ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

PROYECTO DE INVESTIGACIÓN

Brecha de seguridad en el correo electrónico institucional y su impacto en la infraestructura critica digital de la DTIC FT en el año 2022

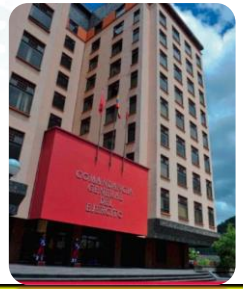
XAVIER DÁVILA, CRISTIAN ARIAS

SUMARIO

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

INTRODUCCIÓN

Macroprocesos de la DTIC FT



Lineamientos y directrices del Comandante General de la F.T.

Plan de Gestion institucional de la F.T.

Inventario de hardware y software

Inventario de comunicaciones

Resultados de evaluaciones tecnicas

Necesidades de comunicaciones e informatica

DIRECCIONAMIENTO DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

GESTIÓN DE COMUNICACIONES E INFORMÁTICA

DESARROLLO DE PROYECTOS

SEGURIDAD TECNOLÓGICA

Norma de gestión del sistema de comunicaciones de la F.T.

Plan de las TICs

Directrices o lineamientos de las TICs

Estándares de las TICs

Proyectos de Comunicaciones, Guerra Electrónica, Informática, Seguridad informática y metrología TECNOLOGÍAS

Software aplicativo y manuales del Sistema Integrado de la Fuerza Terrestre (SIFTE)

Informes técnicos de las TICs

Seguridad digital y comunicaciones

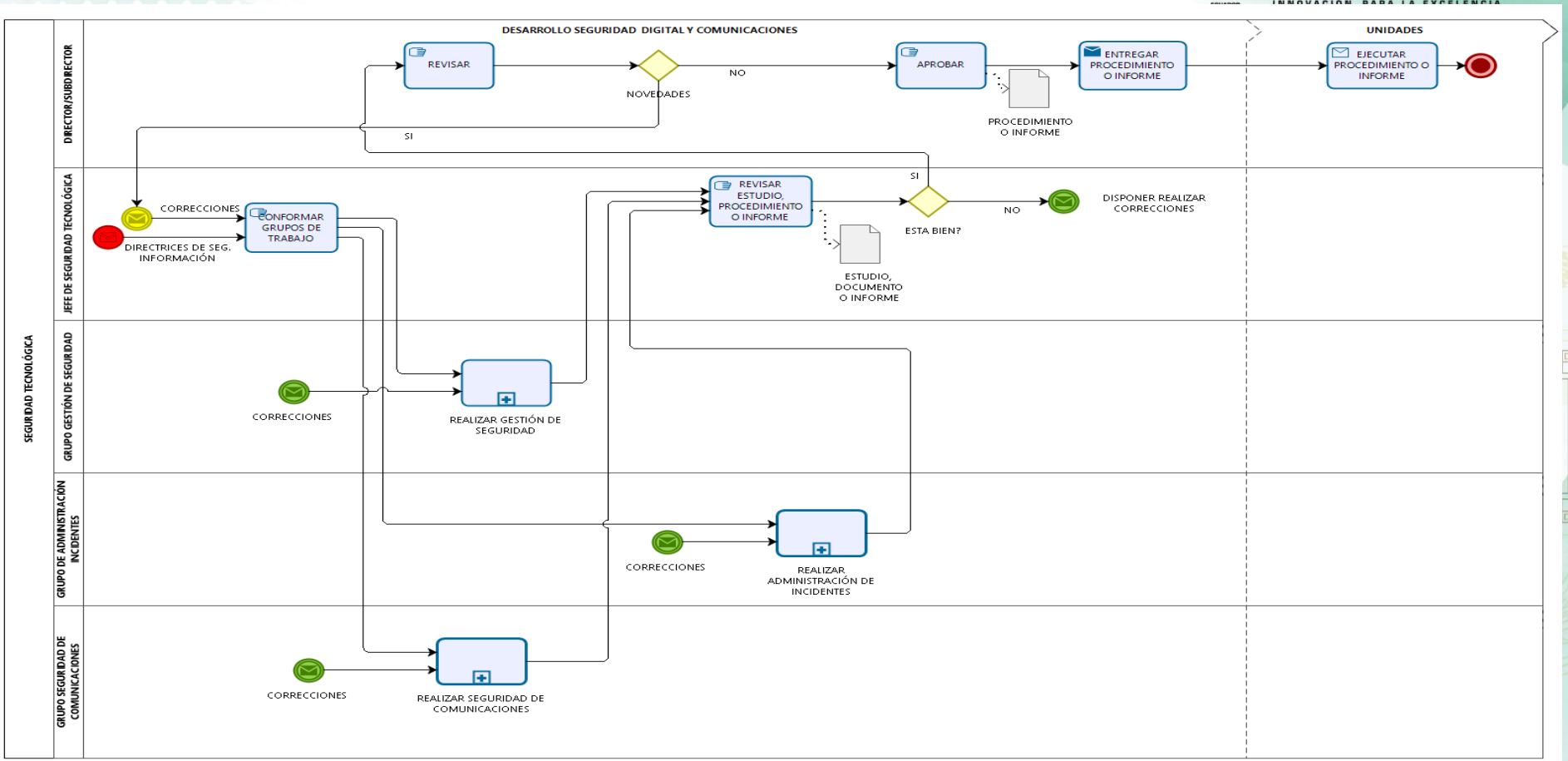
Propósito:
Implementar el EGSI, gestionar riesgos, proporcionar soporte de Seg digital y Seg de Com mediante la gestión de Seg Digital, administración de incidentes y Seg de Com, para incrementar la eficacia de ciberseguridad en la FT.

