidor de correo electrónico institucional.

Pregunta de investigación

Pregunta principal de investigación

¿Cuáles son los controles de seguridad informática que deben implementarse para gestionar los incidentes informáticos ante una posible brecha de seguridad en el servidor de correo electrónico institucional y el impacto que pueda generar en la infraestructura critica digital de la FT en los siguientes cinco años?

Preguntas secundarias de investigación

- ¿El personal técnico responsable de la administración y mantenimiento a la infraestructura crítica digital de la FT, tiene la suficiente expertís en análisis y gestión de vulnerabilidades?
- ¿Existen políticas y protocolos de seguridad de la información implementadas en el servidor de correo electrónico institucional?
- ¿Las herramientas informáticas que dispone la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC FT), para la gestión de

incidentes de seguridad, están en capacidad de alertar ante la presencia de vulnerabilidades?

Variables de la Investigación

Variable Independiente

Norma ISO 27001 Seguridad de la información.

Variable Dependiente

Infraestructura digital de la Fuerza Terrestre, servidor de correo electrónico institucional.

Tabla 1

Operacionalización de variables

Dimensión (Del tema)	**Conceptualización (Marco teórico, revisión previa de papers, libros y tesis)**	**Subdimensiones (De la teoría o del modelo a aplicar)**	**Indicadores (Para cada dimensión o subdimensión)**	**Pregunta de investigación (Proviene del planteamiento del problema)**	**FUENTES (De donde obtendré información primaria y secundaria)**	**INSTRUMENTO (Como levanto la información primaria)**
Variable independiente: Norma ISO 27001 Seguridad de la información	Las normas ISO, son estándares de seguridad establecidas por la Organización Internacional de Estandarización (ISO) y la Comisión Electrónica Internacional (IEC), que se encargan de establecer estándares y guías relacionadas con sistemas de gestión y aplicables a cualquier tipo de organización internacional, con el fin de facilitar el intercambio de información y contribuir a la transferencia tecnológica (INNEVO, 2022).	Física Lógica	Inspecciones programadas y no programadas a través de la Inspectoría de la FT y el Dpto de Seguridad de la Información Digital de la FT. Ethical hacking, a través de herramientas open source y licenciadas.	¿Se cumple con las políticas, directivas, instructivos, etc. referente a la Seguridad Informática en la Fuerza Terrestre?	La información se obtendrá de revistas indexadas, de trabajos de investigación, de páginas web, investigación en campo y documentos digitales.	Encuesta, entrevista, observación, grupos focales
Variable dependiente: Brecha de seguridad en el servidor de correo electrónico institucional	Según (Saroka & Voutssas, 2002), la vulnerabilidad es la debilidad que presenta cualquier recurso o sistema informático, susceptible de ser explotada por una amenaza. En otras palabras, implica una falta de protección ante las amenazas, que pueden generar un efecto nocivo al fallar la seguridad.	Lógica Física (Infraestructura tecnológica) Talento Humano	Herramientas informáticas que dispone la DTIC FT, para la gestión de incidentes de seguridad. Personal técnico que administra y da mantenimiento a la infraestructura crítica digital de la FT. Políticas y protocolos de seguridad de la información implementadas en el servidor de correo electrónico institucional	¿Existen vulnerabilidades o brechas, tanto físicas como lógicas en la infraestructura crítica digital de la Fuerza Terrestre?	La información se obtendrá de revistas indexadas, de trabajos de investigación, de páginas web, documentos digitales, centro de datos de la FT.	Encuesta, entrevista, observación, grupos focales

Nota. Esta tabla muestra la operacionalización de las variables

Capítulo III:

Metodología

Diseño de la investigación

“Los diseños de la investigación son el plan, la estructura y las estrategias que se utilizarán para obtener respuestas a las preguntas de investigación e hipótesis controlando la varianza experimental, extraña y de error” (Reidi Martínez, 2012). Los diseños implican partir de un marco de referencia, señalar como se obtendrán los datos (serán medidos, observados o se consultarán registros existentes). El diseño también señala cuántos y cuáles registros u observaciones se realizarán, cómo se analizará la información obtenida (de manera cualitativa o cuantitativa) (Reidi Martínez, 2012, pág. 37). En este contexto el presente proyecto de investigación, se inclinará por el diseño de investigación cuantitativa ya que “Se entiende que la investigación cuantitativa parte de datos evidenciables” (Del Canto & Silva, 2013).

Entonces la versión cuantitativa tiene como principio la suposición de un criterio lógico, en la que establece un apretado conjunto de relaciones reguladas entre premisas y conclusiones, de modo que para pasar de las primeras a las segundas no habrá más que seguir sus estipulaciones. (Del Canto & Silva, 2013).

El enfoque para la presente investigación científica, es la cuantitativa, empleando varios procesos como el deductivo, que va de lo general a lo particular. Se caracteriza por la recolección de datos para comprobar hipótesis, respaldada por la comprobación numérica y análisis estadístico, este enfoque se describe por ser secuencial y probatorio, esta parte con la idea, identificación, formulación y delimitación del problema, derivando las preguntas de investigación y objetivos de la misma, complementando una revisión de la literatura para el marco teórico, se define su alcance determinación de la hipótesis y variables, diseñamos la investigación, para posterior realizar la recolección, mediciones, análisis e interpretación de datos estadísticos y finalmente elaborar el reporte de los resultados, para la comprobación de las hipótesis planteada (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010)

Tipo de investigación

“Los tipos de investigación que existen son: Histórica, descriptiva, experimental, exploratoria, correlacional, explicativa, comparativa y otros” (Carrillo Punina, 2022). Otros autores como por ejemplo Diaz-Narváez (2016) manifiestan que: “En general, no existe acuerdo en la clasificación de las distintas formas de investigación y, la que asume por los diferentes autores, depende del paradigma epistemológico que sustentan. No obstante, algunos metodólogos parecen coincidir en que los tipos de investigación pueden ser clasificados como exploratorios, descriptivos, correlacionales y explicativos” (p.4)

Bajo este concepto se va a realizar una investigación explicativa ya que según Carrillo Punina (2022), “Esta investigación pretende conducir a un sentido de compresión o entendimiento de un fenómeno. Apuntan a las causas de eventos físicos o sociales. Pretenden responder a peguntas como: ¿Por qué ocurre? ¿En qué condiciones ocurre? Son más estructurados y en la mayoría de los casos requieren del control y manipulación de las variables en un mayor o menor grado” (p.68)

La presente investigación aplica la investigación descriptiva ya que se fundamenta en la medición de variables o conceptos, con el fin de especificar las propiedades importantes del fenómeno. Según los actores (Abalde Paz & Muñoz-Cantero, 1992), el método descriptivo es uno de los métodos más utilizados en la investigación, para estudiar cualquier tipo de fenómeno desconocido, observar en su ambiente natural y, a continuación, describirlo lo más detalladamente posible. Underwood & Saughnessy (como se citó en Abalde Paz & Muñoz-Cantero, 1992) plantea que los métodos descriptivos pueden desempeñar cuatro funciones:

- Ayudar a identificar fenómenos importantes
- Sugerir posibles conductas que más tarde pueden ser estudiadas por medio de experimentos adecuados.
- Utilizarse como instrumento de estudio como no pueden ser utilizados.

Población y muestra

Población

Para definir a la población hay que iniciar desde el uso popular, en la cual se puede decir que es la cantidad de personas en un momento y lugar determinado, siendo el mismo principio en la aplicación de la población en la estadística, en la que se utiliza para los integrantes de cualquier muestra. Para considerar la población en el presente trabajo, (Carrillo Punina, 2022) describe como “Una población o universo es el conjunto de todos los casos que concuerdan con una serie de especificaciones”. Para realizar el presente trabajo de investigación se considera una población netamente con conocimiento técnico perteneciente al área de las TIC, con especial atención a la seguridad informática pertenecientes a las unidades militares de la Fuerza Terrestre del Ecuador.

Las unidades de análisis previstas para esta investigación corresponden al Centro de Datos administrado por la Dirección de Tecnologías de la Información y Comunicaciones y las unidades militares de Comunicaciones de la Fuerza Terrestre, el cual esta descrita en la delimitación espacial y como población se considera al personal técnico militar y servidores públicos que laboran en estas dependencias, y que tienen perfiles con diferente privilegios de acceso a la administración de su infraestructura crítica digital.

Muestra

Dadas las características de la investigación, se consideró a una población militar específica, con competencias y responsabilidades en la gestión y administración de la seguridad informática de las unidades militares de la Fuerza Terrestre, (Carrillo Punina, 2022) manifiesta que: “La muestra es un subgrupo de la población de interés sobre el cual se recolectarán datos”. Para realizar el cálculo de la muestra, entre otras, se ha considerado pertinente aplicar la siguiente fórmula:

$$\mathrm{n} = \frac{Z^2 \mathrm{Npq}}{e^2(N-1) + Z^2 pq}$$

Dónde:

N= Tamaño del universo

Z= Nivel de confianza

p= Probabilidad de éxito

q= Probabilidad de fracaso

e= error de estimación

En nuestro proceso de investigación, se ha determinado la muestra cómo se detalla a continuación:

Tabla 2

Conformación de la muestra

UNIDAD MILITAR	CANTIDAD
Personal de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre.	10
Comandantes de las compañías de Comunicaciones de la Fuerza Terrestre.	10
Personal del Cuarto de Control de la Comandancia General, perteneciente al Batallón de Comunicaciones Nro. 1 Rumiñahui.	8
TOTAL	28

Nota. En esta tabla se muestra la conformación de la muestra y es de elaboración propia

Luego de aplicar la fórmula para extraer el tamaño de la muestra, el resultado es de 21,16 lo que equivale a que se debe aplicar a 21 del universo de 28 encuestas.

