UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

PROGRAMA DE FORMACIÓN DE SEGURIDAD INFORMÁTICA, BASADO EN LA PUBLICACIÓN NIST SP 800-50 PARA LA CONTRALORÍA GENERAL DEL ESTADO - DIRECCIÓN PROVINCIAL DE IMBABURA

Trabajo de Investigación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

AUTOR: Cristian Fernando Rodríguez Erazo

TUTOR: Msc. Fausto Alberto Salazar Fierro

IBARRA - ECUADOR

2023

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Investigación con el tema: "PROGRAMA DE FORMACIÓN DE SEGURIDAD INFORMÁTICA, BASADO EN LA PUBLICACIÓN NIST SP 800-50 PARA LA CONTRALORIA GENERAL DEL ESTADO - DIRECCIÓN PROVINCIAL DE IMBABURA" de autoría de Rodríguez Erazo Cristian Fernando, para obtener el Título de Magíster en Computación con mención en Seguridad Informática, doy fe que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 24 días del mes de octubre de 2023

1002172631
FAUSTO
ALBERTO
SALAZAR FIERRO

Firmado digitalmente por 1002172631 FAUSTO ALBERTO SALAZAR FIERRO
Fecha: 2023.10.26 16:40:38 -05'00'

Msc. Fausto Alberto Salazar Fierro

Tutor

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	1002989869		
APELLIDOS Y NOMBRES	Rodríguez Erazo Cristian Fernando		
DIRECCIÓN	Mitimaes SN y Av. El Retorno		
EMAIL	cfrodrigueze@utn.edu.ec		
TELÉFONO FIJO	NA	**TELÉFONO MÓVIL:**	0990362497

DATOS DE LA OBRA	
TÍTULO:	PROGRAMA DE FORMACIÓN DE SEGURIDAD INFORMÁTICA, BASADO EN LA PUBLICACIÓN NIST SP 800-50 PARA LA CONTRALORÍA GENERAL DEL ESTADO - DIRECCIÓN PROVINCIAL DE IMBABURA
AUTOR (ES):	Rodríguez Erazo Cristian Fernando
FECHA: DD/MM/AAAA	1/12/2023
PROGRAMA DE POSGRADO	Maestría en Computación con mención en Seguridad Informática
TITULO POR EL QUE OPTA	Magíster en Computación con mención en Seguridad Informática
TUTOR	Msc. Fausto Salazar Fierro

2. CONSTANCIAS

El autor Cristian Fernando Rodríguez Erazo manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, al 1 día del mes de diciembre del año 2023.

EL AUTOR:

Firma 

Cristian Fernando Rodríguez Erazo

DEDICATORIA

A mi esposa y a mi hijo por todo el amor y paciencia brindados durante todo el tiempo de estudio de esta Maestría, por ser el soporte y motivación de siempre ser mejor persona y mejor profesional.

A mi madre, por todo el amor brindado desde siempre, la dedicación para con sus hijos por sus cuidados, su amor y por habernos educado de la mejor manera.

A mi padre, por siempre estar al pendiente de toda mi familia, por ser un ejemplo de hombre trabajador, por su amor, su comprensión y paciencia.

A mis hermanas por darme todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño y por todo su apoyo para cumplir con éxito una de las principales metas de mi vida.

AGRADECIMIENTO

A Dios, por brindarme la oportunidad de cumplir todas las metas que me he planteado y por las que seguiré cumpliendo en un futuro.

Al Msc. Fausto Salazar y a la Phd. Cathy Guevara, Tutor y Asesora del presente proyecto, quienes con sus conocimientos y tiempo supieron guiarme en la realización de este trabajo de investigación.

A todos los docentes de la Maestría, quienes supieron compartir todo el conocimiento necesario para ampliar mi campo profesional.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

"PROGRAMA DE FORMACIÓN DE SEGURIDAD INFORMÁTICA, BASADO EN LA PUBLICACIÓN NIST SP 800-50 PARA LA CONTRALORIA GENERAL DEL ESTADO - DIRECCIÓN PROVINCIAL DE IMBABURA"

Autor: Rodríguez Erazo Cristian Fernando

Correo: cfrodrigueze@utn.edu.ec

El desconocimiento de los funcionarios de la Contraloría General del Estado - Dirección Provincial de Imbabura (CGE-DPI) y la escasa formación en materia de seguridad informática podrían ocasionar situaciones que provoquen daños a los activos de información y a los datos de la Institución. El objetivo del presente estudio se centró en implementar un programa de formación de seguridad informática. El enfoque de investigación fue de carácter cuantitativo, se realizó una recopilación e interpretación de los datos obtenidos de la formación que se llevó a cabo, así como la validación del programa propuesto, mediante la evaluación de la efectividad y el impacto que generó en los funcionarios. El procedimiento metodológico, que se utilizó, para conocer a fondo la situación de la problemática presentada fue la investigación de campo para la obtención de la información necesaria para el desarrollo del programa de formación. Los instrumentos utilizados para investigar la problemática planteada, fueron a través de las diferentes técnicas de este tipo de investigación, en este caso: observación, formularios de evaluación, reportes y encuestas. Todas estas técnicas se realizaron a una población de 47 funcionarios de los cuales participaron 31, los resultados fueron sometidas al análisis respectivo, obteniéndose conclusiones y |recomendaciones. Los resultados evidenciaron que existió un antes y un después de la implementación del programa de formación de seguridad informática. Evidenciándose una efectividad del 58,82% del programa, al verificar que existió una disminución en la ocurrencia de incidentes de seguridad post implementación.

ABSTRACT

"COMPUTER SECURITY TRAINING PROGRAM, BASED ON NIST SP 800-50 PUBLICATION FOR THE CONTRALORIA GENERAL DEL ESTADO - DIRECCIÓN PROVINCIAL DE IMBABURA"

Author: Rodríguez Erazo Cristian Fernando

Email: cfrodrigueze@utn.edu.ec

The lack of knowledge of the Contraloría General del Estado - Dirección Provincial de Imbabura (CGE-DPI) employees and the limited training in computer security could cause situations that cause damage to the information assets and data of the Institution. The objective of this study focused on implementing a computer security training program. The research approach was quantitative in nature, a compilation and interpretation of the data obtained from the training that was implemented, as well as the validation of the proposed program, by evaluating the effectiveness and the impact it generated on the employees. The methodological procedure that was used to fully understand the situation of the problem presented was field research to obtain the necessary information for the development of the training program. The instruments used to investigate the problem raised were through the different techniques of this type of research, in this case: observation, evaluation forms, reports and surveys. All these techniques were implemented on a population of 47 employees, of which 31 participated, The results were subjected to the respective analysis, obtaining conclusions and recommendations. The results showed that there was a before and after the implementation of the computer security training program. Evidence of an effectiveness of 58.82% of the program, verifying that there was a decrease in the occurrence of security incidents post-implementation.

CAPÍTULO I

EL PROBLEMA

1.1 Introducción

En la seguridad informática, el factor humano es siempre el eslabón más débil. A nivel informático, se traduce en que la gran mayoría de las infecciones de malware que se producen son responsabilidad directa del usuario, en muchas ocasiones de forma totalmente involuntaria. Un estudio en materia de seguridad informática realizado por Check Point a finales de 2016 dio como resultado que: el malware sigue creciendo en las empresas fundamentalmente porque los propios empleados descargan algún tipo de este software malicioso cada cuatro segundos. Una situación que se vuelve incluso más complicada si se analizan los dispositivos móviles, cada vez más implantados en cualquier tipo de negocio debido a las ventajas en movilidad y productividad que ofrecen soluciones informáticas como Office 365. (Awe & Awe, 2016)

De esta manera, la seguridad de estos dispositivos se ve comprometida bien porque se realiza la descarga de algún tipo de malware en éstos o bien por conectarse a redes inseguras o maliciosas. La conclusión del estudio es que no basta con implementar gran infraestructura tecnológica para buscar la protección de los sistemas o dispositivos, sino que hace falta también formar a los usuarios para que mantengan en todo momento buenas prácticas y aseguren la integridad de los archivos y equipos. (Awe & Awe, 2016)

1.2 Problema de investigación

Las amenazas informáticas avanzan en la misma medida que surgen innovaciones tecnológicas, mismas que tienden a neutralizar las iniciativas maliciosas. Es una carrera que no tiene fin, ya que, cuando se logra hacer frente a un determinado malware, los usuarios maliciosos estudian la nueva tecnología y pueden crear nuevos vectores de ataque. (Castillo & Castillo, 2020)

Actualmente las nuevas tecnologías permiten tener una adecuada seguridad en la información de las organizaciones, estas tecnologías son cada día más sofisticadas, desde cifrado de extremo a extremo para las conversaciones de audio, texto y documentos hasta códigos de verificación de 2 pasos. De igual manera, las soluciones informáticas para tener la adecuada infraestructura en los sistemas han estado mejorando día a día las

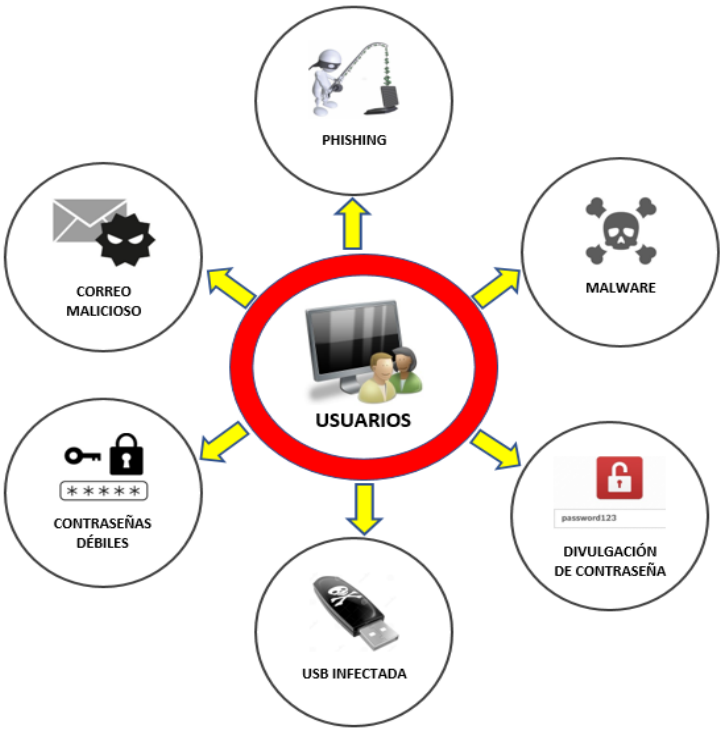
estrategias, pero, a pesar de todas estas soluciones y de que las organizaciones cuenten con complejos sistemas que garanticen no ser víctimas de un ciberataque, el factor humano sigue siendo un gran problema. (Castillo & Castillo, 2020)

Las organizaciones ya no pueden confiar únicamente en sus métodos comunes de defensa tecnológica para mantenerlas a salvo. Los ciberdelincuentes están utilizando sofisticadas técnicas de ingeniería social para evadir estas defensas. Y todo lo que se necesita es que un empleado haga clic en un enlace malicioso o descargue un archivo infectado para que su información quede en riesgo. (Ciberseg., 2019)

Los empleados deben ser la primera línea de defensa contra la ciberdelincuencia, por lo que es vital que posean todos los conocimientos y habilidades necesarias para proteger la organización. Un programa de formación de seguridad informática es la mejor manera de educar al personal y crear una cultura de seguridad prioritaria. (Ciberseg., 2019)

Figura 1

Descuido o desconocimiento de los usuarios



Nota. Este gráfico muestra las amenazas que podrían aprovechar el desconocimiento de los usuarios.

La falta de conocimiento de los funcionarios de la Contraloría General del Estado - Dirección Provincial de Imbabura (CGE-DPI) y la escasa formación en materia de seguridad

informática podrían ocasionar situaciones que provoquen daños a los activos de información y a los datos de la Institución.

Los principales incidentes que se han presentado dentro de la Institución, provocados por el desconocimiento de los funcionarios han sido por utilizar memorias usb en cualquier dispositivo, no cerrar la sesión del computador cada vez que no se encuentran frente al equipo, contraseñas débiles, divulgar y compartir las contraseñas, ataques de ingeniería social, pérdida de información por ransomware, irrespetar o desconocer la normativa vigente, etc.

La Institución cuenta con una gran infraestructura tecnológica, ofrece una alta disponibilidad de sus servicios informáticos, sin embargo, esto no es suficiente, sino que también los funcionarios deben ser parte fundamental de la seguridad informática.

Son por estas razones que dentro de la CGE-DPI debe ser una prioridad, mejorar los métodos para que los funcionarios entiendan la importancia de la seguridad de sus datos, es necesario formar y generar una cultura de seguridad adecuada para que logren identificar una potencial amenaza, por ejemplo, saber la diferencia entre un correo fraudulento y uno genuino, ya que de esto depende que no se lamenten por haber perdido toda su información.

1.3 Interrogantes de la investigación

- ¿Cuáles son las amenazas de seguridad informática que podrían afectar la protección de los activos e información digital en la Contraloría General del Estado - Dirección Provincial de Imbabura?
- ¿Cuál es el nivel de conocimiento sobre seguridad informática que tienen los funcionarios de la Contraloría General del Estado - Dirección Provincial de Imbabura?
- Los funcionarios de la Contraloría General del Estado - Dirección Provincial de Imbabura, ¿se encuentran preparados a la hora de afrontar amenazas informáticas?

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Implementar un programa de formación de seguridad informática, basado en la publicación NIST SP 800-50, para la Contraloría General del Estado - Dirección Provincial de Imbabura.

1.3.2 Objetivos específicos

- Realizar un marco conceptual de las amenazas de seguridad informática, para la protección de activos de información en la CGE-DPI.
- Determinar el nivel de conocimiento sobre seguridad informática que poseen los servidores de la CGE-DPI.
- Diseñar el programa de formación sobre la seguridad informática, de acuerdo a las directrices de la NIST SP 800-50.
- Evaluar la efectividad del programa de formación al personal de la CGE-DPI, en base al modelo 2 de la NIST SP 800-50.

1.5 Justificación

Intentar cambiar los hábitos de los usuarios no es una tarea sencilla, pero se debe iniciar paso a paso, realizando planes o programas de formación y concientización, para orientar e instruir a los empleados, ya que, usuario que ignora aspectos de seguridad informática, puede provocar que todo el trabajo de meses sea encriptado, al ser víctimas de un ransomware, como son varios casos que se han suscitado a nivel de Latinoamérica, quienes recibieron un ataque de este tipo, en el que se secuestró información para posteriormente extorsionar a la empresa y solicitar un depósito millonario para facilitar la llave de desencriptación; todo sucedió por un usuario que abrió un correo malicioso y, desconociendo las medidas básicas de prevención de seguridad informática, cayó en la trampa de los criminales. (Castillo & Castillo, 2020)

Existen ciberdelincuentes que intentarán penetrar la seguridad de los dispositivos con intenciones maliciosas como pueden ser atacar a otros equipos o sitios web o redes simplemente para molestar. (De Expertos En Ciencia Y Tecnología, 2022)

Se debe prevenir el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos, hojas de cálculo, etc. Es primordial durante las actuales comunicaciones. Muchas de las acciones diarias dependen de la seguridad informática a lo largo de toda la ruta que siguen nuestros datos. Los datos almacenados en un computador también pueden ser mal utilizados por accesos no autorizadas. (De Expertos En Ciencia Y Tecnología, 2022)

Los anteriores aspectos vuelven a evidenciar la necesidad de que los datos deben permanecer seguros y protegidos confidencialmente. Son por estas razones que, no sólo tenemos que invertir en la adecuada infraestructura tecnológica, sino también en la formación de los empleados para permitir el correcto uso de las tecnologías. Por lo tanto, es necesario desarrollar programas de formación y concientización que complementen y contribuyan a la Seguridad de la Información. (Castillo & Castillo, 2020)

CAPITULO II

MARCO REFERENCIAL

2.1 Antecedentes

Al realizar diversas consultas en las en diferentes bases de datos de investigación académica con respecto a las investigaciones previas, se encontraron los siguientes proyectos que aportan aspectos significativos relacionados con el presente proyecto:

La utilización de las nuevas tecnologías de la información y comunicaciones se ha convertido en un aspecto fundamental de la globalización. El avance continuo de las herramientas disponibles para la gestión de la información, tales como celulares, tabletas, portátiles, etc., permiten ingresar a un universo de información de todo tipo de contenido, tales como redes sociales, correos electrónicos, fotos, chats, blogs, etc., y a su vez permite a los cibercriminales ampliar su panorámica, respecto a sus objetivos, accediendo a información personal, financiera, social y demás. Toda esta tecnología y su constante evolución constituyen altos riesgos en la seguridad de la información, lo que genera la necesidad de aplicar controles efectivos que permitan protegerse de dichas amenazas. (Augusto, 2017)

Este documento trata las recomendaciones para crear concienciación en seguridad de la información en favor de la seguridad y así explotar de la mejor manera el avance tecnológico. (Augusto, 2017)

A diario se descubren nuevas debilidades, por lo general, son pocos los responsables de Tecnología que comprenden la importancia que tiene la seguridad y cómo pueden afrontar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de una organización y cometer delitos en función del robo de información. (Fases de un ataque informatico, 2014)

En este marco, donde los principales actores son las organizaciones de cualquier magnitud, los sistemas de información, el dinero y ciberdelincuentes; es absolutamente necesario y primordial planear estrategias de seguridad que permitan instaurar barreras defensivas orientadas a disminuir efectivamente ataques tanto externos como internos. (Fases de un ataque informatico, 2014)

Para disminuir de manera eficaz el impacto provocado por los ataques informáticos, es de gran importancia conocer de qué manera atacan y cuáles son las vulnerabilidades de un sistema comúnmente explotadas, en los que se deben encaminar los esfuerzos de seguridad tendientes a la prevención de los mismos. (Fases de un ataque informatico, 2014)

2.2 Marco teórico

2.2.1 Seguridad informática

Concepto

La ciberseguridad se refiere al resguardo de la información y, principalmente, al procesamiento que se hace de la misma, con la finalidad de impedir la manipulación de datos y procesos por personas no autorizadas. Su principal objetivo es que tanto usuarios como infraestructura tecnológica e información cuenten con protección contra daños y amenazas hechas por ciberdelincuentes. (CX Solutions, s. f.)