Disparador:
- Lineamientos del Director
- Incidentes del Seg informática

Entradas:
- EGSI
- Reportes de incidentes informáticos
- Requerimientos de Seg de Com

Subprocesos:
- *Gestión de seguridad digital*
- Administración de incidentes informáticos
- Seguridad de Comunicaciones

Proceso de Seguridad tecnológica



Árbol de problemas

Consecuencias

A través de la brecha de seguridad en el correo electrónico, la FT es vulnerable a recibir ataques informáticos, afectando a la integridad, disponibilidad y confidencialidad de la información.

Efecto final

Vulnerabilidad en la seguridad informática

Escasos proyectos de seguridades informáticas.

No existe resiliencia ante ataques

Problema central

Brecha de seguridad en el correo electrónico de la FT.

Personal no capacitado

Restricción económica

Falta de herramientas tecnológicas

Causas

Justificación

Disponer de una guía metodológica y aplicar controles de seguridad de la información. ISO 27001

DTIC, BC1,CIA DIV, CIA BRIG, PEL COM

Objetivos

General

Analizar el impacto de la brecha de seguridad en el correo electrónico institucional en la infraestructura crítica digital de la DTIC FT en el año 2022, con el fin de diseñar una guía metodológica que permita implementar controles de seguridad.

Específicos

Diagnosticar el estado de seguridad en el correo electrónico institucional desde la percepción de los usuarios de la FT y, evaluar la situación de seguridad de la información implementada en la DTIC FT 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 DTIC FT.

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.

Preguntas de investigación

NORMA ISO 27001 Seguridad de la información

Variable Independiente

Secundarias:

- Expertís del personal
- Políticas y protocolos de Seguridad
- Herramientas informáticas, alertan vulnerabilidades

PP: ¿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?

Infraestructura digital de la FT.