Técnica e instrumentos de investigación

En 1950 Dalkey desarrolla la técnica Delphi que nos permite conocer la opinión de un grupo de personas en relación a un problema, sin que los integrantes se reúnan físicamente. Es por ello que para la presente investigación hemos escogido esta técnica por dos motivos: el

primero porque físicamente no pueden estar todos a los que se va a encuestar, segundo porque permite tratar de un problema detectado por un grupo de expertos en el tema.

Instrumentos

El autor (Tesis y Masters, 2023) plantea que los tipos de instrumentos que se utiliza para la recolección de datos son:

- Entrevista. – Se trata de una herramienta que permite acceder a testimonios reales de personas que tienen algún valor para la investigación. Principalmente, es un instrumento utilizado en estudios de tipo cualitativo, y un punto a destacar, es la facilidad que ofrece para adaptarse a las necesidades del investigador.
- Cuestionario. – Es un recurso estratégico para obtener datos estandarizados y generalizados sobre un tema específico, el cuestionario brinda datos cuantitativos.
- Observación. – Consiste esencialmente en observar al fenómeno o persona de interés, es clave que se practique en un ambiente natural donde el desarrollo normal del fenómeno no este condicionado por el investigador, la observación puede ser individual, grupal, e incluso de comunidades completas, dependiendo del tipo de investigación.
- Grupos focales. – Se trata de un método cualitativo de recolección de datos, que consiste en realizar una entrevista en grupo, dirigida por un moderador neutral. Con esto pretende obtener información sobre un limitado número de preguntas predefinidas, para garantizar la validez y el carácter científico, es importante que su realización atienda a ciertas normas metodológicas, un punto a destacar es que permite explorar y estimular distintos puntos de vista.
- Comunidades en línea. – Se configuran como un espacio de estudio en sí, esto se debe a que en un mismo lugar puedes llevar adelante tanto encuestas o sondeos, como grupos focales, tener un tablero de generación de ideas, premiar a los participantes por su retroalimentación. Estudiar estas comunidades implica

posicionarse en un paradigma esencialmente cualitativo, que aborda desde el análisis de contenido de las discusiones virtuales hasta la etnografía o etnografía aplicada a internet.

Para obtener resultados que permitan desarrollar la presente investigación. Se ha considerado como muestra a técnicos especialistas a través de una encuesta en línea a través de internet. La encuesta aplicada permitirá identificar los servicios críticos, identificar si se implementan políticas de seguridad, verificar incidentes de seguridad los cuales se dan con más frecuencia en la infraestructura digital de la Fuera Terrestre.

Validez y confiabilidad

"La confiabilidad y validez son constructos inherentes a la investigación desde la perspectiva positivista para otorgarle a los instrumentos y a la información recabada, exactitud y consistencia necesarias para efectuar las generalizaciones de los hallazgos, derivada del análisis de las variables de estudio" (Hidalgo, 2006).

Hidalgo (como se citó en Patton, 1982 p. 39), plantea que estos procesos han sido considerados con otra connotación en la investigación cualitativa, la cual trata de comprender los fenómenos de la realidad en un contexto específico tal y como es, en un "marco del mundo real donde el investigador no intenta manipular el fenómeno de interés". Así todo investigador ya sea cualitativo como cuantitativo debe considerar estos dos constructos al realizar investigaciones, analizar resultados y evaluar su calidad (Hidalgo, 2006)

En base a este argumento, se puede manifestar que es muy importante la validez y confiabilidad, ya que se puede dar fe que los datos obtenidos son de muy buena fuente, con lo cual aportaran satisfactoriamente en el desarrollo de la presente investigación.

Técnicas de análisis de datos

Se aplicará la técnica de la correlación en la interpretación de los datos, aprovechando también las bondades del programa informático Microsoft Excel, en la aplicación de

estadísticas descriptivas, elaboración de tablas y elaboración de diagramas estadísticos que puedan ser utilizados para comprender y visualizar el comportamiento de las variables.

Técnica de investigación y comprobación de hipótesis

Fuentes de información

Primaria (levanta el investigador artículo científico), secundaria.

Instrumentos de Investigación

Para desarrollar la presente investigación se ha considerado como instrumento de investigación a la encuesta, la cual fue aplicada vía online al personal técnico de las unidades de la DTIC FT.

Procesamiento de la información

Herramientas informáticas de análisis estadístico, Excel, spss, Atlas pi, herramientas estadísticas, medidas de dependencia central, de correlación Pirson, mac.

Para el análisis, procesamiento de interpretación de los datos de la presente investigación se utilizará el aplicativo de Microsoft Forms para la generación de las encuestas en línea, el cual permite generar matrices en Excel y nos permite obtener los resultados estadísticos de los datos muestreados.

El procesamiento de datos se refiere a todo el proceso que sigue un investigador desde la recolección de datos, hasta la presentación de los mismos en forma resumida. Tiene básicamente tres etapas: recolección y entrada, procesamiento y presentación. El procesamiento de datos por medio de programas informáticos, representan una ventaja en tiempo, dinero y espacio ya que arrojan resultados inmediatos. En este proceso cuenta, sobre todo, la habilidad del ser humano para capturar los datos y procesarlos de acuerdo algún parámetro estadístico.

Paquete software

Los datos obtenidos de la presente investigación se procesan con el paquete informático de Microsoft Excel, con el que se organizarán y se generará gráficos para la interpretación y análisis de datos de la encuesta realizada.

Herramientas estadísticas

De la misma manera los paquetes informáticos que se ha utilizado para el análisis de los datos organizados es el Microsoft Excel, en lo referente al análisis estadístico.

Capítulo IV:

Propuesta

Análisis de los resultados

Fuentes de información

Primaria (levanta el investigador artículo científico).

Instrumentos de investigación

Para desarrollar la presente investigación se ha considerado como instrumento de investigación a la encuesta, la cual fue aplicada vía online al personal técnico que trabaja en la DTIC FT.

Procesamiento y análisis

Herramientas informáticas de análisis estadístico, Excel, spss, Atlas pi. Herramientas estadísticas, medidas de dependencia central, de correlación Pirson, mac

Para el análisis, procesamiento e interpretación de los datos de la presente investigación se utiliza el aplicativo de Microsoft Forms para la generación de las encuestas en línea, el cual permite generar matrices en Excel y nos permite obtener los resultados estadísticos de los datos muestreados.

Discusión de resultados

Análisis de resultados

Para el desarrollo de la presente investigación se aplicó una encuesta en línea al personal técnico de comunicaciones e informática, que tiene a su cargo el área de TIC´s de las unidades militares de la Fuerza Terrestre. Las preguntas objeto de esta encuesta se detallan a continuación con los respectivos resultados e interpretación.

¿Dispone de un equipo informático entregado por la Organización para realizar su trabajo?

Tabla 3

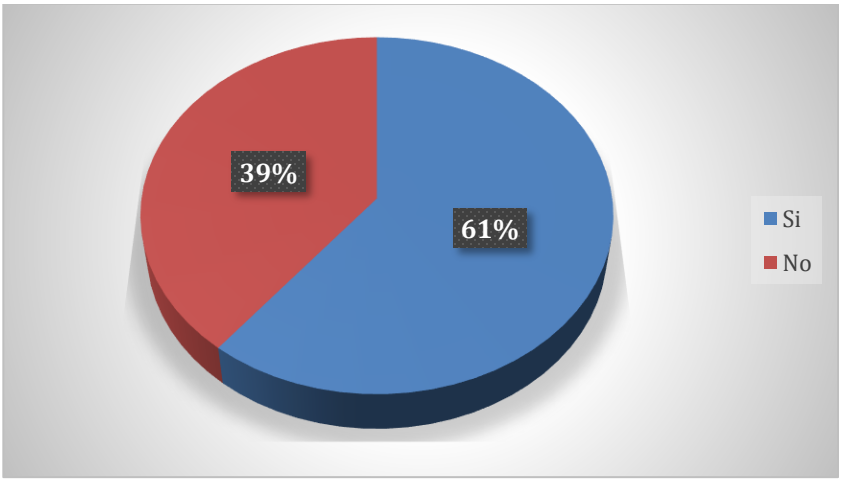
Dispone de equipo informático institucional

Opciones	f	%
Si	17	61
No	11	39
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 1

Figura 5

Dispone de equipo informático institucional



Nota. La figura muestra el desarrollo de la primera pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que 17 personas (61%) colocaron que Si disponen equipo informático entregado por la institución y 11 personas (39%) indicaron que NO. El autor (ÁTICO34, 2022), en su blog determina los tipos de vulnerabilidades informáticas en ciberseguridad; en la cual las agrupa de acuerdo al diseño, implementación uso y vulnerabilidades de día cero. De acuerdo al diseño, destaca a las Políticas de Seguridad deficientes e inexistentes. De este análisis al existir políticas deficientes o inexistentes para el uso de equipos informáticos de uso personal en el trabajo, esta omisión o incumplimiento es considerado como una amenaza para la institución, conforme el listado de amenazas y

vulnerabilidades en ISO 27001 (EXCELENCIA, 2019), al comprometer información confidencial de la institución.