Por esta razón, la protección de la privacidad de la información dentro de los sistemas informáticos se ha vuelto parte indispensable para las empresas y la operación de las organizaciones. (CX Solutions, s. f.)

Se sabe que no existen sistemas 100% seguros, por lo que las organizaciones que hacen uso de la actual tecnología, deben buscar los mecanismos idóneos para garantizar la seguridad de su información, a través de los diferentes tipos de seguridad informática que existen. (Unir, 2022)

Tipos

- **Seguridad orientada al hardware**: Resguardo principal del dispositivo, ya que sin elementos de hardware no puede haber dispositivo en sí. Este tipo de seguridad se centra en el resguardo del firmware, entre otros aspectos, este elemento es el encargado de ejecutar y dar paso al software en el equipo o dispositivo. Por tal razón, si se vulnera alguna seguridad en el firmware, se podrá acceder casi con total seguridad de forma indirecta al software. (Llamas, 2022)

- **Seguridad orientada al software**: Este tipo de seguridad es la más conocida y la que más ataques recibe en el mundo virtual, ya que es la más vulnerable, y el número de iniciativas para intentar penetrarla es muy grande en comparación con

la seguridad de hardware. Deteriorar el funcionamiento del sistema operativo o de un programa en concreto, con fines relacionados con el espionaje o el robo de información, son los más comunes. (Llamas, 2022)

- **Seguridad orientada a la red**: La seguridad que se basa en redes es aquella que trata el resguardo de los canales por los que se envía y recibe información entre dispositivos. Frecuentemente suele ser noticia que los servidores de una aplicación o software han sido presa de un ataque, sin ser los dispositivos de forma directa el objetivo de ataque. La información que buscan los atacantes es la que se almacena en los servidores, los cuales guardan gran cantidad de información personal de los usuarios. (Llamas, 2022)

Pilares

- **Confidencialidad**

Este aspecto impide que la información se difunda públicamente a individuos u organizaciones no autorizadas; esto significa que, certifica que el acceso a la información sea únicamente a las personas autorizadas.

Es así que, abarca todos los mecanismos que eviten que se divulgue información que no es conveniente que se conozca por usuarios ajenos a la organización. (AdminIberoBlogs, 2021)

- **Disponibilidad**

Característica de la información de estar al alcance de quienes deben acceder a ella, ya sean usuarios, organismos o procesos, en el momento que sea requerido.

Es de gran importancia, ya que un acceso limitado en el tiempo puede ser una ventaja para la seguridad, pero también una desventaja para la operación. Es así que la disponibilidad debe tener este equilibrio. (AdminIberoBlogs, 2021)

- **Integridad**

La integridad de la información es la garantía de que los datos no han sido modificados y que la información es completamente cierta.

La capacidad de asegurar con exactitud que la información que fue generada sigue siendo la misma, sin modificaciones no autorizadas e incluso garantizar un registro de

estos casos, es relevante para no utilizar información manipulada y que lleve a la toma de decisiones bajo contextos equívocos. (AdminIberoBlogs, 2021)

En los últimos tiempos ha comenzado a tener mayor relevancia e interés una característica adicional, ya que la suplantación de identidad es una amenaza potencial. Esta característica es la **autenticación,** misma que permite reconocer la identidad de la persona que brinda y accede a la información. Es posible que puede estar considerada como parte de la integridad o disponibilidad, sin embargo, es trascendental darle la relevancia para evitar que pase desapercibida. (AdminIberoBlogs, 2021)

¿Qué protege?

Los elementos más relevantes que la ciberseguridad busca proteger en cualquier sistema informático son el hardware, el software y la información. El hardware corresponde a todas las partes físicas que conforman el sistema, desde los dispositivos que se encuentran dentro del CPU(memorias, unidades, tarjetas, entre otros) hasta los que se encuentra por fuera de él (teclado, mouse, pantalla, entre otros). El Software hace referencia todos aquellos componentes lógicos (Sistemas Operativos y Aplicaciones) que le dan funcionamiento al hardware. La información corresponde a todos aquellos datos procesados y organizados que se almacenan en un Sistema Informático. (Augusto, 2017)

¿De qué protege?

Protege a los diferentes sistemas de información con el objetivo de que éstos se encuentren seguros sin que sean susceptibles de ser atacados frente a diferentes amenazas. Son varias las amenazas que pueden atacar a un sistema informático, se puntualizan las más comunes que tiene la seguridad informática: (Augusto, 2017)

- **Los propios usuarios**: la falta de conocimiento o la escasa formación en materia de seguridad puede causar situaciones no deseables. Insertar las memorias usb en cualquier dispositivo, no cerrar o bloquear la sesión de usuario cada vez que no se encuentren frente al equipo, irrespetar o desconocer la normativa vigente...

- **Fallos en el desarrollo de software**: un software desarrollado, pero con errores informáticos, sin los respectivos controles de seguridad, es una puerta abierta donde hackers y crackers se aprovechan de dicha vulnerabilidad.

- **Intrusos**: controlar el acceso tanto a los medios electrónicos (bases de datos, programas de trabajo...) como a los medios físicos (el acceso a las salas donde se encuentra el centro de datos o donde se almacenan las grabaciones de las cámaras de seguridad). Un acceso por parte de terceros puede provocar daños graves, más aún si no se tiene conocimientos, es una situación que puede llegar a ser catastrófica. (Augusto, 2017)

- **Catástrofes naturales**: son imprevistas, con baja probabilidad de que sucedan, no se esperan, pero las catástrofes y desastres naturales son una amenaza frente a la protección de los sistemas. Para esto siempre lo mejor es la prevención. (Augusto, 2017)

¿Qué es y por qué proteger los activos de información?

Un activo de información es cualquier información o sistema relacionado con el tratamiento de la misma que represente valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipamiento informático, talento humano, soportes de información, redes, equipamiento auxiliar o instalaciones. Puede ser atacado deliberada o accidentalmente con efectos graves para la organización. (Infordisa / Security Operations Center, 2021)

Proteger estos activos de información es salvaguardar el proceso del negocio, hacerlo más fiable y asegurar su continuidad. Para lograrlo hay que aplicar medidas que prevengan tanto su pérdida como su interrupción e impedir daños en la información confidencial y en los sistemas que son trascendentales para el correcto funcionamiento del negocio. (Tituaña, 2017)

Ataque

Cuando se habla de un ataque informático se hace referencia a la realización de un intento de poner en riesgo la seguridad informática de un equipo o conjunto de equipos, con el fin de provocar daños deliberados que deterioren su funcionamiento. (Caser, 2023)

Ciberdelincuente

Es todo aquel que realiza acciones delictivas a través de internet, como el robo, el uso ilegítimo de información, el acceder a redes privadas, estafas y engaños. En general,

todo lo concerniente con delitos e ilegalidad en el mundo digital, internet y los sistemas informáticos, ya que estas personas cuentan con amplios conocimientos en tecnología. (Méndez G., 2021)

Hacker

Un Hacker es una persona con amplio conocimiento de tecnología de la información y comunicaciones, dedicado a detectar fallas de seguridad informática. Un hacker puede ser un ciberdelincuente, pero la diferencia es que éste saca provecho y se beneficia de manera ilegal de todas estas fallas de seguridad que encuentra. (Méndez G., 2021)

2.2.2 Marco conceptual de amenazas

Una amenaza informática es toda aquella acción que aprovecha una vulnerabilidad para atacar o entrar en un sistema informático. Las principales amenazas informáticas que podrían vulnerar a las organizaciones provienen en gran medida de ataques externos, aunque también existen amenazas internas como lo es el robo de información o el uso inadecuado de los sistemas. (Team, s. f.)

Algunas de las amenazas más comunes a las que se enfrentan las organizaciones a diario:

Usuarios

Los usuarios son considerados la mayor causa de problemas referentes a la seguridad informática. Es así porque con sus acciones podrían ocasionar graves consecuencias, son el eslabón más débil de la cadena de la ciberseguridad. (xeral.net, 2017)

- **Desconocimiento**

Muchos de los incidentes de seguridad más comunes y frecuentes, como las campañas de phishing o el ransomware, tienen un punto en común: requieren de cierta interacción y "cooperación" del propio usuario para lograr su objetivo. (*El desconocimiento de los usuarios, ¿principal causa de infecciones?*, 2017)

Los ciberdelincuentes se aprovechan del descuido y, por qué no, de la ingenuidad de una gran cantidad de usuarios para apropiarse de sus datos personales, sus números de

tarjeta de crédito y sus contraseñas. Simultáneamente, las amenazas informáticas se camuflan en supuestas facturas pendientes de pago, multas de tránsito o documentos sensibles, y siguen infectando víctimas. (*El desconocimiento de los usuarios, ¿principal causa de infecciones*?, 2017)

Situación que puede evitarse si los usuarios conocieran mejor el proceder de las amenazas y las estafas, lo cual les permitiría estar alertas y protegerse. Identificando las características de un correo o sitio fraudulento, es mucho más fácil evitar caer en la trampa. (Pagnotta, s. f.)

Por esta razón no es un error decir que el desconocimiento de los usuarios, lo que generalmente se denomina "el error humano", es una de las mayores causas de incidentes informáticos. (Pagnotta, s. f.)

- **Malas prácticas**

Contraseñas.- Son la llave al mundo privado, es común compartir o dejar a la vista de todos, son predecibles e inseguras. La contraseña más usada es 123456, según la empresa ESET. (Jiménez, s. f.)

Redes públicas.- No se conoce su nivel de seguridad y pueden ser intervenidas por un tercero. A pesar de aquello los usuarios las utilizan para compartir información personal. No utiliza sus datos móviles o se conecta en su casa para tratar asuntos privados. En redes públicas no se debe: sincronizar fotos o videos, abrir aplicaciones de bancos e instituciones financieras, hacer compras en línea. (Jiménez, s. f.)

Privacidad de la información.- no hay cautela a la hora de compartir datos personales. No se evita ni se cuida lo que se envía y con quién se comparte esta información. No se cierra o se bloquea la sesión cuando no se encuentran frente al computador. Esto facilita a los ciberdelincuentes obtener fotos o videos íntimos, que son información que puede prestarse para para ciber extorsiones. Se ha evidenciado que las claves y contraseñas se comparten por medios digitales, se publican en redes sociales información sensible: correos, teléfonos, cédulas o direcciones. (Jiménez, s. f.)

Enlaces, archivos adjuntos- Los enlaces son una forma común de robar información. Es frecuente que los usuarios abran enlaces de remitentes desconocidos o que no son confiables; de esta manera pueden ser en algún momento víctimas de "phishing". De la

misma manera sucede cuando los usuarios descargan y abren archivos adjuntos de remitentes no confiables, se puede caer en algún tipo de "malware". (Jiménez, s. f.)

Malware

Conocido como software malicioso, es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. El malware es un enemigo, intrusivo e intencionadamente fastidioso y molesto, intenta invadir, deteriorar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, por lo general tomando el control parcial de las operaciones de un dispositivo. (Belcic, 2023)

- **Ransomware**

El ransomware es uno de los diferentes tipos de malware, diseñado para rechazar el acceso a un sistema informático o a la información hasta que se pague un rescate. Se propaga a través de correos electrónicos de phishing, publicidad maliciosa, visitando sitios web infectados o ingresando dispositivos usb infectados. (Ciberseg, 2019)

Los ataques de ransomware causan tiempo de inactividad, fugas de datos, robo de propiedad intelectual, cifrado y pérdida de datos. La razón por la que este tipo de malware es tan peligroso es porque una vez que los ciberdelincuentes se apoderan de los archivos, no hay ningún software de seguridad ni restauración del sistema capaz de recuperarlos. A menos que se pague el rescate e incluso si se paga dicho rescate, no hay ninguna garantía de que los ciberdelincuentes devuelvan los archivos, las cantidades por pagos de rescates pueden llegar a ser de cientos de miles de dólares. (Ciberseg, 2019)

Figura 2

Ransomware

Nota. Adaptado de Chau, G. (2020, 10 febrero). Ransomware. *acebusiness*. https://www.acebizservices.com/post/2020/02/10/ransomware

- **Virus**

Un virus informático, al igual que un virus de gripe, está diseñado para difundirse de un dispositivo a otro y tiene la capacidad de replicarse. Al igual que el virus común, no pueden reproducirse sin una célula que los acoja, los virus informáticos no pueden reproducirse ni multiplicarse sin una programación, por ejemplo, un archivo o un documento. (What is a computer virus?, s. f.)

Figura 3

Virus

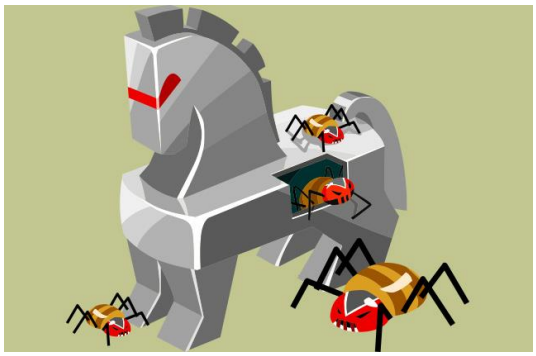
Nota. Adaptado de 123RF. (s. f.). Concepto antivirus portátil. https://es.123rf.com/clipart-vectorizado/virus_computer.html

- **Troyanos**

Un troyano es un archivo o software que parece ser verdadero y seguro, pero en realidad se trata de un código malicioso. Los troyanos se empaquetan y se entregan dentro de un programa legítimo y son diseñados para espiar a las víctimas o robar su información. Los troyanos aparentan ser algo inofensivo, pero es solo una envoltura para ocultar su verdadera intención. (Belcic, 2023)

Figura 4

Troyano



Nota. Adaptado de Belcic, I. (2023). ¿Qué es un malware Troyano? Guía definitiva. ¿Qué es un malware troyano? Guía definitiva. https://www.avast.com/es-es/c-trojan

- **Gusanos**

Un gusano informático es un tipo de malware que se reproduce a sí mismo, mientras se difunde por las redes a tantos dispositivos como sea posible. Razón que hace que el gusano informático sea característicamente peligroso para las organizaciones. (Gusanos informáticos - definición, reconocimiento y protección, 2020)

Figura 5

Gusano

Nota. Adaptado de Ryan. (2022). What are computer worms and how do they work? Blue Bastion. https://www.bluebastion.net/computer-worms-and-how-they-work/

- **Keylogger**

Los keyloggers actúan realizando un seguimiento y registrando cada tecla que se pulsa en un teclado, generalmente sin el permiso ni el conocimiento del usuario. Los keyloggers son un spyware malicioso usado para capturar información confidencial, como contraseñas o información financiera que luego serán enviados a terceros para su aprovechamiento con fines delictivos. (¿Qué es un keylogger?, 2023)

Figura 6

Keylogger

Nota. Adaptado de ¿Qué es un keylogger? (2023, 19 abril). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/keylogger

Ingeniería Social

La ingeniería social se aprovecha de las personas a través de la manipulación, para que compartan información que no deberían compartir, descarguen software que no deberían descargar, accedan a sitios web que no deberían acceder, envíen dinero a ciberdelincuentes e incurran en otros errores que compliquen la seguridad de los activos o seguridad personal o empresarial. (¿Qué es la ingeniería social? | IBM, s. f.)

La ingeniería social actúa a través de la naturaleza humana, en lugar de un ataque informático técnico, manipula la psicología de las personas para que comprometan la seguridad personal o empresarial. (¿Qué es la ingeniería social? | IBM, s. f.)

- **Phishing**

Es el delito de engañar a los usuarios para que faciliten su información confidencial como contraseñas y números de tarjetas de crédito. Al igual como sucede en la pesca, existe más de una forma de atrapar a una víctima, pero hay una forma de phishing que es la más común. (Anatomy of a Phishing Attack, s. f.)