Variable Dependiente

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

METODOLOGÍA

Investigación

1 DISEÑO DE INVESTIGACIÓN

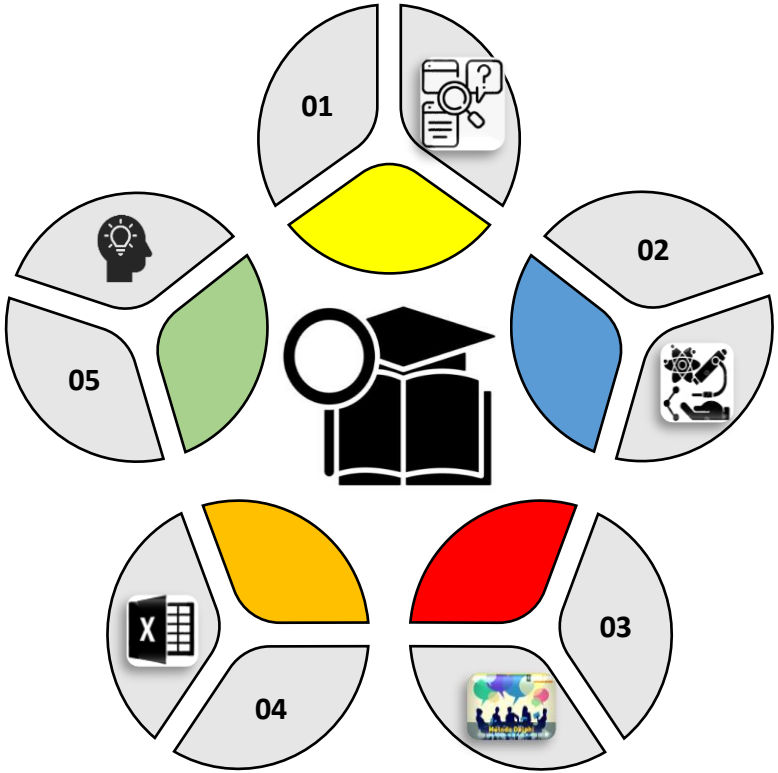
Se aplicó el diseño de investigación **cuantitativa,** ya que parte de datos evidenciables.

2 TIPO DE INVESTIGACIÓN

Se utilizó la **investigación explicativa** ya que se pretende la compresión o entendimiento de un fenómeno.

3 TÉCNICA DE INVESTIGACIÓN

Se utilizó la **técnica Delphi**, la cual nos permite conocer la opinión de un grupo de personas en relación a un problema, sin que los integrantes se reúnan físicamente.



4 TÉCNICA DE ANÁLISIS DE DATOS

Se aplicará **la técnica de la correlación** en la interpretación de los datos, a través del programa informático **Microsoft Excel.**

5 COMPROBACIÓN DE HIPÓTESIS

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**.

Población y muestra

Se consideró una población **con conocimiento técnico** perteneciente al **área de las TIC**

01

Gestión y administración de la seguridad informática.

02

Personal técnico militar y servidores públicos, que tienen perfiles con diferente privilegios.