¿Qué cuenta de correo electrónico utiliza más para enviar o recibir información de su trabajo?

Tabla 4

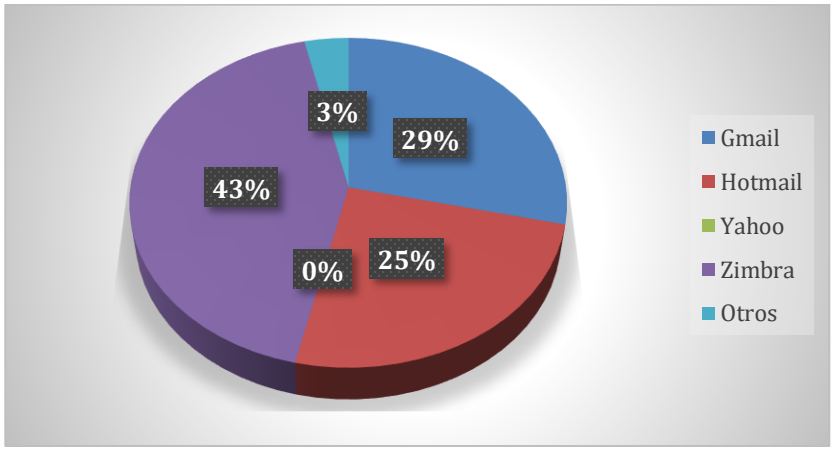
Cuenta de correo electrónico que más utiliza en el trabajo

Opciones	f	%
Gmail	8	29
Hotmail	7	25
Yahoo!	0	0
Zimbra	12	43
Otros	1	4
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 2

Figura 6

Cuenta de correo electrónico que más utiliza en el trabajo



Nota. La figura muestra el desarrollo de la segunda pregunta de la encuesta realizada

De las respuestas obtenidas en la pregunta, se tiene que un 43% de las personas utilizan la cuenta de correo institucional Zimbra en su trabajo, así también hay que considerar que un 25% utilizan Hotmail y 29% Gmail que son plataformas comerciales, las cuales, al no

existir políticas para el uso exclusivo de correo electrónico institucional para la gestión documental, podrían ser consideradas como potenciales vulneraciones a la seguridad, ya que al no tener el control de estas cuentas de correo, se pudiera hacer mal uso de la información, o posiblemente exista fuga de la misma, sin que quede registro.

¿Dispone de una cuenta (usuario y contraseña) en el Sistema De Gestión Documental "Chasqui"?

Tabla 5

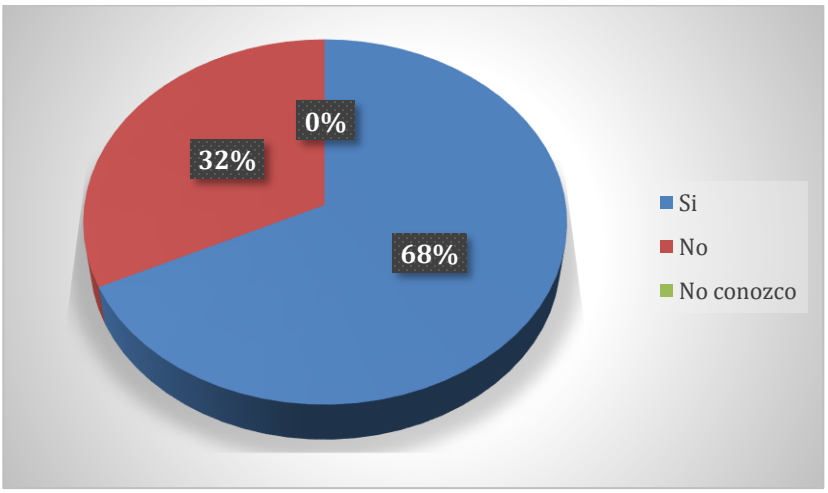
Dispone de una cuenta en el Chasqui

Opciones	f	%
Si	19	68
No	9	32
No conozco	0	0
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 3

Figura 7

Dispone una cuenta en el Chasqui



Nota. La figura muestra el desarrollo de la tercera pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que un 68% de las personas si disponen de un usuario y contraseña en el Sistema de Gestión Documental "Chasqui", sin

embargo, hay un alto porcentaje (32%) que no dispone de una cuenta, lo que pude influir en la evasión de responsabilidad que pueden asumir los funcionarios que no la tienen.

¿Qué versión de Windows está instalada en la computadora del trabajo que normalmente usa para conectarse a Internet?

Tabla 6

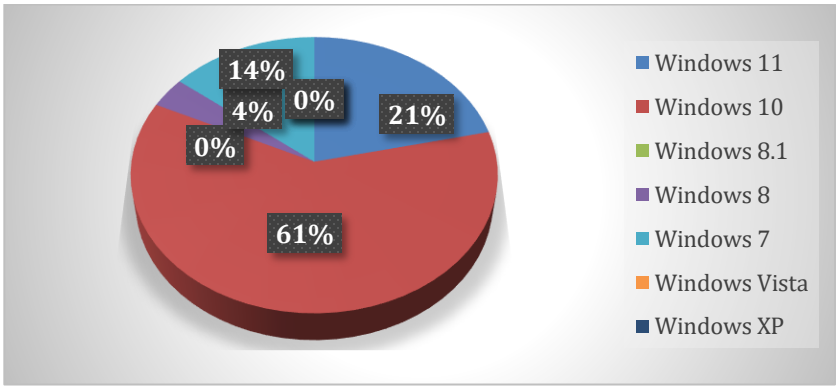
Versión de Windows instalada en su equipo informático

Opciones	f	%
Windows 11	6	68
Windows 10	17	32
Windows 8.1	0	0
Windows 8	1	0
Windows 7	4	0
Windows Vista	0	0
Windows XP	0	0
Otro	0	0
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 4

Figura 8

Versión de Windows instalada en su equipo informático



Nota. La figura muestra el desarrollo de la cuarta pregunta de la encuesta realizada

De las respuestas obtenidas en la pregunta, se tiene que un 61% de las personas utilizan Windows 10, garantizado actualizaciones y parches por parte de Microsoft para este

Sistema Operativo, sin embargo, hay un alto porcentaje (21%) que tiene instalado Windows 7, el cual no tiene actualizaciones disponibles al haber cumplido su vida útil, no tiene soporte ni actualizaciones; por lo cual se recomienda migrar a Windows 10 (ESET, 2020) para reducir la vulnerabilidad de esos equipos.

¿Tiene instalado un software antivirus en su computadora del trabajo?

Tabla 7

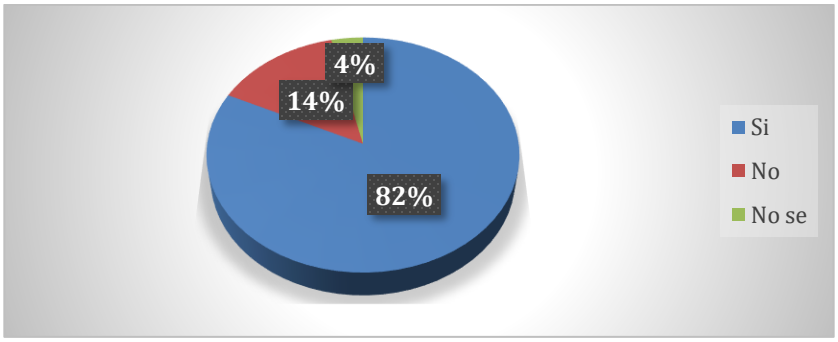
Tiene instalado antivirus en su equipo informático

Opciones	f	%
Si	23	82
No	4	14
No se	1	1
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 5

Figura 9

Tiene instalado antivirus en su equipo informático



Nota. La figura muestra el desarrollo de la quinta pregunta de la encuesta realizada

De las respuestas obtenidas en la pregunta, se tiene que un 82% de las personas utilizan un antivirus en su equipo informático, fortaleciendo la seguridad en esos equipos, sin embargo, hay un porcentaje (14%) que no dispone de antivirus, lo cual incrementa la vulnerabilidad de esos equipos al quedar desprotegidos ante el accionar de ciberdelincuentes.

¿El software antivirus instalado en su equipo de trabajo, es licenciado o es una versión gratuita?