Los usuarios que son víctimas de este ataque reciben un correo electrónico o un sms que plagia o suplanta la identidad de una persona u organización, por ejemplo, un compañero de trabajo, un banco o una oficina de gobierno. Cuando la persona abre el correo electrónico o el sms, encuentra un mensaje diseñado intencionalmente para asustar, para debilitar su buen juicio al provocar el miedo. El mensaje indica que la víctima vaya a un sitio web y actúe inmediatamente o tendrá que afrontar alguna consecuencia. (Malwarebytes, 2019)

Si un usuario cae en la trampa y hace clic en el enlace, se le redirecciona a un sitio web idéntico al legítimo. Es aquí cuando se le solicita que se registre con el nombre de usuario y contraseña. Si la persona es lo suficientemente inocente y lo hace, la información de inicio de sesión llega al ciberdelincuente, la cual será utilizada para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro. (Malwarebytes, 2019)

Figura 7

Phishing

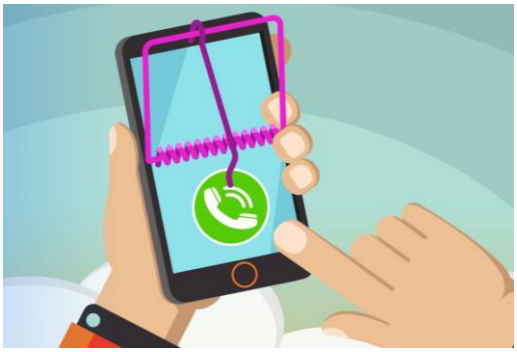
Nota. Adaptado de Cardozo, R. (2023, 22 marzo). «Phishing» y «smishing», ¿qué son y cómo evitarlos? BBVA NOTICIAS. https://www.bbva.com/es/innovacion/phishing-y-smishing-que-son-y-como-evitarlos/

- **Vishing**

Vishing aparece de la unión de voice y phishing, esto significa que comprende a aquellos ataques de phishing que involucran una voz, ya sea robótica o humana. En este tipo de ataque, los ciberdelincuentes pueden llegar a la víctima mediante llamadas telefónicas masivas, como un call-center corporativo, o dejando correos de voz. Entre los temas escogidos por los estafadores a través de estas comunicaciones, encontramos referencias a problemas financieros o de seguridad del computador, dispositivo móvil, o la suplantación de identidad de un supuesto familiar o conocido. (WeLiveSecurity, 2023)

Figura 8

Vishing



Nota. Adaptado de Diaz, I. M. C. (2023). ¿Que es Vishing? INFORMÁTICA FORENSE COLOMBIA. https://www.informaticaforense.com.co/vishing-2/

- **Pharming**

Es un tipo de estafa que los atacantes utilizan para instalar malware en computadores personales o servidores. El término proviene de las palabras inglesas “farming” (cultivo) y “phishing” y es relativamente una técnica nueva y más complicada que los atacantes utilizan para acceder a información sensible. (Security, 2023)

Figura 9

Pharming

Nota. Adaptado de Klusaitė, L., & Klusaitė, L. (2023). ¿Qué es un ataque de Pharming? NordVPN. https://nordvpn.com/es/blog/que-es-pharming/

Ataque de contraseñas

- **Ataque de fuerza bruta**

Es un tipo de ataque básico a las contraseñas que llevan a cabo los atacantes de forma continua. Se produce al realizar un gran número de intentos de acceso a una red utilizando un listado de contraseñas comunes o altamente comprometidas. (Valenzuela, 2022)

- **Relleno de credenciales**

El Credential Stuffing es un hackeo automatizado en el que se tratan combinaciones de nombres de usuario y contraseñas robadas en el proceso de ingreso de credenciales. (Serem, 2022)

- **Ataque de diccionario**

Es una variación del ataque de fuerza bruta. Su objetivo es el de optimizar el tiempo requerido para identificar la clave. Para ello, se utilizan listas de palabras, conocidas también como diccionarios, las cuales incluyen términos frecuentemente usados como contraseñas e inclusive pueden contener contraseñas filtradas en el mercado

negro. El uso de diccionarios puede aumentar significativamente la probabilidad de éxito de un ataque de contraseña. (KeepCoding, 2023)

Correo malicioso

También llamado spam o correo basura, tiene distintas formas de presentarse siendo alguna de ellas más destructivas que otras. Estos mensajes suelen parecer que los envía una fuente acreditada o bien pide el vínculo a una página oficial, cuya apariencia es igual a la oficial. (Correo malicioso-Universidad de Extremadura, s. f.)

Seguridad física

- **Acceso físico**

El acceso no autorizado es una de las frecuentes amenazas de seguridad física y más conocidas actualmente. ¿De qué sirve implementar el mejor cortafuegos del momento si el atacante puede abrir el equipo y llevarse el disco duro o copiar la información? (Jurado & Jurado, 2023)

- **Vandalismo**

El vandalismo es actualmente una amenaza potencial para la seguridad informática, especialmente en situaciones de revueltas sociales o conflictos civiles. Generalmente no es común que los vándalos ingresen físicamente a un edificio para dañar el mobiliario y los equipos informáticos, sin embargo, en casos de levantamientos, existe el riesgo de que los delincuentes se aprovechen de las circunstancias para saquear, destruir o robar equipos electrónicos. (Jurado & Jurado, 2023)

- **Desastres naturales**

Los desastres naturales, terremotos, inundaciones o filtraciones de humedad representan otra gran amenaza física para los equipos físicos que no cuentan con la debida protección. (Jurado & Jurado, 2023)

2.2.3 Publicación NIST SP 800-50

Este documento procura ser una guía para estructurar un programa efectivo de concientización y entrenamiento en seguridad informática para agencias federales de

Estados Unidos. Pero, también puede ser utilizado por otro tipo de organizaciones, en otros países. (Wilson & Hash, 2003)

Estructura

La guía establece cuatro pasos críticos en el ciclo de vida de un programa de concientización y entrenamiento:

- **Diseño del programa**: Conlleva un relevamiento dentro de la organización y, a partir de su resultado, se desarrolla y aprueba la estrategia a seguir durante el programa, siguiendo la misión de la organización.

- **Desarrollo del material**: mediante la evaluación del alcance del entrenamiento deseado, el contenido necesario para cubrirlo y las posibles fuentes para desarrollarlo.

- **Implementación del programa**: Se expone y se lanza el programa de concientización y entrenamiento, a través de los medios definidos en la estrategia.

- **Post implementación**: Se busca mantener una mejora continua del programa y monitorear su efectividad.

Modelo 2- Gestión de programas parcialmente descentralizada

Este segundo modelo de gestión de programas parcialmente descentralizado, generalmente es implementado por organizaciones que son grandes o tienen una estructura bastante descentralizada, con responsabilidades claras y asignadas tanto a la sede central como a los niveles de unidad.

Tienen funciones que están distribuidas en un área geográfica amplia, o tienen unidades organizacionales con misiones diversas, de modo que los programas de concientización y capacitación puedan cambiar significativamente, según las necesidades específicas de cada unidad. (Wilson & Hash, 2003)

Figura 10

Modelo 2-Gestión de programas parcialmente descentralizado

Nota. Adaptado de Wilson, M., & Hash, J. *Building an Information Technology Security Awareness and Training Program*. https://doi.org/10.6028/nist.sp.800-50

2.2.4 Marco legal

Constitución de la República del Ecuador

La Constitución de la República vigente desde el año 2008, en el capítulo sexto mencionado como **Derechos de libertad**, se encuentran disposiciones que pueden ser tomadas para el presente programa, específicamente la contenida en el Art. 66 numerales 19 y 21.

Art. 66.- Se reconoce y garantizará a las personas:

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recopilación, archivo, procesamiento, distribución o propagación de estos datos o información requerirán la autorización del titular o el mandato de la ley.

21. El derecho a la inviolabilidad y a la intimidad de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial 18 y con la obligación de guardar la intimidad de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.

Ley Orgánica de Protección de Datos Personales

El capítulo II Principios, señala que:

g) Confidencialidad.-El tratamiento de datos personales debe entenderse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

j) Seguridad de datos personales.-Los responsables y encargados de tratamiento de los datos personales implementarán todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto

Reglamento de Políticas de Seguridad de la Información y uso responsable de los Recursos de Tecnología de la Información y Comunicación de la Contraloría General del Estado

Art. 19.- Uso de la contraseña.- La contraseña tiene por objeto garantizar que únicamente el servidor público a quien se le haya asignado, disponga de acceso a los sistemas y recursos de tecnologías de la información institucionales que estrictamente le correspondan, de acuerdo con su perfil de usuario, funciones y responsabilidades. La contraseña es de uso personal, exclusivo, reservado, confidencial e intransferible.

Art. 36.- Prohibiciones en el uso de computadoras de escritorio, portátiles y demás dispositivos móviles.- En lo que a la utilización de equipos y recursos informáticos respecta, queda estrictamente prohibido:

a) Emplearlos para asuntos personales y/o ajenos a la actividad laboral, aún fuera del horario de trabajo y de las instalaciones de la institución;

b) Obtener por cualquier medio y sin consentimiento, información de los computadores o de la red informática de la Contraloría General del Estado, para utilizarla de forma personal o en favor de terceros;

c) Trasladar los equipos informáticos fuera de la institución sin contar con autorización expresa previa y por escrito del titular de la unidad administrativa correspondiente;

d) Manipular los equipos informáticos institucionales; esto es, entre otros similares: instalar, extraer, acoplar o cambiar dispositivos externos o internos, piezas de hardware, accesorios y elementos que no sean de propiedad de la Contraloría General del Estado, sin contar con el consentimiento previo y por escrito de la Dirección Nacional de Tecnología de la Información y Comunicaciones;

e) Instalar en los equipos informáticos institucionales programas de servidores de correo, web, archivos (FTP o TFTP), proxy y similares, ajenos a los proporcionados por la entidad, videojuegos; y, en general, cualquier tipo de software, sea de licencia libre, gratuita o propietaria, puesto que implican un evidente riesgo de daño a los sistemas y perjuicio a la institución. Por software ilegal se entiende cualquier aplicación informática, archivo, imagen, documento, salvapantallas o programa cuya licencia de uso no sea de titularidad de la Contraloría General del Estado. La Dirección Nacional de Tecnología de la Información y Comunicaciones evaluará y autorizará la instalación de software;

f) Instalar, enviar o utilizar aplicaciones informáticas, archivos, imágenes, documentos o programas con contenido ofensivo, inapropiado y/o discriminatorio; en particular, emplear protectores de pantalla, fotos, videos, animaciones o cualquier otro medio de reproducción o visualización con contenido que pueda ser considerado como material de acoso o intimidación en el trabajo;

g) Averiar, dañar o deteriorar intencionalmente las partes y piezas de los equipos informáticos, incluidos puertos USB, entradas y salidas de audio, video, datos y puntos de red;

h) Realizar análisis del flujo de información que pasa por la red (decodificación de paquetes o utilización de sniffers) así como detección de vulnerabilidades de la red y/o equipo de cómputo; y, en definitiva, cualquier forma de ataque o que pretenda acceder a información no autorizada;

i) Acceder, disponer o manipular, sin la correspondiente autorización, repositorios de archivos o bases de datos que contengan información confidencial o reservada;

j) Ausentarse del puesto de trabajo sin bloquear o apagar el computador asignado;

k) Borrar de los equipos y herramientas informáticas archivos, programas; y, en general, cualquier información que tenga relación con la entidad;

l) Operar equipos informáticos no asignados al servidor público para obtener archivos y cualquier otra información en ellos almacenada, o en la red informática de la institución, sin contar con la autorización por escrito del respectivo titular de la unidad administrativa, o por medio de los procedimientos establecidos por la Dirección Nacional de Tecnología de la Información y Comunicaciones para estos efectos;

m)Conectarse a la red con equipos que no sean de propiedad de la Contraloría General del Estado, sin la debida autorización conforme a los términos establecidos por la Dirección Nacional en cuestión;

n) Ejecutar cualquier actividad que afecte perjudicialmente el regular desempeño de las funciones y actividades del resto de servidores públicos y usuarios de red;

o) Utilizar los equipos informáticos institucionales para almacenar y/o manipular documentos ajenos a las funciones y actividades asignadas; y, especialmente, aquellos que contengan material considerado de distracción u ocio; y,

p) Almacenar en los equipos informáticos asignados cualquier archivo o documento de dudosa condición y/o calidad, que pueda ocasionar daños, tanto procedente de internet, como introducido al computador mediante dispositivos de almacenamiento externo (discos duros externos, memorias flash USB, entre otros) de los cuales no se tenga certeza de que están libres de malware.

Art. 39.- Correo electrónico institucional. - Constituye una herramienta autorizada tanto para las actividades de control y auditoría, determinación de responsabilidades, como para las labores de carácter técnico y administrativo de soporte. No obstante, a efectos de evitar eventuales riesgos ocasionados por su inadecuada utilización, se acatarán tanto las disposiciones pertinentes contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.

CAPITULO III
MARCO METODOLÓGICO

3.1 Descripción del área de estudio

La Contraloría General del Estado es la máxima institución de control fiscal del estado ecuatoriano. Es una entidad de carácter nacional con jurisdicción en todo el territorio, es decir en las 24 provincias que lo constituyen. Este organismo controla el buen uso de los recursos estatales a través de auditorías gubernamentales en las entidades públicas y privadas que gestionen fondos y/o bienes públicos. Ejerce sus funciones enmarcada en la autonomía administrativa, financiera, presupuestaria y organizativa que le confiere la Constitución de la República.

Misión

Controlar el uso eficiente y eficaz de los recursos estatales a través de la auditoría gubernamental, contribuyendo al fortalecimiento de la administración pública, en beneficio de la sociedad.

Visión

Ser la entidad fiscalizadora superior de control confiable, moderna y efectiva que, a través de la innovación y con personal capacitado, contribuya al mejoramiento de la administración pública, la buena gobernanza, la transparencia y la lucha contra la corrupción; comprometidos con los intereses ciudadanos y los objetivos nacionales.

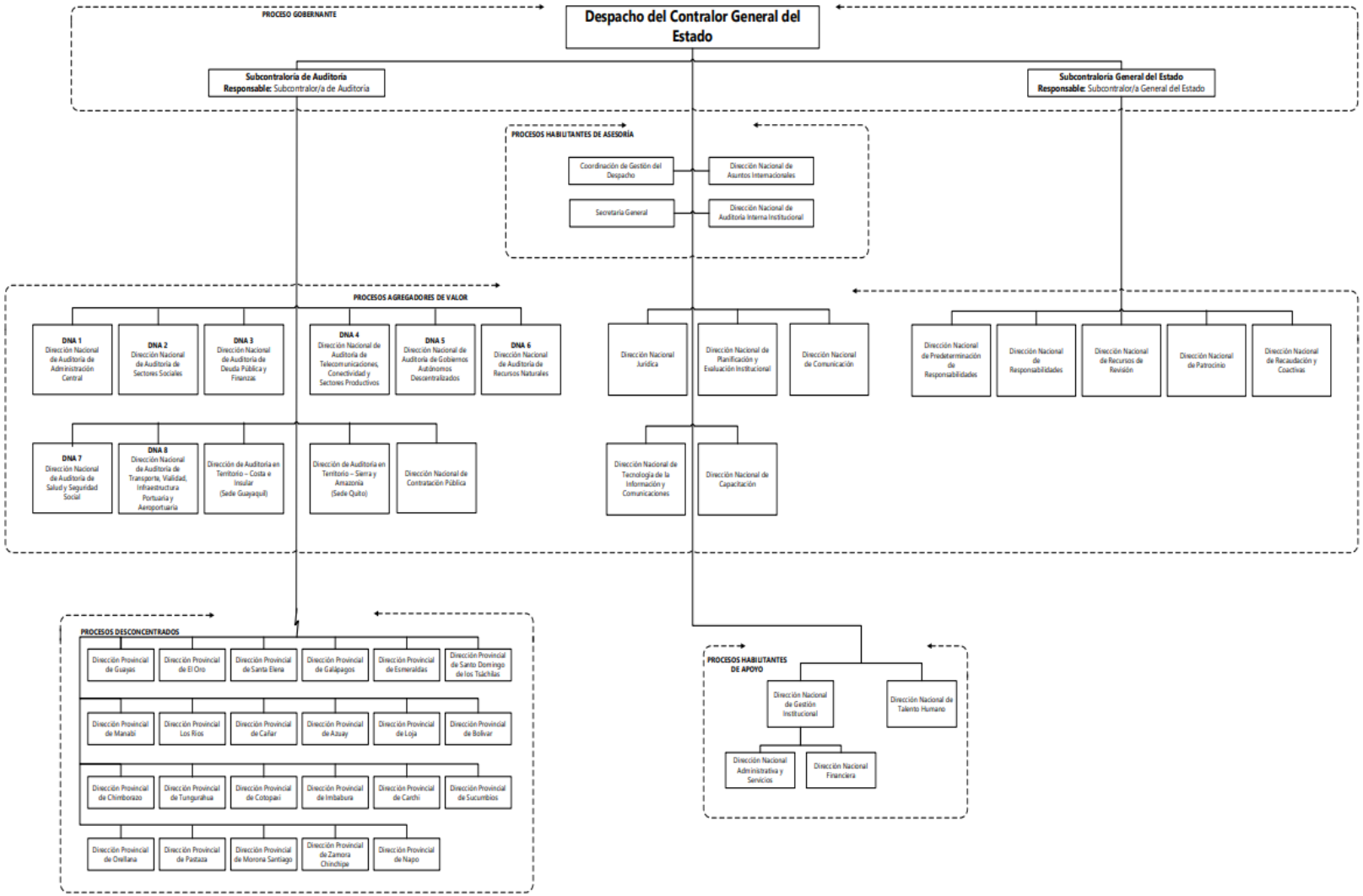
Objetivos estratégicos

- Incrementar la participación ciudadana en el control público.
- Fortalecer la gestión de control y juzgamiento.
- Fortalecer las capacidades institucionales.