03

Ejecución del proyecto

RECOLECCIÓN DE DATOS

COMUNIDADES EN LÍNEA ⟷ **ENCUESTAS**

ENCUESTA

- Correo electrónico
- Políticas de Seguridad
- Personal capacitado

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

RESULTADOS

Resultados de la investigación

43%
Zimbra

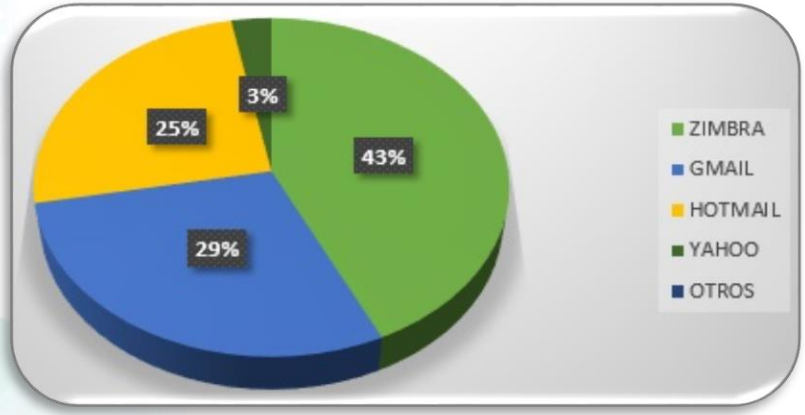
29%
Gmail

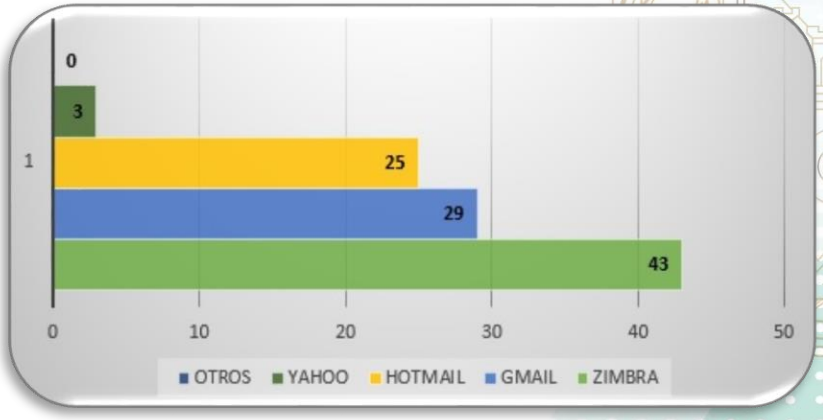
25%
Hotmail

3%
Yahoo

0%
Otros

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





Resultados de la investigación

50%

No se dispone

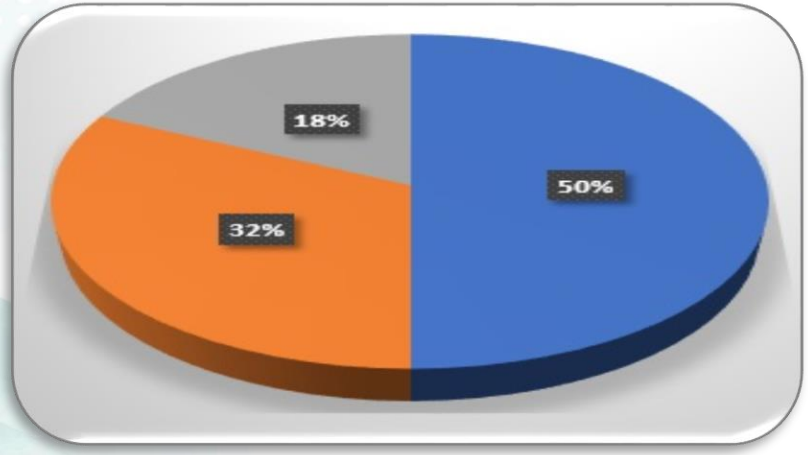
32%

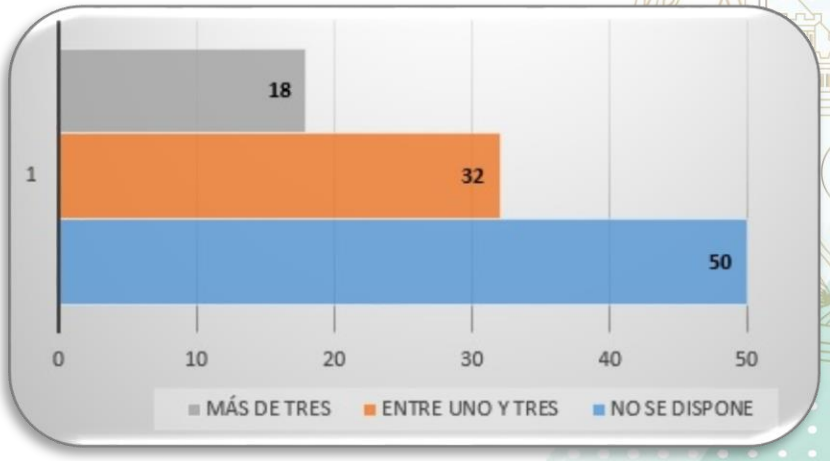
Entre uno y tres

18%

Más de tres

¿En su organización cuenta con personal capacitado en seguridad o ciberseguridad informática?