Tabla 8

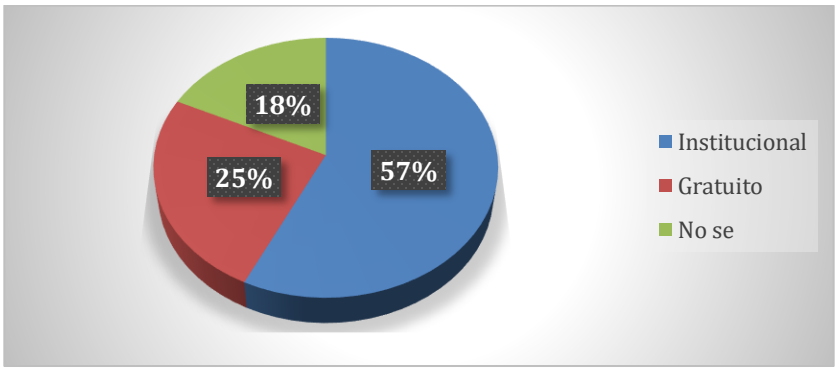
Antivirus licenciado o gratuito

Opciones	f	%
Institucional	16	57
Gratuito	7	25
No se	5	18
Total	**28**	**100**

Nota: Esta tabla muestra la pregunta 6

Figura 10

Antivirus licenciado o gratuito



Nota. La figura muestra el desarrollo de la sexta pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que apenas un 57% de las personas utilizan un antivirus institucional en su equipo informático, sin embargo, es preocupante que un 25% usen una versión gratuita descargado de internet y un 18% no sepan que función cumple un antivirus en sus equipos, lo cual incrementa la vulnerabilidad.

¿Con qué frecuencia realiza un análisis antivirus completo del sistema?

Tabla 9

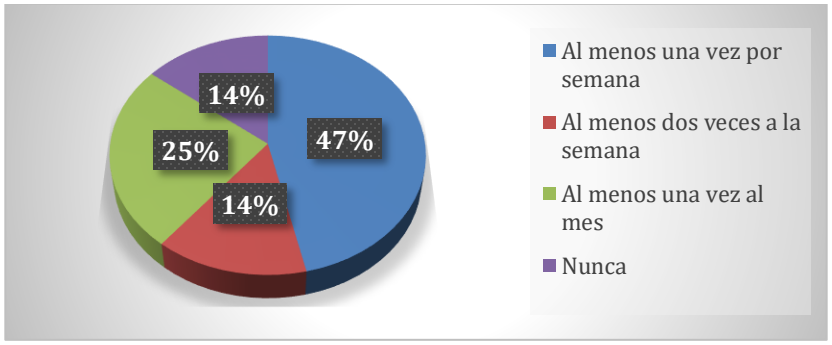
Frecuencia de análisis de Antivirus

Opciones	f	%
Al menos una vez por semana	13	46
Al menos dos veces a la semana	4	14
Al menos una vez al mes	7	25
Nunca	4	14
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 7

Figura 11

Frecuencia de análisis de Antivirus



Nota. La figura muestra el desarrollo de la séptima pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que un 47% al menos una vez por semana utilizan antivirus en sus equipos, así también un 25% al menos una vez al mes, sin embargo, es preocupante que un 14% nunca lo usen, lo cual al no utilizar un antivirus los equipos se exponen a posibles ataques de virus o malware, que pueden ser aprovechados por ciberdelincuentes que podrían fácilmente explotar esta vulnerabilidad.

¿Utiliza un software de firewall [5]en su computadora?

Tabla 10

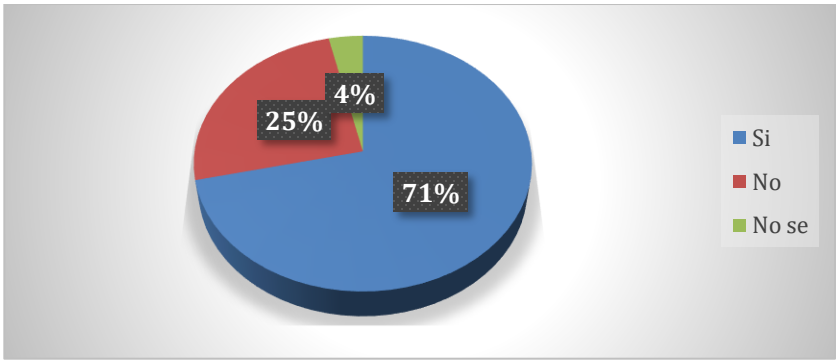
Utilizan firewall en sus equipos informáticos

Opciones	f	%
Si	20	71
No	7	25
No se	1	4
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 8

Figura 12

Utilizan firewall en sus equipos informáticos



Nota. La figura muestra el desarrollo de la octava pregunta de la encuesta realizada

De las respuestas obtenidas en la pregunta, se tiene que un 71% de las personas utilizan un software firewall en su equipo informático, sin embargo, es preocupante que un 25% no usen el firewall, al no utilizarlo, los equipos pueden ser más vulnerables a recibir ataques de virus, malware, hackers, o programas no autorizados.

[5] Firewall: Dispositivo de seguridad que monitorea el tráfico de red entrante y saliente, decide si permite o bloquea el tráfico específico en función de las políticas establecidas. (CISCO)

¿Conoce usted, que es un incidente de seguridad o ciberseguridad informática?

Tabla 11

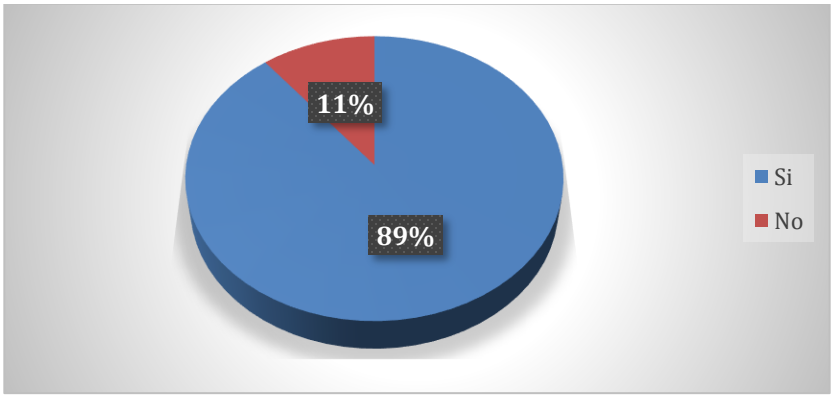
Conoce que es un incidente de seguridad

Opciones	f	%
Si	25	89
No	3	11
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 9

Figura 13

Conoce que es un incidente de seguridad



Nota. La figura muestra el desarrollo de la novena pregunta de la encuesta realizada

De las respuestas obtenidas en la pregunta, se tiene un 89% de las personas conocen que es un incidente de seguridad o ciberseguridad informática, sin embargo, es preocupante que un 11% no lo conozca, lo cual puede ser un factor negativo al momento de ser resiliente ante un ciberataque.

¿En su organización (Unidad/Dirección), cuenta con personal capacitado en seguridad o ciberseguridad informática?

Tabla 12

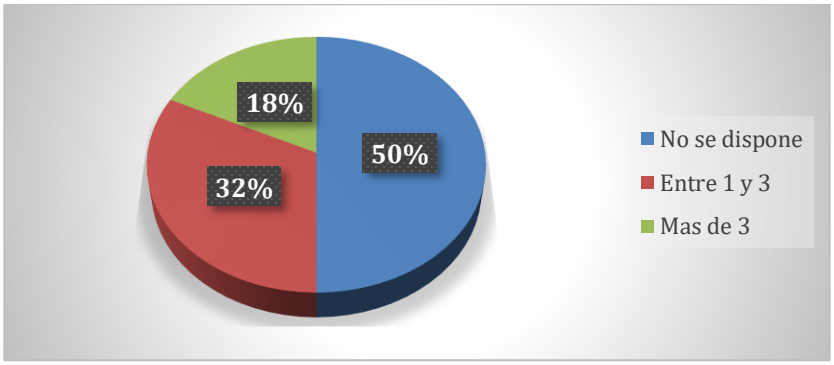
Dispone personal capacitado en ciberseguridad

Opciones	f	%
No se dispone	14	50
Entre 1 y 3	9	32
Más de 3	5	18
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 10

Figura 14

Dispone personal capacitado en ciberseguridad



Nota. La figura muestra el desarrollo de la décima pregunta de la encuesta realizada

De las respuestas obtenidas en la pregunta, se tiene que un 50% de las personas no disponen de personal capacitado en ciberseguridad, es preocupante que no exista personal capacitado, lo cual puede incrementar el riesgo de amenazas y vulnerabilidades, afectando a la integridad, confidencialidad y disponibilidad de la información de la institución. Además, al no disponer de este personal, puede causar dificultades para hacer detección, prevención y respuesta ante incidentes de seguridad, así como el cumplimiento de las políticas, normativas y regulaciones vigentes.

¿En su organización (Unidad/Dirección), cuántos incidentes de seguridad o ciberseguridad informática ha tenido en el último año?