Organigrama

Figura 11

Organigrama CGE

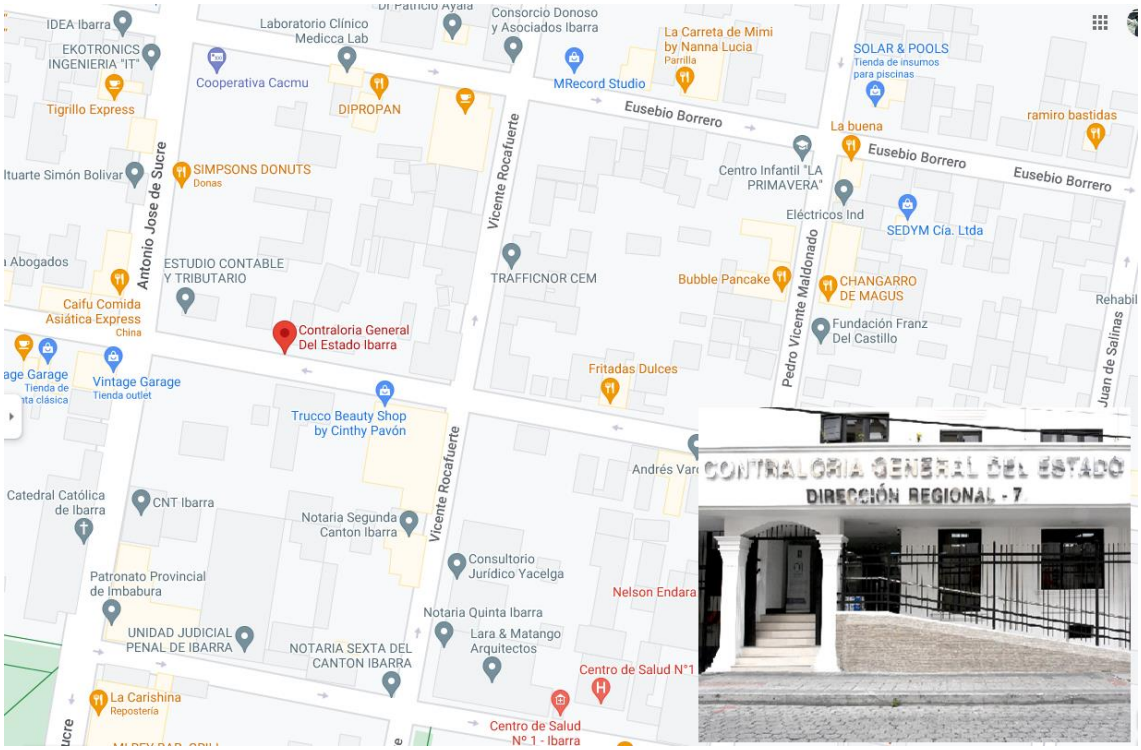


Nota. Adaptado de [Contraloría General del Estado - Inicio (contraloria.gob.ec)]

Para este proyecto se desarrolló el plan de formación de seguridad informática en uno de los procesos desconcentrados de la Contraloría General de Estado, específicamente en la Dirección Provincial de Imbabura, la cual cuenta con cincuenta y cinco funcionarios, con el fin de mitigar los riesgos de seguridad de la información y evitar la materialización de las amenazas que tiene la Institución en seguridad informática.

Figura 12

Ubicación CGE-DPI



Nota. Adaptado de Google Maps.

El programa fue desarrollado hasta la fase de evaluación, los posteriores análisis y actualizaciones depende de la Institución y la persona que designen para tal rol.

3.2 Enfoque y tipo de investigación

El presente programa fue desarrollado bajo un enfoque cuantitativo. Se realizó una recopilación e interpretación de los datos obtenidos de la formación que se llevó a cabo, así como la validación del programa propuesto.

Se utilizó una investigación de campo para la obtención de la información necesaria para el desarrollo del programa de formación, a través de las diferentes técnicas de este tipo de investigación: observación, encuestas, entrevistas, etc.

3.3 Procedimiento de investigación

Fase I: Recopilación de datos

Para la obtención de los datos se utilizaron las siguientes técnicas que posee la investigación de campo:

- Observación. – se utilizó esta técnica de manera participante, involucrándose en el tema de estudio y compartiendo las experiencias en materia de seguridad informática.
- Encuesta. – se aplicó esta técnica en base a un cuestionario digital previamente elaborado, lo cual permitió alcanzar a la gran mayoría de funcionarios de la Institución.

Fase II: Análisis de datos

Se realizó un análisis de los datos obtenidos, y de esta forma se interpretaron los datos de las principales amenazas que podrían haberse presentado dentro de la Institución, así como el nivel de conocimiento sobre seguridad informática que tenía en ese momento el personal.

Fase III: Identificación

En esta fase se estableció una línea de base de los riesgos de seguridad que pueden afectar a la Institución. También se definieron las herramientas y recursos a utilizar.

Fase IV: Desarrollo

Se definieron los temas y puntos clave para la estructuración y desarrollo del programa de formación sobre seguridad informática para la Contraloría General del Estado – Dirección Provincial de Imbabura, de acuerdo a los resultados obtenidos en la fase anterior, y se utilizó como recurso para el desarrollo e implementación la herramienta Moodle.

Fase V: Evaluación

Se evaluaron los resultados del programa propuesto, con la finalidad de evidenciar la efectividad que generó en los servidores de la Contraloría General del Estado – Dirección Provincial de Imbabura.

3.4 Consideraciones bioéticas

No se tienen consideraciones bioéticas debido a que esta investigación no realizó ninguna modificación o experimentación con elementos naturales y/o su información genética.

CAPITULO IV

MARCO ADMINISTRATIVO

4.1 Recursos

Los recursos que se emplearon en este proyecto son:

4.1.1 Bienes

- Materiales de Oficina
- Equipos de computación
- Software

4.1.2. Servicios

- Internet

4.1.3. Humanos

- Investigador
- Autoridades Institucionales
- Servidores de la Contraloría General del Estado – Dirección Provincial de Imbabura

4.1.4 Económicos

- Moodle Cloud para 50 usuarios, 500 MB de Almacenamiento

  Costo anual $180

4.2 Cronograma de actividades

Tabla 1

Cronograma de actividades

Actividades	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**
Realizar un marco conceptual de las amenazas de seguridad informática, para la protección de activos de información en la CGE-DPI.	X					
Determinar el nivel de conocimiento de los funcionarios de la CGE-DPI mediante observación y encuesta.	X					
Analizar e interpretar los datos obtenidos.	X	X				
Definir las amenazas que puedan afectar a la seguridad informática en la Institución.		X	X			

Estructurar el programa de formación de acuerdo a la publicación Nist SP 850.	X	X			
Implementar el programa de formación a los servidores de la Institución.		X	X		
Evidenciar la efectividad que generó el programa. (post-implementación)					X

Nota. Esta tabla muestra las actividades a realizar para el programa de formación.

CAPITULO V
DESARROLLO

5.1 Diseño del programa de formación

5.1.1 Evaluación de necesidades

En este punto se pudo determinar las necesidades más críticas de formación en cuanto a temas de seguridad informática se refiere, mediante el análisis del conocimiento general que tenían los funcionarios previo a la implementación del programa de formación, además del análisis de las amenazas a los activos de información relevantes de la CGE-DPI.

Nivel de conocimiento pre-implementación

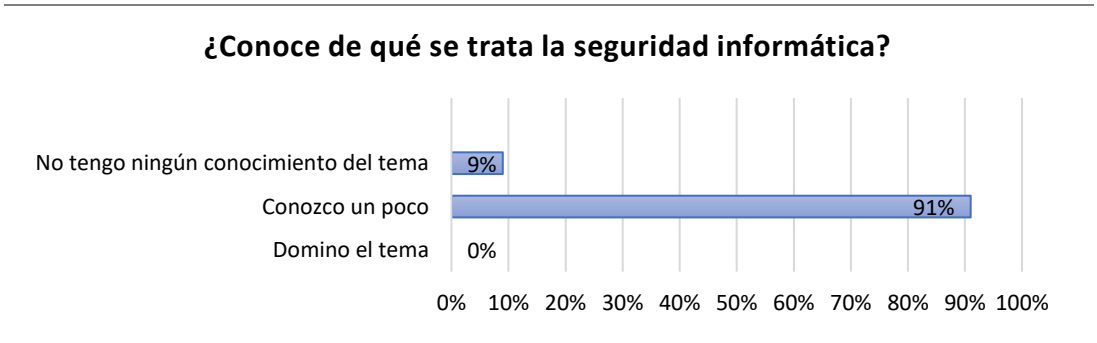
Para determinar el nivel de conocimiento pre- implementación, se utilizaron dos de las técnicas que posee la investigación de campo: la encuesta y la observación.

Se elaboró una encuesta mediante Microsoft Forms, con dieciséis preguntas relacionadas con los siguientes temas: Aspectos básicos de seguridad, Malware, Ingeniería Social, Correos y sitios web fraudulentos, Gestión de contraseñas, Políticas institucionales de seguridad, Redes sociales, Buenas prácticas de seguridad.

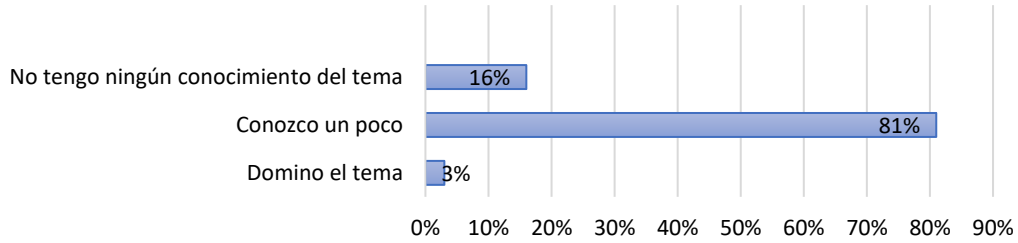
El formulario se configuró con respuestas cerradas, para determinar el nivel de conocimiento que tenían los funcionarios de la CGE-DPI previo al programa de formación, el cual fue respondido por un total de treinta y dos participantes. Cabe señalar que el programa estuvo enfocado a personas que no tienen formación técnica en el área de tecnología de la información.

Tabla 2

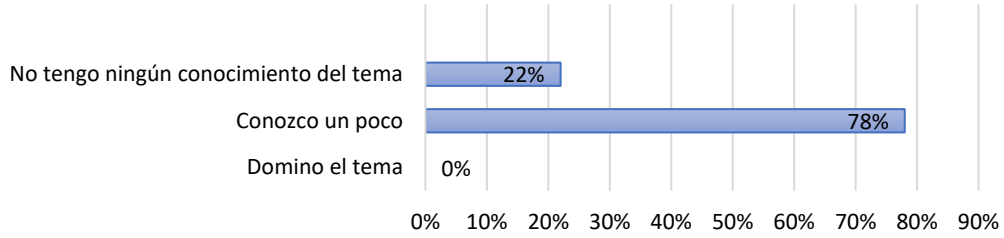
Resultados de la encuesta - nivel de conocimiento



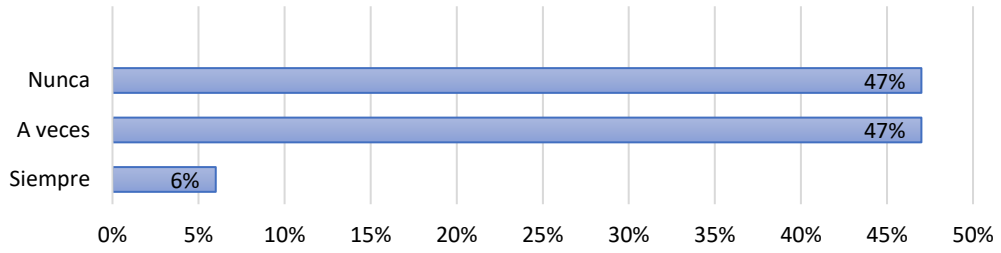
¿Sabe lo qué es un ataque informático?



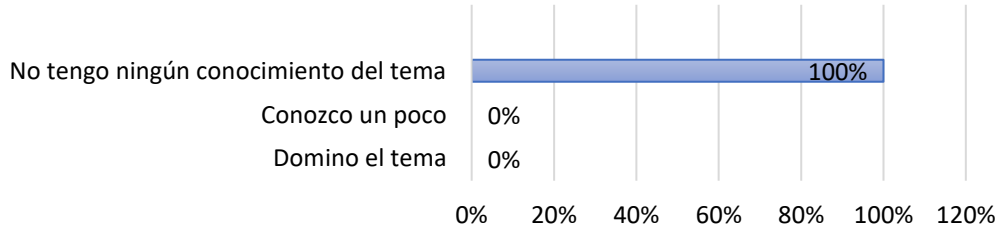
¿Conoce lo qué es un ciberdelincuente?



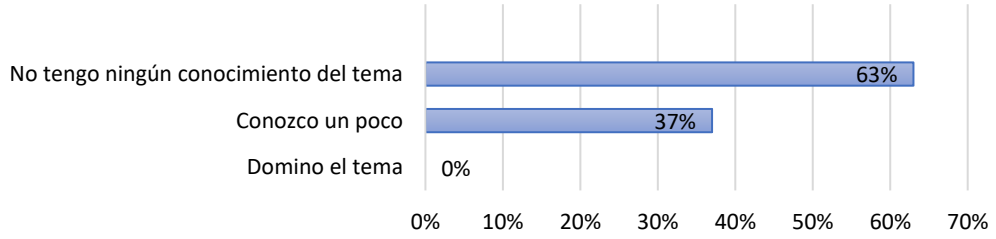
¿Generalmente escanea un dispositivo usb con el antivirus antes de utilizarlo?



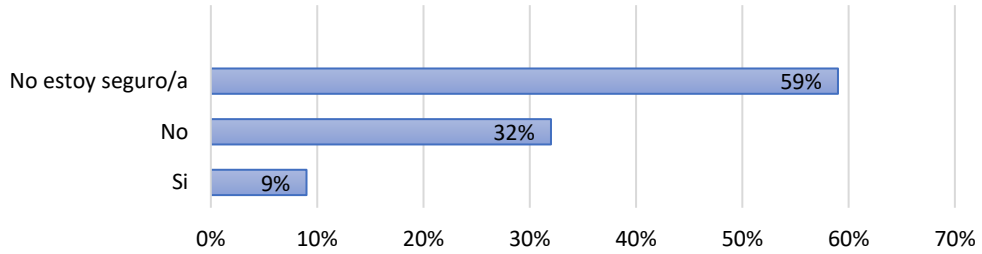
¿Conoce qué es el ransomware?



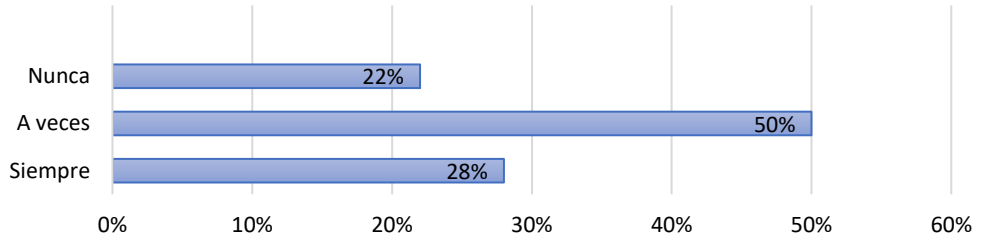
¿Conoce de qué se trata un ataque de phishing?



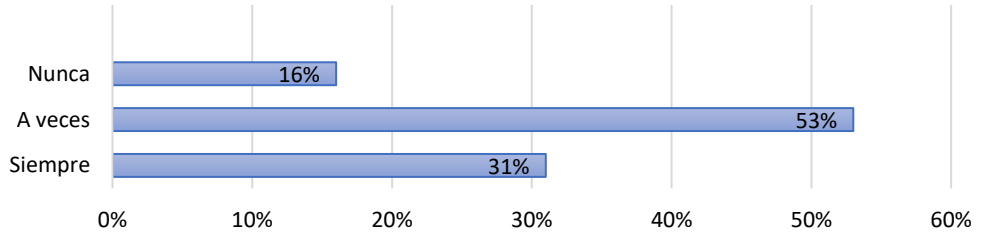
¿Podría reconocer una página web fraudulenta?



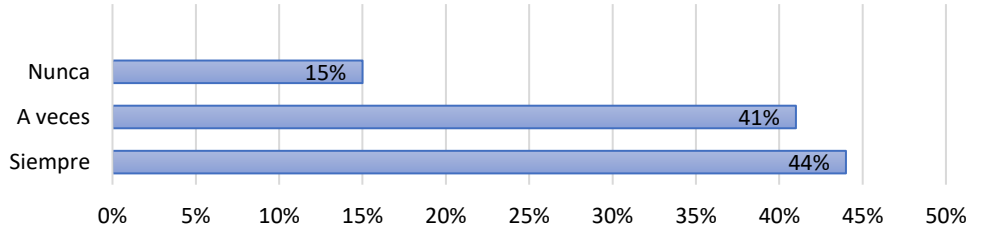
¿Verifica el remitente de sus correos electrónicos, antes de abrir enlaces o descargar archivos adjuntos?



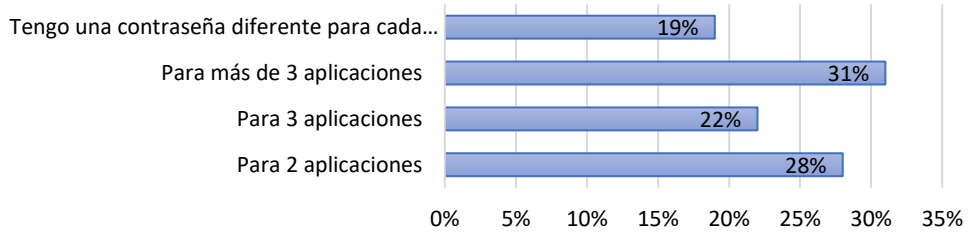
¿Bloquea o cierra sus sesión cuando abandona momentáneamente su estación de trabajo?