Resultados de la investigación

64%

Se cuenta con políticas

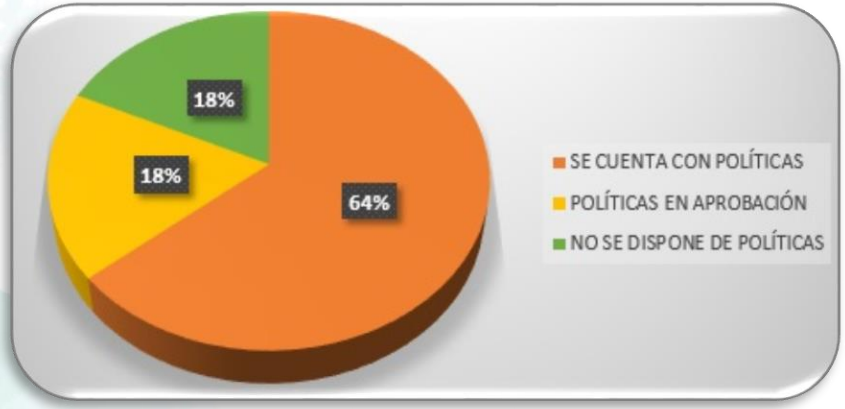
18%

Políticas en aprobación

18%

No se dispone de políticas

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



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

PROPUESTA

Guía metodológica

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.

Apéndices

GUÍA METODOLÓGICA PARA IMPLEMENTAR CONTROLES DE SEGURIDAD EN LA FT

Apéndice 1: GUÍA METODOLÓGICA PARA IMPLEMENTAR CONTROLES DE SEGURIDAD EN LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA FT.

	PREGUNTAS	CUMPLE	NO CUMPLE	OBSERVACIONES
POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	¿Existen políticas, procesos, prácticas y registros relacionados con proveedores que involucran servicios de TI?			
	¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo?			
	¿Los contratos y acuerdos abordan lo siguiente?			
	- Riesgo de la información, aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada			
	- Información / propiedad intelectual, y obligaciones / limitaciones derivadas			
	- Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información			
	- Requisitos legales y normativos.			
	- Identificación de controles físicos y lógicos			
	- Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio			
	- Habilitación de seguridad de los empleados y concienciación			
	- Pistas de auditoría de seguridad por parte de la Institución			
	¿Existe una obligación contractual de cumplimento?			
	¿Los proveedores de servicios externos son monitoreados rutinariamente para cumplir con los requisitos de seguridad?			
REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	¿Todas las políticas tienen un formato y estilo consistentes?			
	¿Están todos al día, habiendo completado todas las revisiones debidas?			
	¿Se han vuelto a autorizar y se han distribuido?			

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La falta de cumplimiento de las normas y políticas de seguridad de la información establecidas se presentan como las principales dificultades para el mantenimiento de una efectiva ciberseguridad

La falta de una cultura de seguridad por parte de los usuarios influye directamente en generar brechas de seguridad que pueden atentar en la fuga de información

La falta de personal capacitado que administre la infraestructura tecnológica, crean brechas de seguridad.

A través de una guía metodológica, es factible aplicar controles de seguridad basados en la NORMA ISO 27001 para mejorar la gestión de incidentes informáticos en la infraestructura digital de la FT.

Recomendaciones

Para mitigar las deficiencias en ciberseguridad, una vez se implemente la guía metodológica se requiere desarrollar programas de capacitación para el personal técnico y usuarios finales para mantener un estricto cumplimiento de la normativa y estándares vigentes.

Incentivar a crear una cultura de seguridad en el personal, crear conciencia en la importancia de mantener la integridad, confidencialidad y disponibilidad de la información.

Considerar nuevos proyectos a futuro, sobre la base del que nos ataña.

MUCHAS GRACIAS