Tabla 13

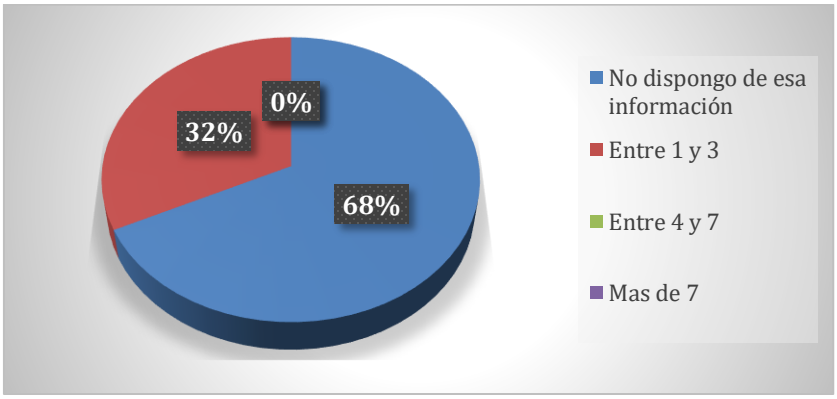
Incidentes de ciberseguridad en sus unidades

Opciones	f	%
No dispongo de esa información	19	68
Entre 1 y 3	9	32
Entre 4 y 7	0	0
Más de 7	0	0
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 11

Figura 15

Incidentes de ciberseguridad en sus unidades



Nota. La figura muestra el desarrollo de la décima primera pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que un 68% de las personas no disponen de información ni herramientas informáticas, que permitan detectar incidentes de ciberseguridad, apenas un 32% entre 1 y 3 incidentes se han presentado y conocen sus afectaciones, lo cual incrementa la vulnerabilidad de recibir ciberataques.

¿Qué tipo de incidentes de seguridad o ciberseguridad ha tenido en su organización?

Tabla 14

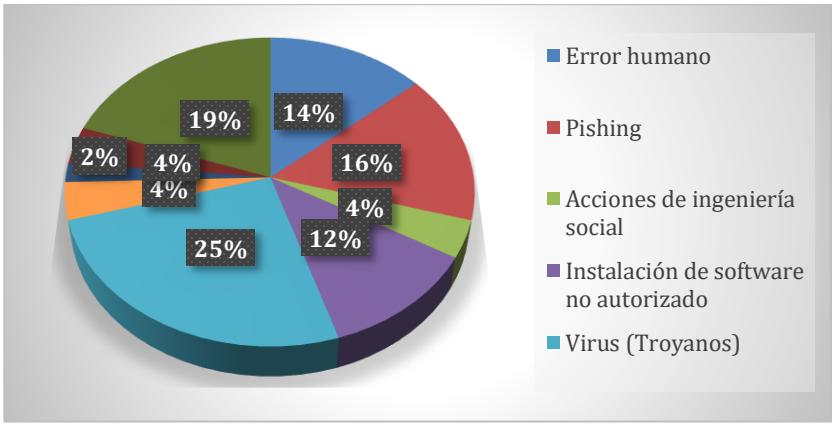
Incidentes que se han presentado en la organización

Opciones	f	%
Error humano	7	7
Phishing	8	8
Acciones de ingeniería social	2	2
Instalación de software no autorizado	6	6
Virus (Troyanos)	13	13
Ciberataques (APT o ataques dirigidos	2	2
Suplantación de identidad	1	1
Ransomware	2	2
No dispongo de esa información	10	10
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 12

Figura 16

Incidentes que se han presentado en la organización



Nota. La figura muestra el desarrollo de la décima segunda pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que apenas un 25% de las personas declaran y tienen conocimiento de que han sufrido un incidente por parte de virus troyanos en su organización, mientras que un 19% declara que han sufrido ataques de

ingeniería social y un 14% lo atañen al error humano y un 12% ha sido afectado por la instalación de software no autorizado. El desconocimiento del uso de herramientas de protección contra virus, malware, ataques, etc. reduce la capacidad de resiliencia ante eventuales incidentes de seguridad en la institución.

¿A quién se reportan los incidentes de seguridad o ciberseguridad?

Tabla 15

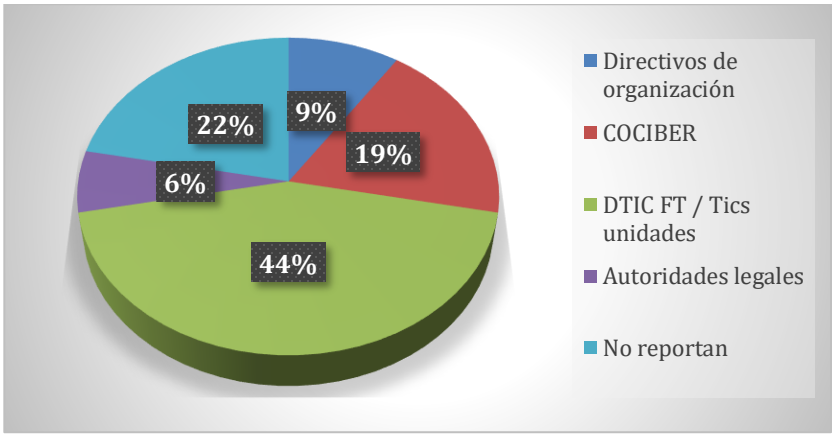
Reportes de incidentes de ciberseguridad

Opciones	f	%
Directivos de organización	3	9
COCIBER	6	19
DTIC FT / Tics unidades	14	44
Autoridades legales	2	6
No reportan	7	22
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 13

Figura 17

Reportes de incidentes de ciberseguridad



Nota. La figura muestra el desarrollo de la décima tercera pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que apenas un 44% de las personas reportan los incidentes de ciberseguridad en sus unidades a la DTIC FT, un 19% lo

reporta al COCIBER y lo que es preocupante para la seguridad es que un 22% no lo reporta a nadie. Al no reportar incidentes de ciberseguridad están vulnerando a la infraestructura tecnológica y comprometiendo la integridad, disponibilidad y confidencialidad de la información.

¿Se realizan evaluaciones de seguridad o ciberseguridad en su organización?

Tabla 16

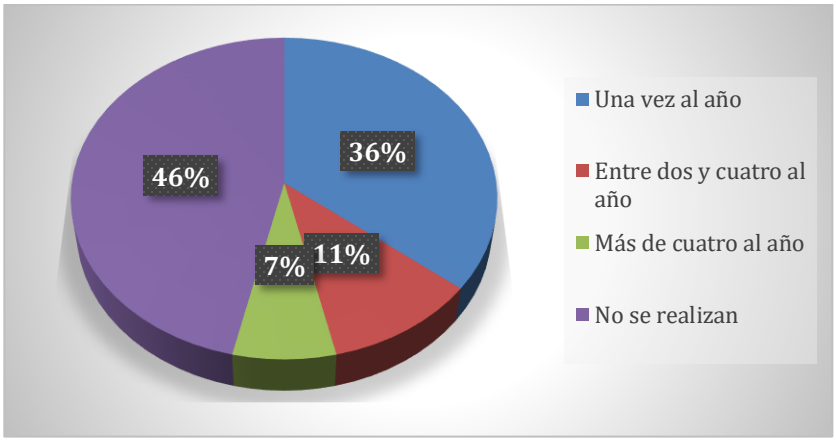
Evaluaciones de ciberseguridad en su organización

Opciones	f	%
Una vez al año	10	36
Entre dos y cuatro al año	3	11
Más de cuatro al año	2	7
No se realizan	13	46
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 14

Figura 18

Evaluaciones de ciberseguridad en su organización



Nota. La figura muestra el desarrollo de la décima cuarta pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que no se realizan evaluaciones de ciberseguridad en la organización en un 46%, sin embargo, en un 36% se la realiza por lo menos una vez al año. Al no realizar evaluaciones de ciberseguridad en la institución, no se

puede identificar ni priorizar los riesgos potenciales; no se puede optimizar el uso de recursos para prevenir, detectar y dar respuesta a los incidentes de seguridad; la institución no genera confianza y credibilidad ante los organismos de control, así como a sus potenciales clientes y empleados; no permite cumplir con la normativa y regulación en lo referente a la protección de datos y seguridad de la información y no se puede evitar los costes asociados a interrupciones de la red, tiempo de inactividad de las aplicaciones y pérdida de información.

¿En su organización, se dispone de políticas de seguridad de la información?

Tabla 17

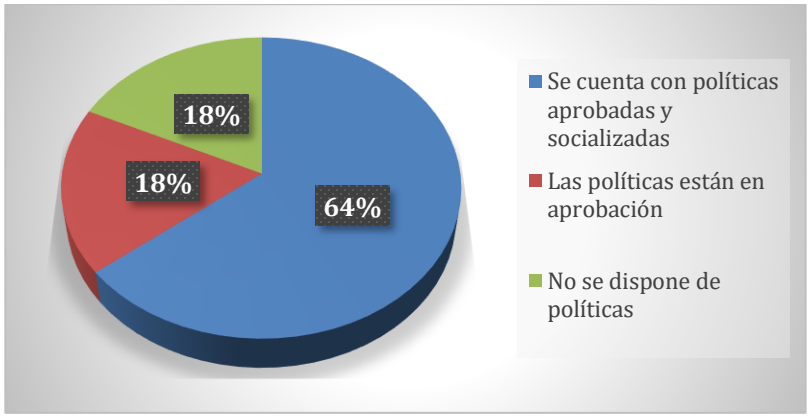
Existen políticas de seguridad en su organización

Opciones	f	%
Se cuenta con políticas aprobadas y socializadas	18	64
Las políticas están en aprobación	5	18
No se dispone de políticas	5	18
Total	**28**	**100**

Nota. Esta tabla muestra la pregunta 15

Figura 19

Existen políticas de seguridad en su organización



Nota. La figura muestra el desarrollo de la décima quinta pregunta de la encuesta realizada.