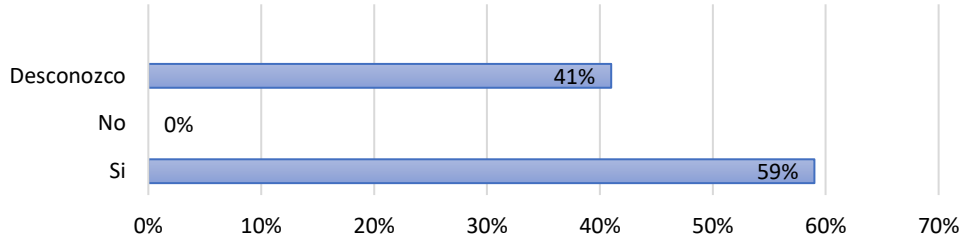
¿Generalmente guarda las contraseñas en uno o varios de estos lugares? (notas, cuaderno, teléfono, archivos de texto, fotografías, navegador web)



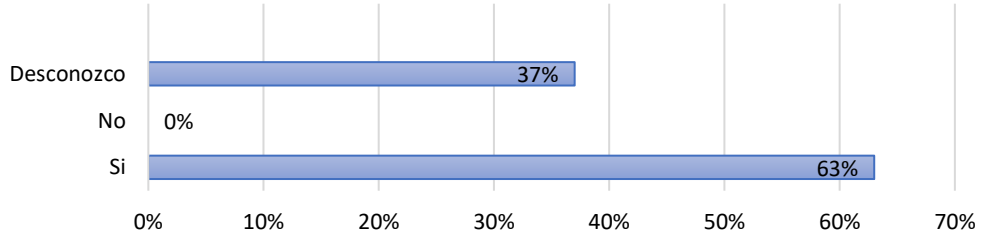
¿Reutiliza la misma contraseña para sus aplicaciones? (cuentas institucionales, personales)



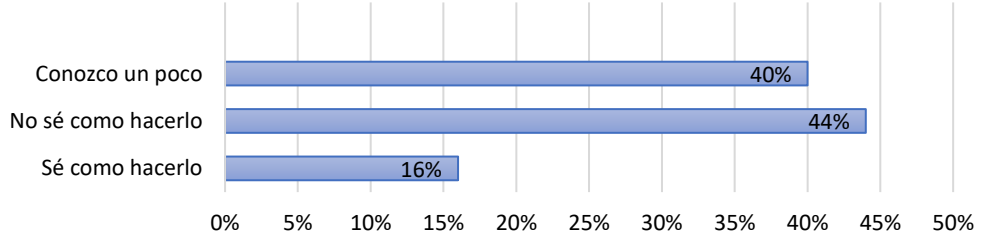
¿La Contraloría General del Estado cuenta con políticas de seguridad informática?

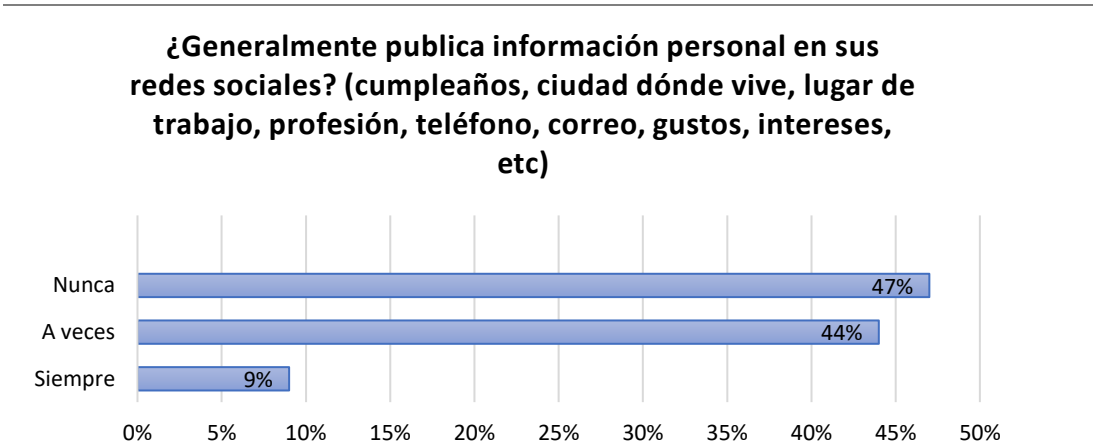


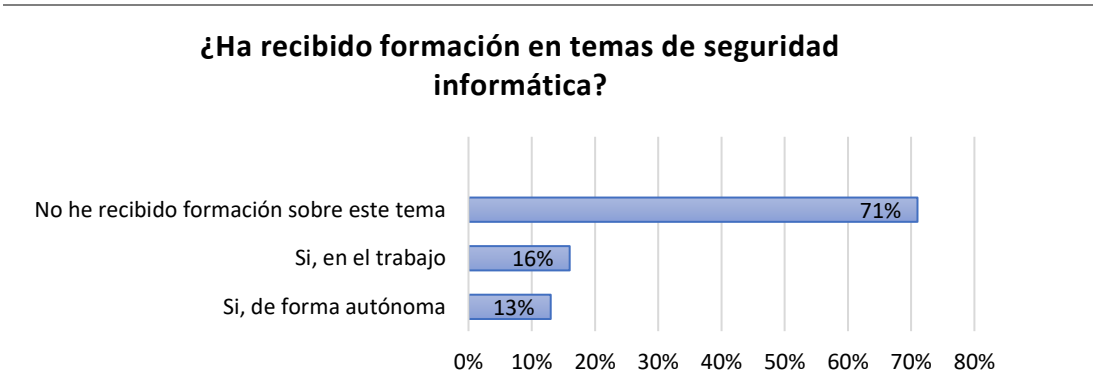
¿En la CGE existen directrices para el uso seguro de los equipos y manejo adecuado de la información?



¿Conoce cómo establecer la privacidad de la información de sus redes sociales? (Ej. Facebook, Instagram, Whatsapp)



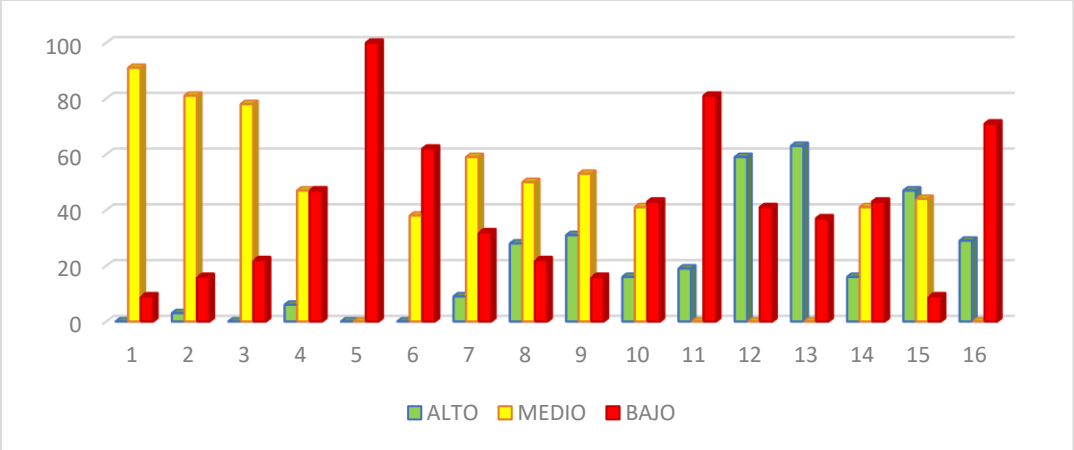




Nota. Esta tabla muestra los resultados obtenidos por cada pregunta de la encuesta.

Figura 13

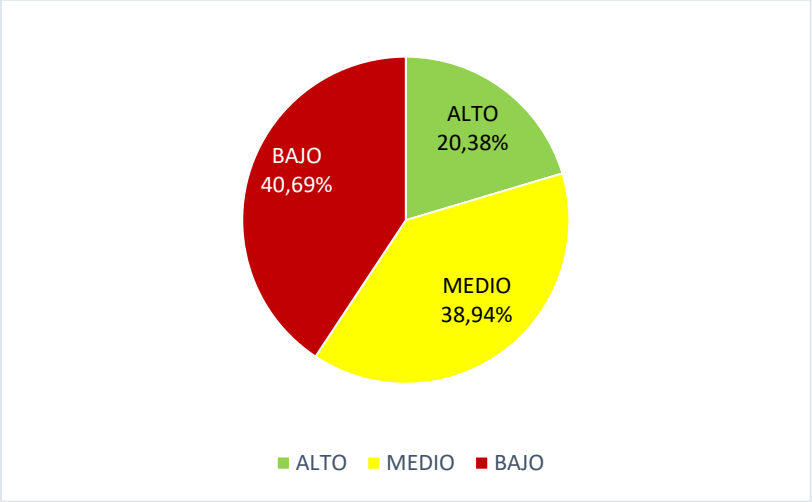
Nivel de conocimiento por pregunta



Nota. Gráfica de nivel de conocimiento por pregunta.

Figura 14

Nivel de conocimiento general



Nota. Gráfica de nivel de conocimiento general

Activos de información

Se realizó una identificación de los activos de información de la CGE-DPI y se estableció su valoración en términos de confidencialidad, integridad, disponibilidad y autenticación, considerando la importancia del activo para la Institución. Para esta actividad se utilizó la metodología Magerit, la cual se enfoca en un análisis cualitativo.

- **Identificación-valoración de activos**

Tabla 3

Identificación-Valoración de activos

ACTIVOS	C	I	D	A	VALOR DEL ACTIVO	VALOR DEL ACTIVO
1. [info] [classified] INFORMACIÓN-DATOS CLASIFICADOS	10	10	9	8	9,25	MUY ALTO
2. [d] [password] DATOS-CREDENCIALES	10	8	7	9	8,5	ALTO
3. [s] [email] SERVICIOS-CORREO ELECTRÓNICO	7	6	8	7	7	MEDIO
4. [sw] [os] APLICACIONES-SISTEMA OPERATIVO	8	7	5	6	6,5	MEDIO
5. [sw] [av] APLICACIONES-ANTIVIRUS	6	7	5	3	5,25	MEDIO
6. [hw] [pc] HARDWARE-COMPUTADORAS PERSONALES	9	7	8	6	7,5	ALTO

MA > 9
A <= 9
M <= 7
B <= 4
MB < 1

7. [hw] [network] HARDWARE-DISPOSITIVOS DE RED (switch, router, access point)	7	6	9	9	7,75	**ALTO**
8. [com] [wifi] [lan] COMUNICACIÓN-RED INALÁMBRICA-RED LOCAL	8	6	10	8	8	**ALTO**
9. [com] [internet] COMUNICACIÓN-INTERNET	7	7	9	6	7,25	**ALTO**
10. [media] [electronic][disk] [usb] DISCOS EXTERNOS-DISPOSITIVOS USB	4	5	4	2	3,75	**BAJO**
11. [l] [building] INSTALACIONES-EDIFICIO	8	8	9	1	6,5	**MEDIO**
12. [p] [ui] PERSONAL-USUARIOS INTERNOS	9	9	6	5	7,25	**ALTO**

Nota. Esta tabla muestra los activos de la CGE-DPI y su valoración.

- **Identificación de amenazas**

Tabla 4

Identificación de amenazas

ACTIVOS	AMENAZAS
1. [info] [classified] INFORMACIÓN-DATOS CLASIFICADOS	1.1 [E.1] Errores de los usuarios
	1.2 [E.14] Escapes de información
	1.3 [A.15] Modificación de la información
	1.4 [A.17] Corrupción de la información
	1.5 [A.19] Divulgación de información
	1.6 [A.11] Acceso no autorizado
2. [d] [password] DATOS-CREDENCIALES	2.1 [E.1] Errores de los usuarios
	2.2 [A.11] Acceso no autorizado
	2.3 [A.19] Divulgación de información
3. [s] [email] SERVICIOS-CORREO ELECTRÓNICO	3.1 [E.1] Errores de los usuarios
	3.2 [A.5] Suplantación de la identidad del usuario
	3.3 [A.7] Uso no previsto
	3.4 [A.11] Acceso no autorizado
	3.5 [A.13] Repudio
4. [sw] [os] APLICACIONES-SISTEMA OPERATIVO	4.1 [E.1] Errores de los usuarios
	4.2 [A.8] Difusión de software dañino
	4.3 [E.21] Errores de mantenimiento / actualización
	4.4 [A.5] Suplantación de la identidad del usuario
	4.5 [A.7] Uso no previsto
	4.6 [A.11] Acceso no autorizado
	4.7 [A.22] Manipulación de programas
5. [sw] [av] APLICACIONES-ANTIVIRUS	5.1 [E.1] Errores de los usuarios
	5.2 [A.8] Difusión de software dañino
	5.3 [E.21] Errores de mantenimiento / actualización

	5.4 [A.5] Suplantación de la identidad del usuario
	5.5 [A.7] Uso no previsto
	5.6 [A.11] Acceso no autorizado
	5.7 [A.22] Manipulación de programas
6. [hw] [pc] HARDWARE-COMPUTADORAS PERSONALES	6.1 [E.1] Errores de los usuarios
	6.2 [E.23] Errores de mantenimiento / actualización de equipos
	6.3 [A.7] Uso no previsto
	6.4 [A.11] Acceso no autorizado
	6.5 [A.25] Robo
	6.6 [A.26] Ataque destructivo
7. [hw] [network] HARDWARE-DISPOSITIVOS DE RED (switch, router, access point)	7.1 [E.2] Errores del administrador
	7.2 [E.23] Errores de mantenimiento / actualización de equipos
	7.3 [A.7] Uso no previsto
	7.4 [A.11] Acceso no autorizado
	7.5 [A.25] Robo
	7.6 [A.26] Ataque destructivo
8. [com] [wifi] [lan] COMUNICACIÓN-RED INALÁMBRICA-RED LOCAL	8.1 [E.1] Errores de los usuarios
	8.2 [E.24] Caída del sistema por agotamiento de recursos
	8.3 [A.5] Suplantación de la identidad del usuario
	8.4 [A.7] Uso no previsto
	8.5 [A.11] Acceso no autorizado
9. [com] [internet] COMUNICACIÓN-INTERNET	9.1 [E.4] Errores de configuración
	9.2 [A.5] Suplantación de la identidad del usuario
	9.3 [A.7] Uso no previsto
	9.4 [A.11] Acceso no autorizado
10. [media] [electronic][disk] [usb] DISCOS EXTERNOS-DISPOSITIVOS USB	10.1 [A.11] Acceso no autorizado
	10.2 [A.26] Ataque destructivo
	10.3 [A.25] Robo
11. [l] [building] INSTALACIONES-EDIFICIO	11.1 [N.*] Desastres naturales
	11.2 [A.7] Uso no previsto
	11.3 [A.11] Acceso no autorizado
	11.4 [A.26] Ataque destructivo
12. [p] [ui] PERSONAL-USUARIOS INTERNOS	12.1 [E.7] Deficiencias en la organización
	12.2 [E.28] Indisponibilidad del personal
	12.3 [A.29] Extorsión
	12.4 [A.30] Ingeniería social

Nota. Esta tabla muestra las amenazas para cada activo.

- **Impacto**

Tabla 5

Determinación del impacto potencial

IMPACTO		DEGRADACIÓN				
		MA	A	M	B	MB
VALOR DEL ACTIVO	MA	MA	MA	A	A	M
	A	MA	A	A	M	M
	M	A	A	M	M	B
	B	A	M	M	B	B
	MB	M	M	B	B	MB

Nota. Esta tabla muestra cómo se determinó el impacto.

- **Riesgo**

Tabla 6

Determinación del riesgo potencial

RIESGO		PROBABILIDAD				
		MA	A	M	B	MB
IMPACTO	MA	MA	MA	A	A	M
	A	MA	A	A	M	M
	M	A	A	M	M	B
	B	A	M	M	B	B
	MB	M	M	B	B	MB

Nota. Esta tabla muestra cómo se determinó el riesgo.