De las respuestas obtenidas en la pregunta, se tiene que en un 64% de la organización cuenta con políticas aprobadas y socializadas, mientras que en un 18% las políticas están

pendiente su aprobación y un 18% de la organización no dispone de políticas de seguridad. Al no existir políticas de seguridad en la institución, puede generar varios riesgos como: No contar con un marco de referencia para establecer objetivos, responsabilidades y procedimientos de seguridad informática; no definir procedimientos y mecanismos para protegerla información frente a amenazas internas o externas; No se garantiza el cumplimiento de las normas y regulaciones del EGSI y la ISO 27001; finalmente no permite fomentar en sus usuarios la ***Cultura de seguridad*** para prevenir y mitigar incidentes de seguridad

Luego de obtener los resultados de la encuesta en base a la estimación e información otorgada por los técnicos, se pudo determinar que no existen políticas y una guía de hardening que permita al personal encargado en las unidades militares orientar su esfuerzo para mitigar y ser resilientes ante ciberataques, así también el personal con conocimiento técnico es escaso y por ende se incrementa la vulnerabilidad de mantener la integridad, confidencialidad y no repudio de la información disponible.

Comprobación de la Pregunta principal de investigación

Desarrollo del primer objetivo específico

Diagnosticar el estado de seguridad en el correo electrónico institucional desde la percepción de los usuarios de la Fuerza Terrestre y, evaluar la situación de seguridad de la información implementada en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre para determinar la brecha de seguridad en el correo electrónico institucional.

Tomando como base, entrevistas y encuestas realizadas al personal técnico que trabaja en la DTIC FT, es evidente la limitación de personal con la suficiente expertís en seguridad, también se puede recalcar la falta de una cultura de seguridad informática en los usuarios finales y técnicos que administran el correo electrónico institucional. Solo un 43% de los usuarios utilizan el correo electrónico de la institución, quedando un 57% que utiliza otras plataformas, esto se da porque no existen políticas restrictivas en cuanto al uso obligatorio del

correo electrónico institucional para la gestión documental, existe un cumplimiento empírico de las políticas establecidas para la seguridad de la información digital de los diferentes niveles, por lo tanto existen políticas que se cumplen sin tener un conocimiento cabal de las tácticas, técnicas y procedimientos para mantener la ciberseguridad.

El uso de otras plataformas de correo electrónico por parte de los usuarios de la FT, genera una brecha de seguridad en su infraestructura tecnológica, técnicamente es imposible tener un servicio de correo electrónico cien por ciento seguro, ya que este servicio está expuesto permanentemente a recibir ataques por parte de ciberdelincuentes, los cuales pueden causar daños a los usuarios, así como a la institución al atentar contra la integridad y privacidad de la información que fluye a través del mismo. Las principales amenazas de seguridad a través del servicio de correo electrónico que afectan a los usuarios son las siguientes: Malware, Spam, Phishing, Modificación del Hombre en el Medio, Ingeniería Social, Ransomware, Spoofing, Ataques de Open Relay (Pérez & Hernández, 2021). Por lo tanto, se comprueba que el primer objetivo específico planteado es válido y aplicable.

Desarrollo del segundo objetivo específico

Medir el impacto de la brecha de seguridad en el correo electrónico institucional en la infraestructura critica digital de la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre.

Para obtener resultados al medir el impacto que genera la brecha de seguridad en el correo electrónico en el año 2022, se procedió a validar el sistema operativo sobre el cual se encuentran funcionando los componentes del correo electrónico Zimbra (LDAP, Mailbox, MTA), de lo cual se pudo extraer lo siguiente:

- El Sistema Operativo de los servidores LDAP, Mailbox y MTA es la versión Red Hat 6.6
- El sistema operativo no se encuentra con una licencia vigente
- La versión de correo electrónico es Zimbra 8.6.0
- El certificado digital que dispone a la fecha caduco en agosto del año 2019

De la problemática analizada, se pudo determinar que el sistema operativo de la infraestructura de correo electrónico se encuentra funcionando sobre una versión de Red Hat que no posee subscripción, por lo tanto, esta versión no permite instalar parches y actualizaciones de seguridad para prevención de la explotación de vulnerabilidades, considerando que existen otras versiones estables que se encuentran en el mercado que brindan mayor seguridad al servidor. La consola de administración de Zimbra no permite monitorear el estado de los servicios de LDAP, Mailbox y MTA, ya que se encuentra funcionando a través del puerto 2222. El servidor Malibox, se encuentra con varias particiones de diferente capacidad de almacenamiento, cuando se satura este servidor se gestiona manualmente otras particiones ocasionando complejidad en la operación e incluso puede detener el servicio por falta de espacio disponible.

Adicional, en las pruebas realizadas se pudo validar que existen varias cuentas de correo de la FT con los buzones al cien por ciento de su capacidad asignada, por lo tanto, desde dichas cuentas no se puede enviar y recibir correos porque ya no tienen espacio. Cuando los correos no llegan a estas bandejas se quedan encolados en el servidor en espera de ser entregados en el momento que exista disponibilidad de espacio. Actualmente los correos que se encolan están siendo eliminados por una tarea programada en el servidor, lo cual implica que, si un correo importante se encuentra en dicha cola, al ejecutarse la tarea de borrado de correos diferidos serán también borrados.

Lo correcto sería indicarle al usuario como realizar el respaldo, como acceder a su respaldo y vaciar la cuenta para que tenga espacio para recibir y enviar correo.

La configuración de Relay de correo no tiene herramientas que filtren el correo saliente de spam o virus, lo cual ocasiona que el servidor MTA de Zimbra entregue directamente los correos a sus destinatarios sin una previa revisión y/o gestión de virus y spam. Esto ocasiona que la entrega de correos clasifique la IP pública de la FT en listas negras, por lo tanto, se

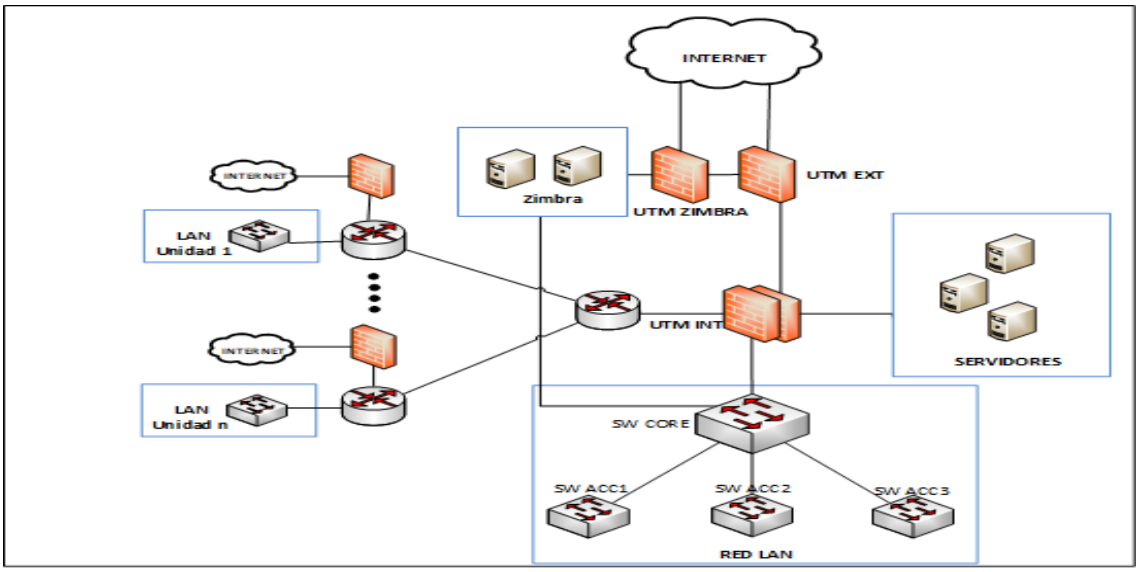
bloquea esta IP para envío de correos, originando encolamiento por el tiempo que permanezca en estas listas.

En el mercado existen nuevas versiones de Zimbra que ofrecen mayor seguridad a los servidores, por lo cual se recomienda realizar la respectiva actualización para prevenir vulnerabilidades y corregir bugs de la versión que actualmente dispone la FT.

A continuación, se muestra el estado de conectividad del servidor de correo electrónico en el año 2022.