Tabla 7

Análisis final

ACTIVO	AMENAZA	VALOR DEL ACTIVO	DEGRADACIÓN	IMPACTO	PROBABILIDAD	RIESGO
1. **[info] [classified] INFORMACIÓN-DATOS CLASIFICADOS**	**1.1** [E.1] Errores de los usuarios	MA	MA	MA	A	MA
	1.2 [E.14] Escapes de información		B	A	B	M
	1.3 [A.15] Modificación de la información		M	A	B	M
	1.4 [A.17] Corrupción de la información		M	A	B	M
	1.5 [A.19] Divulgación de información		M	A	B	M
	1.6 [A.11] Acceso no autorizado		A	MA	M	A
	2.1 [E.1] Errores de los usuarios		MA	MA	A	MA

2. **[d] [password] DATOS-CREDENCIALES**	**2.2** [A.11] Acceso no autorizado	A	M	A	M	A
	2.3 [A.19] Divulgación de información		A	A	A	A
3. **[s] [email] SERVICIOS-CORREO ELECTRÓNICO**	**3.1** [E.1] Errores de los usuarios	M	MA	A	MA	MA
	3.2 [A.5] Suplantación de la identidad del usuario		A	A	B	M
	3.3 [A.7] Uso no previsto		B	M	M	M
	3.4 [A.11] Acceso no autorizado		M	M	M	M
	3.5 [A.13] Repudio		M	M	A	A
4. **[sw] [os] APLICACIONES-SISTEMA OPERATIVO**	**4.1** [E.1] Errores de los usuarios	M	A	A	A	A
	4.2 [A.8] Difusión de software dañino		M	M	B	M
	4.3 [E.21] Errores de mantenimiento / actualización		B	M	MB	B
	4.4 [A.5] Suplantación de la identidad del usuario		M	M	B	M
	4.5 [A.7] Uso no previsto		B	M	M	M
	4.6 [A.11] Acceso no autorizado		M	M	M	M
	4.7 [A.22] Manipulación de programas		M	M	M	M
5. **[sw] [av] APLICACIONES-ANTIVIRUS**	**5.1** [E.1] Errores de los usuarios	M	M	M	A	A
	5.2 [A.8] Difusión de software dañino		B	M	B	M
	5.3 [E.21] Errores de mantenimiento / actualización		B	M	MB	B
	5.4 [A.5] Suplantación de la identidad del usuario		B	M	B	M
	5.5 [A.7] Uso no previsto		MB	B	B	B
	5.6 [A.11] Acceso no autorizado		M	M	M	M
	5.7 [A.22] Manipulación de programas		M	M	M	M
6. **[hw] [pc] HARDWARE-COMPUTADORAS PERSONALES**	**6.1** [E.1] Errores de los usuarios	A	MA	MA	A	MA
	6.2 [E.23] Errores de mantenimiento / actualización de equipos		M	A	MB	M
	6.3 [A.7] Uso no previsto		A	A	B	M
	6.4 [A.11] Acceso no autorizado		A	A	M	A
	6.5 [A.25] Robo		MA	MA	B	A
	6.6 [A.26] Ataque destructivo		A	A	MB	M
	7.1 [E.2] Errores del administrador		A	A	MB	M
	7.2 [E.23] Errores de mantenimiento / actualización de equipos		M	A	MB	M

7. **[hw] [network] HARDWARE-DISPOSITIVOS DE RED (switch, router, access point)**	**7.3** [A.7] Uso no previsto	A	M	A	MB	M
	7.4 [A.11] Acceso no autorizado		A	A	MB	M
	7.5 [A.25] Robo		M	A	B	M
	7.6 [A.26] Ataque destructivo		A	A	MB	M
8. **[com] [wifi] [lan] COMUNICACIÓN-RED INALÁMBRICA-RED LOCAL**	**8.1** [E.1] Errores de los usuarios	A	M	A	M	A
	8.2 [E.24] Caída del sistema por agotamiento de recursos		M	A	M	A
	8.3 [A.5] Suplantación de la identidad del usuario		B	M	MB	B
	8.4 [A.7] Uso no previsto		M	A	A	A
	8.5 [A.11] Acceso no autorizado		A	A	MB	M
9. **[com] [internet] COMUNICACIÓN-INTERNET**	**9.1** [E.4] Errores de configuración	A	A	A	B	M
	9.2 [A.5] Suplantación de la identidad del usuario		M	A	MB	M
	9.3 [A.7] Uso no previsto		A	A	A	A
	9.4 [A.11] Acceso no autorizado		A	A	MB	M
10. **[media] [electronic][disk] [usb] DISCOS EXTERNOS-DISPOSITIVOS USB**	**10.1** [A.11] Acceso no autorizado	B	M	M	MB	B
	10.2 [A.26] Ataque destructivo		B	B	MB	B
	10.3 [A.25] Robo		B	B	B	B
11. **[l] [building] INSTALACIONES-EDIFICIO**	**11.1** [N.*] Desastres naturales	M	M	M	MB	B
	11.2 [A.7] Uso no previsto		MB	B	MB	B
	11.3 [A.11] Acceso no autorizado		M	M	MB	B
	11.4 [A.26] Ataque destructivo		A	A	MB	M
12. **[p] [ui] PERSONAL-USUARIOS INTERNOS**	**12.1** [E.7] Deficiencias en la organización	A	A	A	B	M
	12.2 [E.28] Indisponibilidad del personal		M	A	B	M
	12.3 [A.29] Extorsión		A	A	MB	M
	12.4 [A.30] Ingeniería social		A	A	A	A

Nota. Esta tabla muestra cómo se determinó el riesgo para los activos de la CGE-DPI.

En base a los resultados obtenidos de la encuesta, se pudo determinar que gran parte de los funcionarios de la CGE-DPI tienen un nivel de conocimiento **Bajo-Medio** con respecto a temas de seguridad informática.

De la misma manera, con los resultados del análisis de riesgos realizado a los activos de información de la CGE-DPI, se pudo observar que las amenazas directamente relacionadas a acciones de los usuarios, tienen un riesgo **Medio**, **Alto** y **Muy alto**.

De acuerdo a estos resultados, fue evidente la obligación de desarrollar un programa de formación de seguridad informática y se pudo determinar las principales necesidades de formación.

5.1.2 Estructuración del programa

De acuerdo a la NIST SP 800-50, se utilizó para la estructuración el "Modelo 2 - Modelo de Gestión de Programas Parcialmente Descentralizado", ya que este se ajusta a la organización de la Contraloría General del Estado.

En base a este modelo y los resultados obtenidos en la evaluación de necesidades, la estructura del programa de formación se estableció de la siguiente manera:

Tabla 8

Estructura del programa de formación

MÓDULOS	DESCRIPCIÓN
MÓDULO 1: Introducción a la Seguridad Informática	➢ ¿Qué es la Seguridad Informática?
	➢ ¿Qué protege la SI?
	➢ ¿De qué protege la SI?
	➢ ¿Qué es y por qué proteger los activos de información?
	➢ Pilares de la SI (Confidencialidad, Integridad, Disponibilidad)
	➢ Definiciones importantes (Ataque, ciberdelincuente, hacker)
MÓDULO 2: Vulnerabilidades y Amenazas	**Vulnerabilidades** (definición, razones frecuentes)
	Amenazas
	➢ Usuarios
	• Desconocimiento
	• Malas prácticas (contraseñas, acceso a redes públicas, privacidad información, enlaces, archivos adjuntos)
	➢ Malware
	• Ransomware (Caso CGE-DPI)
	• Virus
	• Troyanos
	• Gusanos
	• Keyloggers
	➢ Ingeniería social
	• Phishing
	• Vishing (Caso DPI-CGE)
	• Pharming

	➢ Ataque de Contraseñas (fuerza bruta, diccionario)
	➢ Correo malicioso
	➢ Seguridad física
MÓDULO 3: Phishing, Gestión de contraseñas	**Caso Práctico de Phishing** (Ejemplo práctico de como un ciberdelincuente obtiene las credenciales de acceso a través de la Ingeniería Social)
	Gestión de contraseñas
	• Contraseñas robustas
	• Reciclaje de contraseñas
	• Exposición contraseñas (notas físicas, digitales, guardadas en navegadores, compartir)
	• Errores al establecer una contraseña
	• Recomendaciones para establecer una buena contraseña
MÓDULO 4: Reglamento De Políticas de Seguridad de La Información de la CGE	➢ Acuerdo de confidencialidad
	➢ Uso y gestión de la contraseña
	➢ Acceso a los servicios de red, sistema operativo, internet
	➢ Acceso remoto, Cierre/Bloqueo de sesión
	➢ Uso de computadores portátiles y de escritorio, Dispositivos de almacenamiento extraíble
	➢ Correo electrónico
MÓDULO 5: Redes sociales, Buenas prácticas	➢ Privacidad (configuración)
	➢ Publicaciones (qué, dónde, quién)
	➢ Stalking
	➢ Buenas Prácticas de Seguridad Informática

Nota. Esta tabla muestra el contenido del programa de formación.

5.2 Desarrollo del material

Para el desarrollo del programa de formación de seguridad informática, se crearon guías y presentaciones para cada módulo del programa, además se adaptaron videos explicativos para tres puntos muy importantes del programa, un glosario de amenazas mediante la plataforma Genially y se utilizó el Reglamento de Políticas de Seguridad de la Información de la Contraloría General del Estado.

El material que se desarrolló para cada módulo se detalla mediante la siguiente tabla:

Tabla 9

Material del programa de formación

MÓDULOS	RECURSOS
MÓDULO 1: Introducción a la Seguridad Informática	-Guía Módulo 1.pdf -Presentación Módulo 1.pdf

MÓDULO 2: Vulnerabilidades y Amenazas	-Guía Módulo 2.pdf -Presentación Módulo 2.pdf -Amenazas informáticas (Plataforma Genially) -Video Ransomware
MÓDULO 3: Phishing, Gestión de contraseñas	-Guía Módulo 3.pdf -Video Contraseñas
MÓDULO 4: Reglamento De Políticas de Seguridad de La Información de la CGE	-Guía Módulo 4.pdf -Presentación Módulo 4.pdf -Acuerdo No. 018-CG-2021, REGLAMENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA CGE.pdf
MÓDULO 5: Redes sociales, Buenas prácticas	-Guía Módulo 5 Redes sociales.pdf -Guía Módulo 5 Buenas prácticas.pdf -Presentación Módulo 5.pdf -Video Stalking

Nota. Esta tabla muestra el material incluido en cada módulo del programa de formación.

Además, para la demostración práctica de un ataque de phishing, actividad establecida en el módulo 3 de este programa, se desarrolló una página web y se configuró un servidor local con Apache, Php y como base de datos Mysql.

Figura 15

Página educativa de Phishing

Nota. Página web educativa para demostración de phishing.

5.3 Implementación del programa

Para la implementación del programa de formación, se utilizaron dos de las técnicas que están establecidas en la NIST SP 800-50: mediante sesiones basadas en web y mediante sesiones presenciales dirigidas por un instructor.

Se utilizó como plataforma, el sistema de gestión de aprendizaje (LMS) Moodle Cloud, mismo que permitió crear un espacio de aprendizaje virtual, en el que se pudo evidenciar y recoger las actividades de los funcionarios de la CGE-DPI.

Para la retroalimentación e interacción con los funcionarios, se crearon foros para intercambio de opiniones, un crucigrama con conceptos básico de seguridad, un taller sobre Malware, además de tres evaluaciones parciales y una evaluación final para valorar los conocimientos adquiridos.

Tabla 10

Actividades de retroalimentación

MÓDULOS	ACTIVIDADES
MÓDULO 1: Introducción a la Seguridad Informática	-Foro 1 Ciberseguridad -Crucigrama
MÓDULO 2: Vulnerabilidades y Amenazas	-Taller 1 Cuadro comparativo Malware -Evaluación 1 Amenazas
MÓDULO 3: Phishing, Gestión de contraseñas	-Foro 2 Phishing -Evaluación 2 Contraseñas
MÓDULO 4: Reglamento De Políticas de Seguridad de La Información de la CGE	-Evaluación 3 Políticas CGE
MÓDULO 5: Redes sociales, Buenas prácticas	-Evaluación Final

Nota. Actividades para cada módulo, plataforma Moodle.

Figura 16

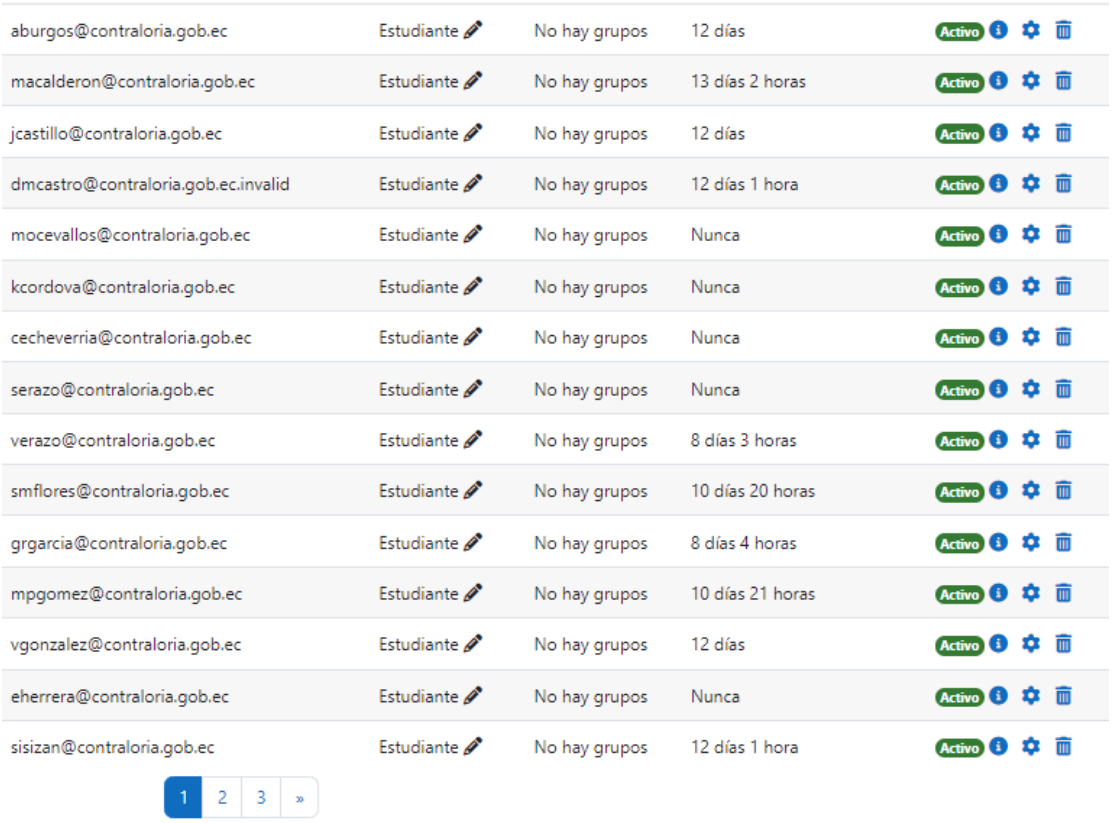
Plataforma Moodle

Nota. Programa de formación en plataforma Moodle.

Se crearon los usuarios de los participantes del programa de formación, los cuales se registraron y fueron asignados con el rol correspondiente de estudiante

Figura 17

Inscripción de participantes



aburgos@contraloria.gob.ec	Estudiante	No hay grupos	12 días	Activo
macalderon@contraloria.gob.ec	Estudiante	No hay grupos	13 días 2 horas	Activo
jcastillo@contraloria.gob.ec	Estudiante	No hay grupos	12 días	Activo
dmcastro@contraloria.gob.ec.invalid	Estudiante	No hay grupos	12 días 1 hora	Activo
mocevallos@contraloria.gob.ec	Estudiante	No hay grupos	Nunca	Activo
kcordova@contraloria.gob.ec	Estudiante	No hay grupos	Nunca	Activo
cecheverria@contraloria.gob.ec	Estudiante	No hay grupos	Nunca	Activo
serazo@contraloria.gob.ec	Estudiante	No hay grupos	Nunca	Activo
verazo@contraloria.gob.ec	Estudiante	No hay grupos	8 días 3 horas	Activo
smflores@contraloria.gob.ec	Estudiante	No hay grupos	10 días 20 horas	Activo
grgarcia@contraloria.gob.ec	Estudiante	No hay grupos	8 días 4 horas	Activo
mpgomez@contraloria.gob.ec	Estudiante	No hay grupos	10 días 21 horas	Activo
vgonzalez@contraloria.gob.ec	Estudiante	No hay grupos	12 días	Activo
eherrera@contraloria.gob.ec	Estudiante	No hay grupos	Nunca	Activo
sisizan@contraloria.gob.ec	Estudiante	No hay grupos	12 días 1 hora	Activo

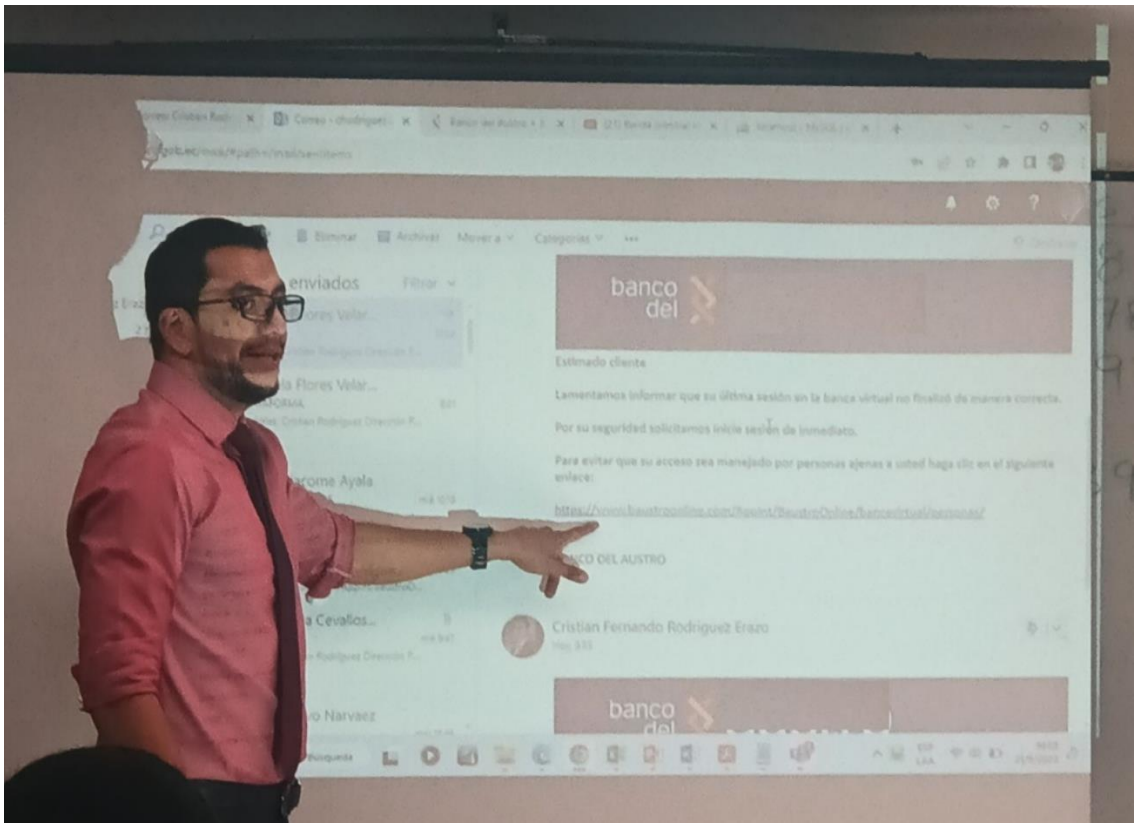
1 2 3 »

Nota. Pantalla de inscripción de participantes, plataforma Moodle.

Una vez concluido este proceso y con la debida autorización por parte de la Contraloría General del Estado, se procedió a impartir el programa de formación de seguridad informática en las instalaciones de la CGE-DPI, al personal de auditoría externa, auditoría interna y área administrativa.

Figura 18

Exposición del programa



Nota. Implementación del programa de formación

CAPITULO VI
RESULTADOS

6.1 Post implementación

Una vez finalizada la implementación, se procedió a realizar la evaluación de la efectividad del programa de formación, mediante el método de evaluación de Kirkpatrick, el cual se aplica en función de satisfacción, aprendizaje, aplicabilidad del conocimiento y resultados. Además, basándose en algunas de las técnicas que nos indica la NIST SP 800-50. (Encuestas, formularios de evaluación, reportes y observaciones independientes).

Figura 19

Técnicas de evaluación

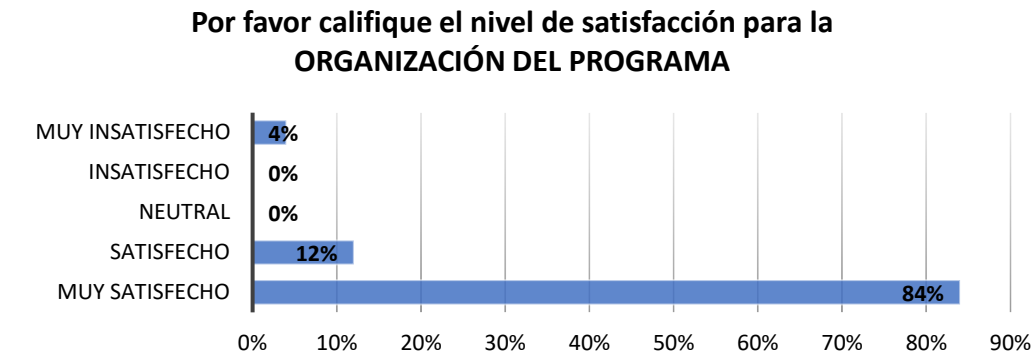
Nota. Técnicas de evaluación NIST SP 800-50

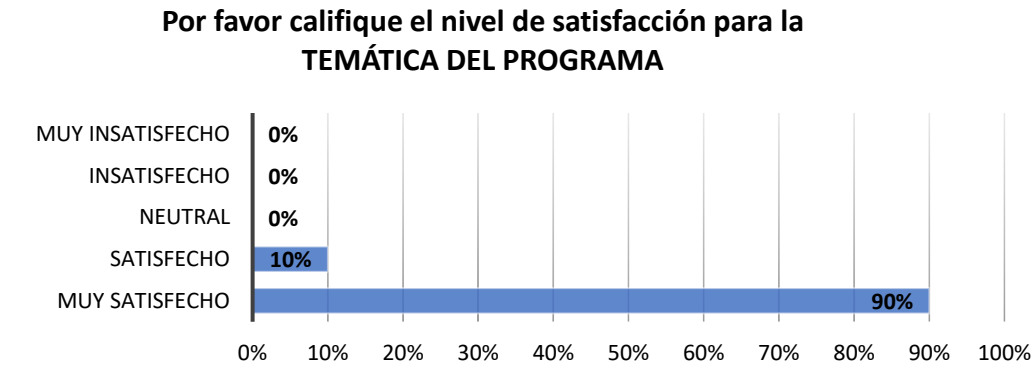
6.1.1 Satisfacción

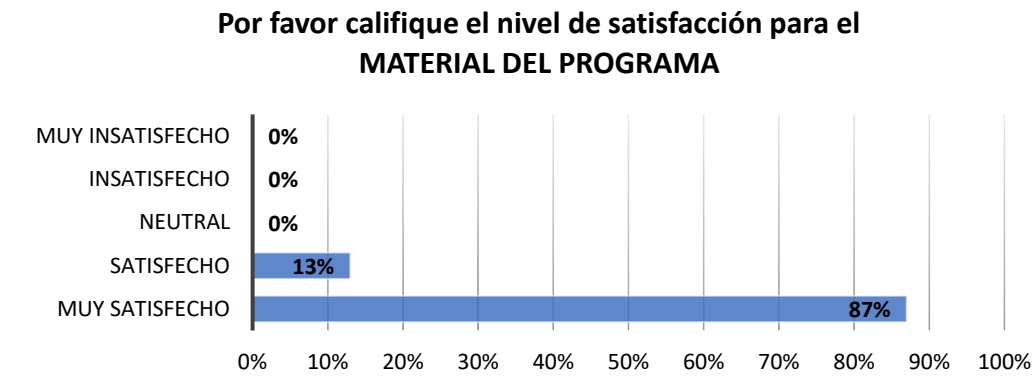
Para poder medir la reacción o grado de satisfacción de los participantes, se elaboró una encuesta mediante Microsoft Forms, con diez preguntas (nueve cerradas y una pregunta para recibir comentarios o sugerencias).

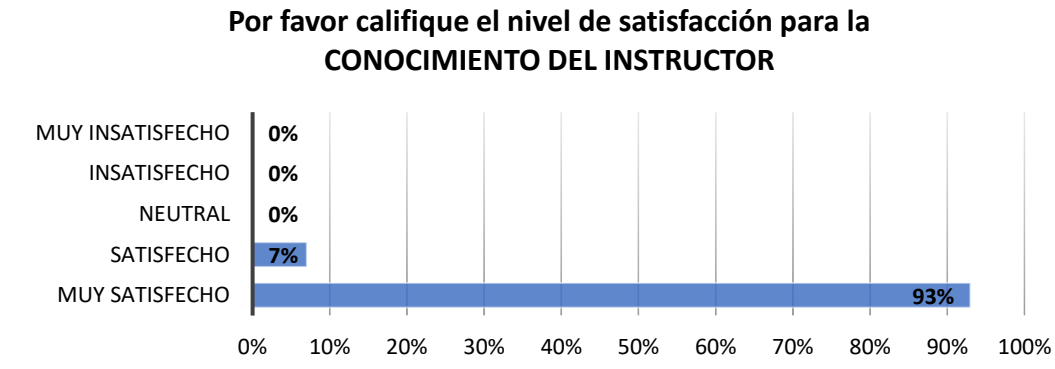
Tabla 11

Resultados de la encuesta - nivel de satisfacción

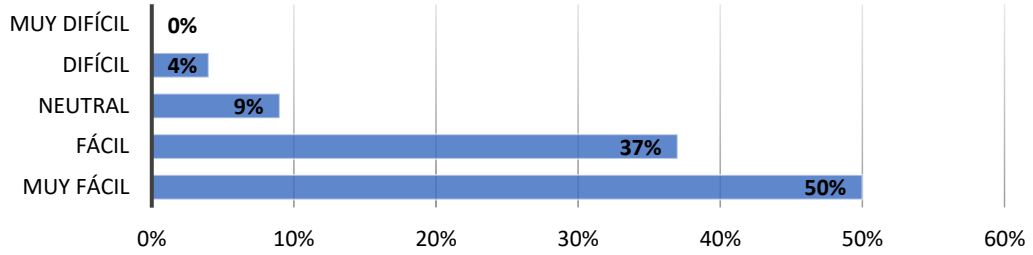




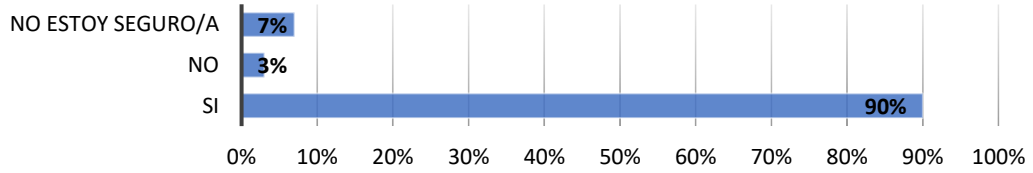




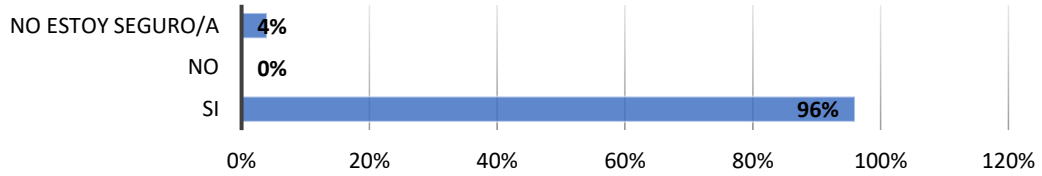
¿Qué tan fácil fue entender los términos que usaba el instructor?



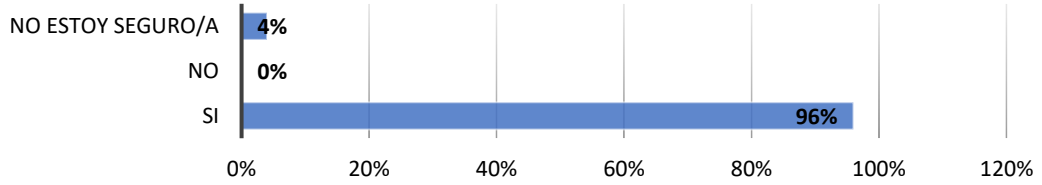
¿Cree que la duración del programa fue lo suficientemente buena como para satisfacer sus expectativas de formación?



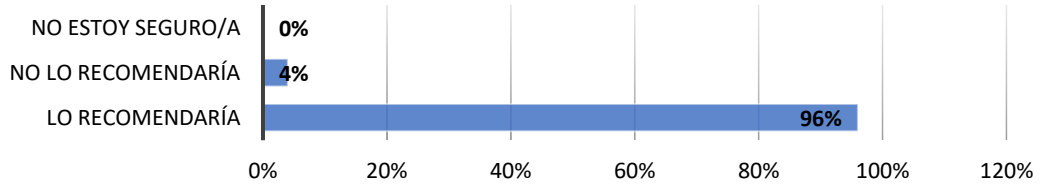
¿Se explicó claramente el objetivo del programa previo a su inicio?



¿El programa de formación le proporcionó aprendizajes prácticos y teóricos?



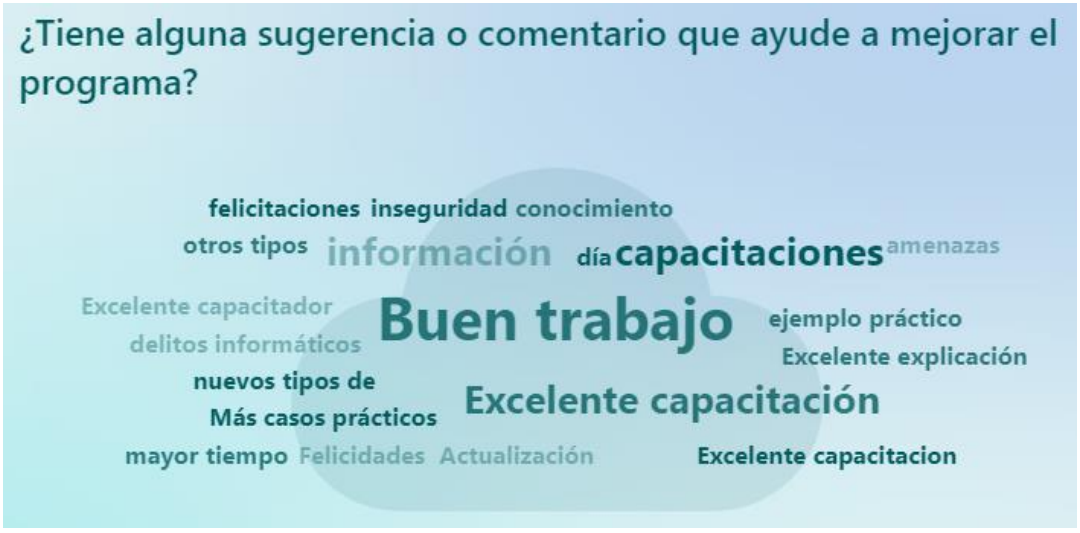
Considerando su experiencia completa con el programa, ¿Recomendaría replicar el programa de formación a los servidores de la CGE a nivel nacional?



Nota. Esta tabla muestra los resultados obtenidos por cada pregunta de la encuesta

Figura 20

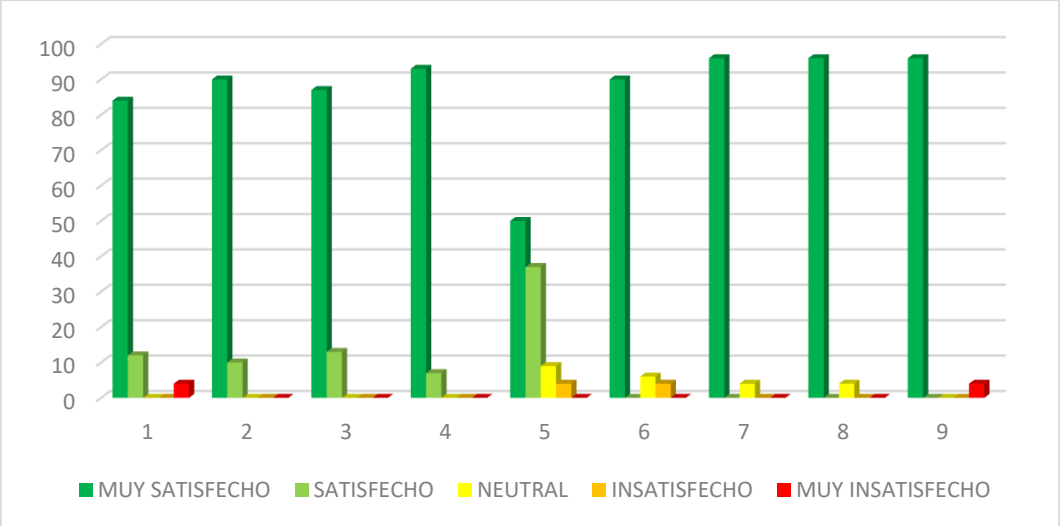
Pregunta abierta encuesta – nivel de satisfacción



Nota. Este gráfico muestra las sugerencias y comentarios enviados respecto al programa de formación.

Figura 21

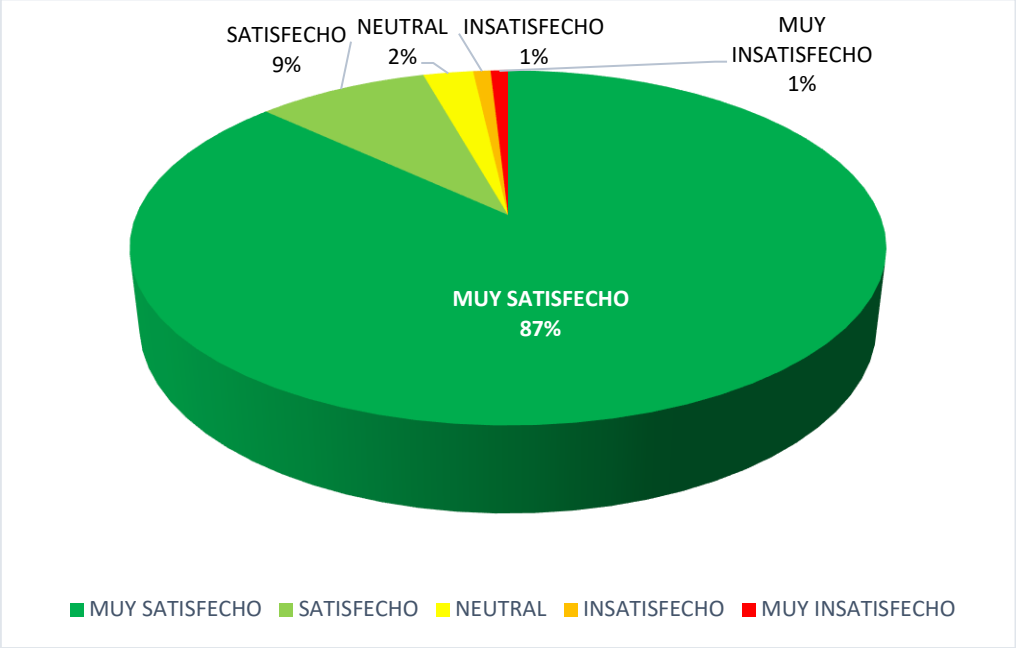
Nivel de satisfacción por pregunta



Nota. Nivel de satisfacción por cada pregunta

Figura 22

Nivel de satisfacción general



Nota. Nivel de satisfacción general

Los resultados arrojados por la encuesta indican que la gran mayoría de los participantes quedaron muy satisfechos con el programa de formación: la organización, la temática, el material y el conocimiento por parte del instructor, fueron aspectos muy bien valorados, además de recibir excelentes comentarios sobre el programa en general.

6.1.2 Aprendizaje

Se evaluó el conocimiento adquirido, mediante las actividades creadas en la plataforma Moodle (foros, taller y evaluaciones).