Figura 20

Estado actual de conectividad del servidor de correo electrónico



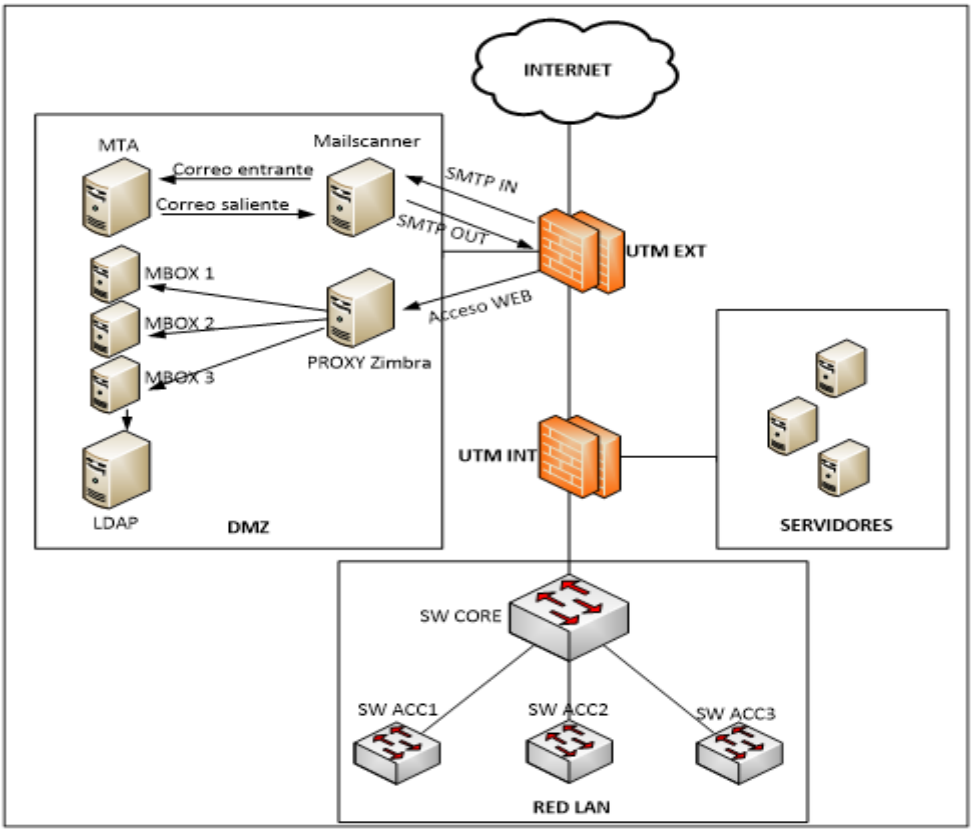
Nota. La figura muestra una representación esquemática del estado de conectividad del correo electrónico, año 2021-2022. Obtenido de DTIC FT

En la figura 20, se observa que cada servidor de correo posee 2 interfaces de red, una interfaz que rutea el tráfico para conectividad interna y otra interfaz que brinda la conectividad hacia la internet, lo cual no es controlado por algún firewall interno, y en caso de compromiso de un servidor de Zimbra se vería comprometida incluso la intranet de la FT.

Para solventar la problemática descrita anteriormente se presenta la siguiente propuesta técnica, en la cual se muestra la arquitectura que podría reducir la brecha de seguridad en el servidor de correo electrónico institucional.

Figura 21

Arquitectura del servidor de correo electrónico propuesta



Nota. La figura muestra una propuesta de la arquitectura del correo electrónico. Obtenido de DTIC FT.

En la arquitectura propuesta se define el servidor de correo electrónico ubicado en la zona de seguridad DMZ, el cual estará protegido por un equipo de seguridad perimetral, que estará encargado de controlar las conexiones hacia el correo electrónico Zimbra. Para mejorar el performance del correo electrónico, se sugiere implementar una versión actual del servidor de correo Zimbra con características de escalabilidad, el cual permita agregar componentes de acuerdo a la necesidad institucional.

Por lo tanto, se evidencia que el segundo objetivo específico planteado es válido y aplicable, para lo cual se entrega una propuesta de una arquitectura que reduciría la brecha de seguridad en la infraestructura digital de la FT.

Desarrollo del tercer objetivo específico

Diseñar una guía metodológica que permita implementar controles de seguridad en la DTIC FT (servidor de correo electrónico institucional), basado en la NORMA ISO/IEC 27001 y el EGSI en su última versión.

La infraestructura tecnológica que dispone la FT está concentrada en el centro de datos de la DTIC FT, existe un centro de redundancia para mantener la disponibilidad de la información en las instalaciones del AGRUCOMGE. En estas instalaciones se da cumplimiento a las políticas de seguridad de la información propias, así también las que están establecidas en el EGSI, siendo el personal técnico del Departamento de Seguridad de la Información el responsable de su aplicabilidad en las unidades militares. La Infraestructura tecnológica de la FT, dentro de algunos de los servicios disponibles cuenta con servidores de correo electrónico (Zimbra), antivirus institucional, adicional se realizan campañas de concientización en la cultura de seguridad informática tanto para los técnicos como así también para los usuarios finales, lo cual permite mantener la seguridad, integridad, confidencialidad y no repudio de la información de la FT.

Para reducir la brecha de seguridad en la infraestructura tecnológica de la FT, en la presente investigación se ha considerado implementar los controles de seguridad de la NORMA ISO/IEC 27001 y del EGSI en su última versión, los cuales permiten implementar y concientizar a los usuarios en el uso de buenas prácticas para el despliegue seguro del servicio de correo electrónico institucional evidenciando que el tercer objetivo específico planteado es válido y aplicable, para lo cual se entrega una propuesta de la guía metodológica que reduciría la brecha de seguridad en la infraestructura digital de la FT.

Capítulo V:

Propuesta

Datos informativos:

Título de la propuesta

Diseñar una guía metodológica que permita implementar controles de seguridad en la DTIC FT (servidor de correo electrónico institucional), basado en la NORMA ISO/IEC 27001 y el EGSI en su última versión.

Antecedentes de la propuesta

El desarrollo tecnológico y la conexión a la internet en un mundo globalizado por el uso de las comunicaciones permite acceder en tiempo real a todas las bondades que brinda la tecnología, así también nos obliga a su dependencia para manejar una gran cantidad de información en los servidores corporativos e institucionales. la información que es uno de los activos más valiosos es vulnerable a sufrir ataques por parte de ciberdelincuentes, que pretenden robar la información que dispone una persona o institución. Dando cumplimiento a las políticas de seguridad de la información emitidas por el Ministerio de Telecomunicaciones a través del Esquema Gubernamental de Seguridad de la Información, se presenta una propuesta de guía metodológica, la cual puede ser aplicada en la DTIC FT y las unidades de comunicaciones de la FT.

Justificación

En la actualidad hay un bajo cumplimiento de políticas de seguridad de la información en las unidades de la FT, así también hay desconocimiento y falta de personal con capacitación en seguridades informáticas, por lo que se presenta la presente guía metodológica que permitirá implementar controles de seguridad en la DTIC FT (servidor de correo electrónico institucional).

De la información obtenida en la DTIC FT, se puede concluir los siguiente:

- Los usuarios al no disponer de un equipo informático institucional, para la institución es considerada como una amenaza, conforme el listado de amenazas y vulnerabilidades en ISO 27001 (EXCELENCIA, 2019), al comprometer información confidencial de la institución.
- Al no existir políticas para el uso exclusivo de correo electrónico institucional para la gestión documental, podrían ser consideradas como potenciales vulneraciones a la seguridad, ya que, al no tener el control de estas cuentas de correo, se pudiera hacer mal uso de la información, o posiblemente exista fuga de la misma, sin que quede registro.
- El no disponer de una cuenta de Chasqui para la gestión documental, pude influir en la evasión de responsabilidad que pueden asumir los funcionarios que no la tienen.
- Existen usuarios que aún mantienen instalado en sus computadoras el sistema operativo Windows 7, mismo no tiene actualizaciones disponibles al haber cumplido su vida útil, no tiene soporte ni actualizaciones. Esto vulnera la seguridad ante ciberataques.
- Un 14% de los usuarios no dispone de antivirus, lo cual incrementa la vulnerabilidad de esos equipos al quedar desprotegidos ante el accionar de ciberdelincuentes.
- Un 25% usan una versión gratuita de antivirus, el cual es descargado de internet y un 18% no saben que función cumple un antivirus en sus equipos, lo cual incrementa la vulnerabilidad.
- Un 14% nunca usan un antivirus, al no utilizarlo los equipos informáticos se exponen a posibles ataques de virus o malware, que pueden ser aprovechados por ciberdelincuentes que podrían fácilmente explotar esta vulnerabilidad.
- Un 25% usan el firewall de su computador, al no utilizarlo, los equipos pueden ser más vulnerables a recibir ataques de virus, malware, hackers, o programas no autorizados.

- Un 11% no conoce que es un incidente de seguridad, lo cual puede ser un factor negativo al momento de ser resiliente ante un ciberataque.
- Un 50% del personal no tiene capacitación en ciberseguridad, lo cual puede incrementar el riesgo de amenazas y vulnerabilidades, afectando a la integridad, confidencialidad y disponibilidad de la información de la institución. Además, al no disponer de este personal, puede causar dificultades para hacer detección, prevención y respuesta ante incidentes de seguridad, así como el cumplimiento de las políticas, normativas y regulaciones vigentes.
- Un 68% de las personas no disponen de información ni herramientas informáticas, que permitan detectar incidentes de ciberseguridad, apenas un 32% entre 1 y 3 incidentes se han presentado y conocen sus afectaciones, lo cual incrementa la vulnerabilidad de recibir ciberataques.
- El desconocimiento del uso de herramientas de protección contra virus, malware, ataques, etc reduce la capacidad de resiliencia ante eventuales incidentes de seguridad en la institución.
- Al no reportar incidentes de ciberseguridad están vulnerando a la infraestructura tecnológica y comprometiendo la integridad, disponibilidad y confidencialidad de la información.
- Al no realizar evaluaciones de ciberseguridad en la institución, no se puede identificar ni priorizar los riesgos potenciales; no se puede optimizar el uso de recursos para prevenir, detectar y dar respuesta a los incidentes de seguridad; la institución no genera confianza y credibilidad ante los organismos de control, así como a sus potenciales clientes y empleados; no permite cumplir con la normativa y regulación en lo referente a la protección de datos y seguridad de la información y no se puede evitar los costes asociados a interrupciones de la red, tiempo de inactividad de las aplicaciones y pérdida de información.

- Al no existir políticas de seguridad en la institución, puede generar varios riesgos como: No contar con un marco de referencia para establecer objetivos, responsabilidades y procedimientos de seguridad informática; no definir procedimientos y mecanismos para protegerla información frente a amenazas internas o externas; no se garantiza el cumplimiento de las normas y regulaciones del EGSI y la ISO 27001; finalmente no permite fomentar en sus usuarios la ***Cultura de seguridad*** para prevenir y mitigar incidentes de seguridad.

Objetivos

Desarrollar una guía metodológica que permita implementar controles de seguridad en la DTIC FT (servidor de correo electrónico institucional), basado en la NORMA ISO/IEC 27001 y el EGSI en su última versión, para reducir la brecha de seguridad informática que puede generar el correo electrónico en la infraestructura tecnológica de la FT.

Fundamentación propuesta

Para dar cumplimiento a la fundamentación de la presente guía, se ha utilizado la normativa vigente del EGSI en su última versión, así también se utilizó la norma ISO/IEC 27001 para la seguridad de la información.

Diseño de la propuesta

Se adjunta el Anexo “A” GUÍA METODOLÓGICA PARA IMPLEMENTAR CONTROLES DE SEGURIDAD EN LA FT.

Metodología para ejecutar la propuesta

La metodología empleada en la presente propuesta se realiza a través de una lista de chequeo, basado en la NORMA ISO/IEC 27001 y el EGSI en su última versión, en la cual se puede reducir la brecha de seguridad que puede ocasionar el servidor de correo electrónico en la FT y la exposición de vulnerabilidades tecnológicas.

Bibliografía

2022, C. (s.f.). Obtenido de https://ciberseguridad.com/servicios/analisis-vulnerabilidades/

Abad y Sandoval, P. W. (10 de diciembre de 2020). *Escuela Politécnica del Ejercito.* Obtenido de Análisis de la Situación Actual de Ciberdefensa en la Fuerza Terrestre 2020: http://repositorio.espe.edu.ec/bitstream/21000/23263/1/T-ESPE-044111.pdf

Abalde Paz, E., & Muñoz-Cantero, J.-M. (1992). Metodología cuantitativa vs. cualitativa. *Repositorio de la Universidad de Coruña*, 50-62.

ÁTICO34, G. (2022). *Vulnerabilidad informática: Qué es y cómo protegerse*. Obtenido de https://protecciondatos-lopd.com/empresas/vulnerabilidad-informatica/

Borbúa, R. V., Herrera, L. R., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. Quito. doi:https://doi.org/10.17141/urvio.20.2017.2571

Carrillo Punina, Á. (2022). *Metodología de la Investigación.* Quito.

CISCO. (s.f.). *Firewalls.* Obtenido de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Comercio. (9 de Septiembre de 2014). *El Comercio*. Obtenido de https://www.elcomercio.com/actualidad/ciberdefensa-ecuador-comando-fuerzasarmadas-ministerioddefensa.html

CONSTITUCIÓN. (20 de OCTUBRE de 2008). *CONSTITUCIÓN DEL ECUADOR.* Obtenido de https://www.cne.gob.ec/wp-content/uploads/2014/04/1_Constitucion_de_la_Republica_del_Ecuador.pdf

Del Canto , E., & Silva Silva, A. (2013). METODOLOGIA CUANTITATIVA: ABORDAJE DESDE LA COMPLEMENTARIEDAD EN CIENCIAS. *Revista de ciencias sociales*, 25-34.

ESET. (Agosto de 2020). *welive security*. Obtenido de https://www.welivesecurity.com/la-es/2020/08/06/advierten-sobre-los-riesgos-de-seguridad-que-supone-seguir-utilizando-windows-7/

Eset. (30 de Agosto de 2022). *welivesecurity by ESET.* Obtenido de https://www.welivesecurity.com/la-es/2022/08/30/campana-malware-dirigida-organismos-alto-perfil-ecuador/

ESET, S. R. (2022). *Security Report*. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf

EXCELENCIA, E. E. (Noviembre de 2019). *Listado de amenazas y vulnerabilidades en ISO 27001*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/

FT. (2017). *OBJETIVOS ESTRATÉGICOS DEL EJÉRCITO ECUATORIANO 2017-2021.* Obtenido de https://ejercitoecuatoriano.mil.ec/institucion/fftt/objetivo-institucional

Gómez, Á. (2014). *Seguridad en equipos informáticos.* Madrid: RA-MA.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la Investigación.* México: McGRAW-HILL.

Hidalgo, L. (2006). Confiabilidad y Validez en el Contexto de la Investigación y Evaluación. 1-2.

ISO: Organización Internacional de Internacionalización. (2022). Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestiòn de la seguridad de la información - Requisitos. Internacional Estàndar: ISO/CEI 27001. Tercera Ediciòn. https://es.scribd.com/document/616176936/ISO-27001-2022-espanol

INEN. (2015). *NTE INEN-ISO/IEC 27002.* Obtenido de https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27002.pdf

INNEVO. (2022). *Norma ISO 27001*. Obtenido de https://www.innevo.com/es/iso27001

ISO. (2005). *ISO 27001.* Obtenido de https://www.normas-iso.com/iso-27001/

Kaspersky. (s.f.). *Malware & Computer Virus Facts & FAQs*. Obtenido de https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

Marketing, & Ecommerce. (2023). *Marketing Ecommerce*. Obtenido de https://marketing4ecommerce.net/usuarios-de-internet-mundo/

MENTOR, A. (s.f.). *Normas ISO sobre gestión de seguridad de la información*. Obtenido de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html#:~:text=ISO%2FIEC%2027001&text=Norma%20que%20especifica%20los%20requisitos,internacional%20en%20octubre%20de%202005.

MINTEL. (28 de octubre de 2019). Obtenido de http://www.pge.gob.ec/images/documentos/LeyTransparencia/2019/octubre/a2/politica_ecuador_digital.pdf

MINTEL. (10 de enero de 2020). *Esquema Gubernamental de Seguridad de la Información (EGSI).* Obtenido de https://www.gobiernoelectronico.gob.ec/egsi-v2

MINTEL. (3 de agosto de 2022). Obtenido de https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/registro-oficial/item/16628-registro-oficial-no-61

Monsalve, J., Aponte, F., & Chaves, D. (Diciembre de 2014). *Revista Facultad de Ingeniería*. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292014000200007

Morillo y Duque, F. R. (8 de diciembre de 2018). *LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS EN EL ÁMBITO DE LAS FUERZAS ARMADAS.* Obtenido de file:///C:/Users/ARIAS/Downloads/wfuertes,+RCSD-V5N1-ART01.pdf

Nacional, A. (21 de junio de 2017). *Ley de Seguridad Pública y del Estado.* Obtenido de https://www.gob.ec/sites/default/files/regulations/2018-11/Documento_Ley-Seguridad-P%C3%BAblica-Estado.pdf

Pérez, A., & Hernández, A. (enero de 2021). *Buenas prácticas para el despliegue seguro del servicio de correo electrónico*. (R. científica, Editor, & U. D. Caldas, Productor) doi:https://doi.org/10.14483/23448350.15838

Reidi Martínez, L. (2012). El diseño de investigación en educación. *Investigación en Educación Médica*, 35-39.

Report Eset, S. (2021). Obtenido de Prensario TI Latin America: https://prensariotila.com/33526-eset-security-report-2021/

Roba, L., Vento, J., & García, L. (2016). Metodología para la Detección de Vulnerabilidades en las Redes de Datos. (R. C. AVANCES, Ed.) pág. 335. Obtenido de https://www.redalyc.org/pdf/6378/637867033003.pdf

Saltos. (30 de Octubre de 2021). *Repositorio Espe.* Obtenido de https://repositorio.espe.edu.ec/handle/21000/4537/simple-search?query=&sort_by=score&order=desc&rpp=10&filter_field_1=dateIssued&filter_type_1=equals&filter_value_1=%5B2020+TO+2022%5D&etal=0&author_page=42

Saroka, R., & Voutssas, M. (2002). *Sistemas de información en la era digital.* Buenos Aires, Argentina: Fundación OSDE.

Tesis y Masters. (19 de febrero de 2023). Obtenido de https://tesisymasters.mx/instrumentos-de-recoleccion-de-datos/

Voutssas, J. (octubre de 2010). *Preservación documental digital y seguridad informática.* doi:http://dx.doi.org/10.22201/iibi.0187358xp.2010.50.21416

Ministerio de Defensa Nacional. (2018). *Política de la Defensa Nacional del Ecuador "Libro Blanco".* Quito: Instituto Geográfico Militar.

Red de Seguridad y Defensa de América Latinas. (2011). *Libro Blanco de la Defensa Nacional - Las Fuerzas Armadas.* Obtenido de https://www.resdal.org/Archivo/ecu-libro-cap4.htm

Apéndices