Tabla 12

Calificaciones

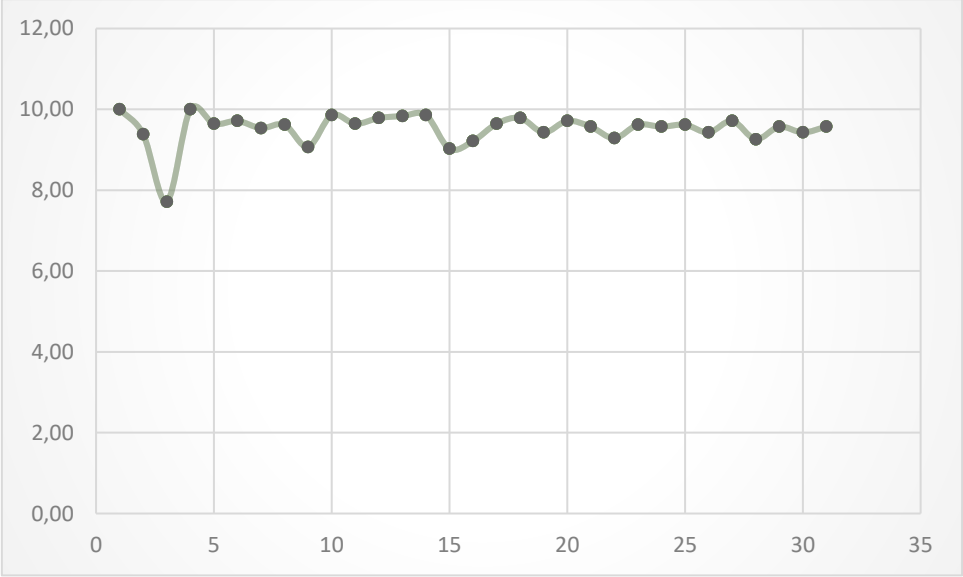
Participante	Taller 1 Malware	Evaluación 1	Evaluación 2	Evaluación 3	Evaluación final	Foro 1 Ciber seguridad	Foro 2 Phishing	Total	Promedio
Participante 1	10,00	10,00	10,00	10,00	10,00	10,00	10,00	70,00	**10,00**
Participante 2	10,00	10,00	6,67	10,00	10,00	10,00	9,00	65,67	**9,38**
Participante 3	7,50	4,83	8,67	10,00	7,00	7,00	9,00	54,00	**7,71**
Participante 4	10,00	10,00	10,00	10,00	10,00	10,00	10,00	70,00	**10,00**
Participante 5	10,00	8,50	10,00	10,00	10,00	10,00	9,00	67,50	**9,64**
Participante 6	10,00	8,00	10,00	10,00	10,00	10,00	10,00	68,00	**9,71**
Participante 7	10,00	10,00	10,00	10,00	8,75	9,00	9,00	66,75	**9,54**
Participante 8	10,00	8,33	10,00	10,00	10,00	10,00	9,00	67,33	**9,62**
Participante 9	10,00	7,50	10,00	10,00	7,00	10,00	9,00	63,50	**9,07**
Participante 10	10,00	10,00	10,00	10,00	9,00	10,00	10,00	69,00	**9,86**
Participante 11	10,00	9,50	10,00	10,00	9,00	10,00	9,00	67,50	**9,64**

Participante 12	10,00	9,50	10,00	10,00	10,00	10,00	9,00	68,50	**9,79**
Participante 13	9,50	10,00	9,33	10,00	10,00	10,00	10,00	68,83	**9,83**
Participante 14	10,00	10,00	10,00	10,00	9,00	10,00	10,00	69,00	**9,86**
Participante 15	10,00	8,50	6,67	10,00	8,00	10,00	10,00	63,17	**9,02**
Participante 16	8,50	10,00	10,00	10,00	6,00	10,00	10,00	64,50	**9,21**
Participante 17	9,50	9,00	10,00	10,00	9,00	10,00	10,00	67,50	**9,64**
Participante 18	10,00	10,00	10,00	10,00	9,00	10,00	9,50	68,50	**9,79**
Participante 19	9,50	7,50	10,00	10,00	10,00	10,00	9,00	66,00	**9,43**
Participante 20	10,00	10,00	10,00	10,00	9,00	9,00	10,00	68,00	**9,71**
Participante 21	10,00	10,00	10,00	10,00	7,00	10,00	10,00	67,00	**9,57**
Participante 22	10,00	9,00	10,00	10,00	7,00	10,00	9,00	65,00	**9,29**
Participante 23	9,00	9,33	10,00	10,00	9,00	10,00	10,00	67,33	**9,62**
Participante 24	10,00	10,00	10,00	10,00	8,00	9,00	10,00	67,00	**9,57**
Participante 25	10,00	8,33	10,00	10,00	10,00	10,00	9,00	67,33	**9,62**
Participante 26	10,00	10,00	10,00	10,00	7,00	10,00	9,00	66,00	**9,43**
Participante 27	10,00	9,00	10,00	10,00	9,00	10,00	10,00	68,00	**9,71**
Participante 28	10,00	9,50	9,33	10,00	8,00	10,00	8,00	64,83	**9,26**
Participante 29	8,00	10,00	10,00	10,00	10,00	10,00	9,00	67,00	**9,57**
Participante 30	9,00	10,00	10,00	10,00	8,00	9,00	10,00	66,00	**9,43**
Participante 31	9,00	10,00	10,00	10,00	9,00	10,00	9,00	67,00	**9,57**

Nota. Esta tabla muestra las calificaciones obtenidas en las actividades del programa.

Figura 23

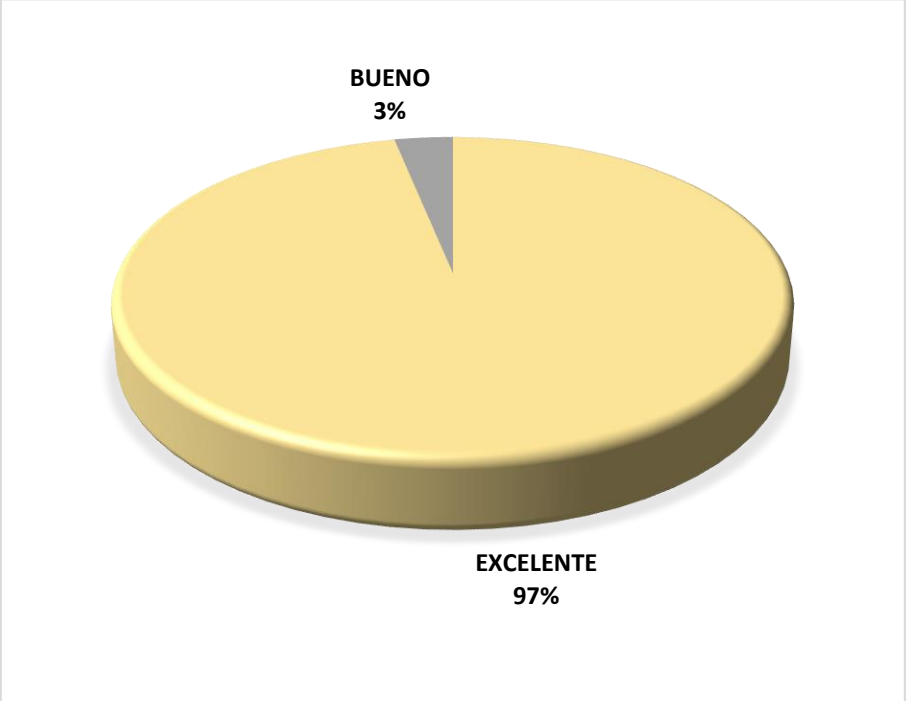
Promedio de calificaciones



Nota. Gráfica del promedio de calificaciones obtenidas por los participantes

Figura 24

Calificación general



Nota. Gráfica de la calificación general del programa de formación.

La calificación general de los funcionarios de la CGE-DPI para el programa de formación, fue en su gran mayoría "EXCELENTE", evidenciándose de esta manera un gran nivel de aprendizaje.

6.1.3 Efectividad

Para la evaluación de la efectividad se tomó en cuenta la aplicación del conocimiento adquirido (cambio en los hábitos) y los resultados de esta aplicación; para esto se utilizaron los reportes del sistema interno de mesa de ayuda, en el cual se registran los casos del área de Tecnología (requerimientos e incidentes).

Para el análisis se utilizaron los reportes del mes previo y posterior a la implementación del programa de formación, tomando en cuenta únicamente los casos relacionados con temas de seguridad informática.

Tabla 13

Reporte de casos de SI previo al programa

Código	Tipo	Título	Descripción	F. Registro	F. Atención	Estado
CASO-00109897	INCIDENTE	POSIBLE ATAQUE DE PHISHING	Compañera reporta correo electrónico que solicita actualizar información de cuenta Outlook	21/8/2023	21/8/2023	FINALIZADO
CASO-00109987	INCIDENTE	INFECCIÓN DE VIRUS	Sistema operativo ralentizado	23/8/2023	23/8/2023	FINALIZADO

CASO-00109992	INCIDENTE	POSIBLE ATAQUE DE PHISHING	Compañera de TH informa que recibió llamada telefónica solicitando información de su tarjeta de crédito.	23/8/2023	23/8/2023	FINALIZADO
CASO-00110009	REQUERIMIENTO	CAMBIO DE CONTRASEÑA	Auditor externo solicita el reseteo de su contraseña, informa que entregó la clave en la CZ1 MIES para instalación de impresora.	29/8/2023	29/8/2023	FINALIZADO
CASO-00110024	INCIDENTE	ACCESO NO AUTORIZADO	Director reporta que le llegó un correo informando de un intento de acceso no autorizado a CGE Aplicativos.	31/8/2023	31/8/2023	FINALIZADO
CASO-00110031	INCIDENTE	COMPUTADOR PORTÁTIL NO ARRANCA	Portátil no inicia sistema operativo, informa que computador se apagó después de insertar usb	31/8/2023	31/8/2023	FINALIZADO
CASO-00110056	INCIDENTE	ARCHIVOS PDF NO SE ABREN	Auditor reporta que no puede abrir ciertos archivos pdf, informa que accedió a una red inalámbrica pública, ya que en la entidad no contaban con buen Internet.	1/9/2023	1/9/2023	FINALIZADO
CASO-00110075	INCIDENTE	CORREO MALICIOSO	Auditor informa que recibió un correo electrónico que dice que ha recibido una transferencia de dinero	4/9/2023	4/9/2023	FINALIZADO
CASO-00110129	INCIDENTE	ARCHIVOS PERDIDOS	Auditor interno indica que varios archivos de análisis de su examen no están en su computador.	6/9/2023	6/9/2023	FINALIZADO
CASO-00110191	REQUERIMIENTO	RESETEO DE CONTRASEÑA	Compañero de Balcón de Servicios solicita resetear clave, ha compartido su contraseña.	11/9/2023	11/9/2023	FINALIZADO
CASO-00110223	INCIDENTE	ACCESO NO AUTORIZADO	Auditora externa informa que apreció un mensaje de windows de una conexión remota en GADM Ibarra	12/9/2023	12/9/2023	FINALIZADO
CASO-00110227	REQUERIMIENTO	ACTUALIZACIÓN DE ANTIVIRUS	Auditor interno requiere actualización de software antivirus	12/9/2023	12/9/2023	FINALIZADO
CASO-00110288	INCIDENTE	ATAQUE DE MALWARE	Jurídico reporta daño en archivos de word	14/9/2023	14/9/2023	FINALIZADO
CASO-00110305	INCIDENTE	SITIO WEB MALICIOSO	Compañera de Balcón de Servicios reporta alerta de sitio malicioso	15/9/2023	15/9/2023	FINALIZADO
CASO-00110316	INCIDENTE	USB INFECTADA	Sistema operativo congelado, indica que insertó una memoria usb	18/9/2023	18/9/2023	FINALIZADO
CASO-00110327	INCIDENTE	POSIBLE ATAQUE DE MALWARE	TH indica que recibió un correo aparentemente de CNT, solicitando descargar archivo para actualización de base de datos	18/9/2023	18/9/2023	FINALIZADO
CASO-00110341	INCIDENTE	CORREO MALICIOSO	Auditor externo informa de posible correo malicioso	19/9/2023	19/9/2023	FINALIZADO

Nota. Esta tabla muestra diecisiete casos de SI registrados en el período agosto-septiembre 2023

Tabla 14

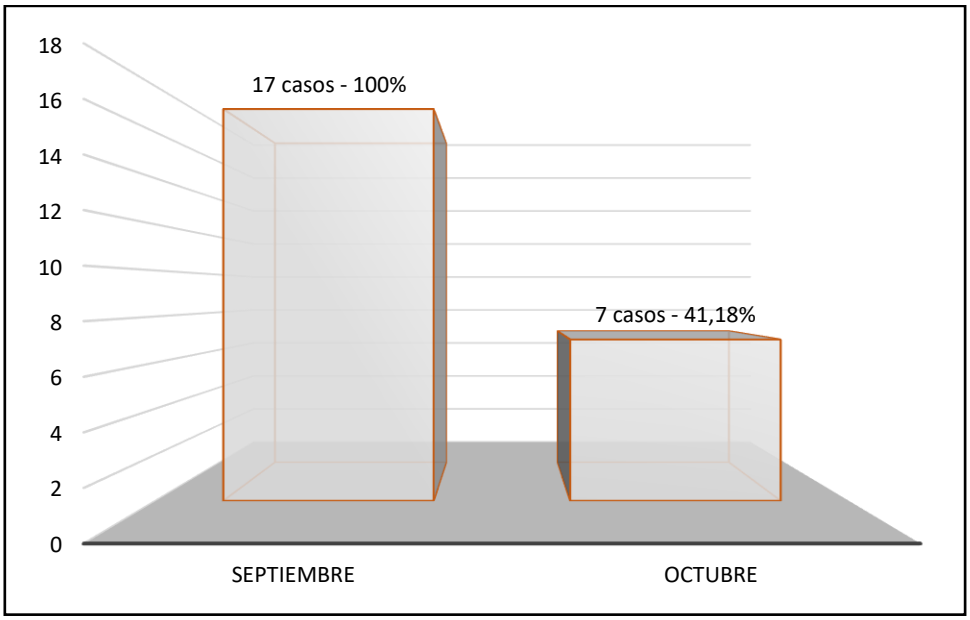
Reporte de casos de SI posterior al programa

Código	Tipo	Título	Descripción	F. Registro	F. Atención	Estado
CASO-00110439	INCIDENTE	ACCESO NO AUTORIZADO	Jurídico reporta correo de alerta de intento de acceso no autorizado a CGE Aplicativos	25/9/2023	25/9/2023	FINALIZADO
CASO-00110512	INCIDENTE	MEMORIA USB	Memoria usb con archivos sospechosos	28/9/2023	28/9/2023	FINALIZADO
CASO-00110634	REQUERIMIENTO	CAMBIO DE CONTRASEÑA	Financiera requiere cambio de contraseña, alerta de acceso denegado por intentos fallidos.	4/10/2023	4/10/2023	FINALIZADO
CASO-00110752	INCIDENTE	ALERTA ANTIVIRUS	Auditor externo informa de alerta del antivirus al ingresar a sitio web	12/10/2023	12/10/2023	FINALIZADO
CASO-00110815	REQUERIMIENTO	CAMBIO DE CONTRASEÑA	Auditor externo solicita el reseteo de su contraseña, no puede acceder a correo electrónico	17/10/2023	17/10/2023	FINALIZADO
CASO-00110874	INCIDENTE	CORREO MALICIOSO	Auditor externo informa de correo malicioso, solicitando acceder a enlace.	19/10/2023	19/10/2023	FINALIZADO
CASO-00110927	INCIDENTE	PC CONGELADA	Computador de escritorio de Balcón de Servicios no responde al escanear usb	19/10/2023	19/10/2023	FINALIZADO

Nota. Esta tabla muestra siete casos de SI registrados en el período septiembre-octubre 2023

Figura 25

Efectividad del programa de formación



Nota. Disminución de la ocurrencia de casos de SI, después de la implementación del programa de formación.

De acuerdo al análisis de los reportes del sistema interno de mesa de ayuda, se pudo evidenciar una disminución del 58,82% en la ocurrencia de casos de seguridad informática, por lo que, es evidente la efectividad que tuvo el programa de formación de seguridad informática en los funcionarios de la CGE-DPI.

CONCLUSIONES

Las amenazas de seguridad informática directamente relacionadas a acciones de los usuarios fueron: **usuarios** (a través del desconocimiento y malas prácticas), **malware** (ransomware, virus, troyanos, gusanos, keyloggers), **ingeniería social** (phishing, vishing, pharming), **ataques de contraseñas** (fuerza bruta, diccionario, relleno de credenciales) y **seguridad física** (accesos no autorizados), mismas que generaron un nivel de riesgo **Medio**, **Alto** y **Muy alto** para la protección de los activos de información de la CGE-DPI.

El 41% de los funcionarios de la CGE-DPI tenían un nivel de conocimiento **Bajo,** con respecto a temáticas específicas de seguridad informática, previo al programa de formación, lo que pudo haber provocado en algún momento pérdida de información, perjuicio a los recursos y a la imagen de la Institución.

El 100% de funcionarios desconocían lo qué es un ransomware, hecho que efectivamente se evidenció mediante un caso presentado en la CGE-DPI que resultó en la pérdida total de la información de una funcionaria.

El 87% de los participantes, dieron una valoración de **Muy satisfechos**, con respecto a la organización, la temática, el material y el conocimiento por parte del instructor, lo cual ratifica que el programa de formación de seguridad tuvo gran aceptación y satisfacción.

El 97% de los participantes tuvieron un aprendizaje general de **EXCELENTE,** por lo tanto, los usuarios se encuentran más preparados para afrontar las amenazas informáticas que se presentan a diario, tanto en sus actividades laborales, como personales.

Se evidenció una disminución del 58,82% en la ocurrencia de casos de seguridad informática, así pues, se evidencia el éxito del programa de formación de seguridad y el impacto positivo que generó en los funcionarios de la CGE-DPI.

RECOMENDACIONES

Replicar el programa de formación de seguridad informática a nivel nacional, en las demás direcciones provinciales y en la matriz de la Contraloría General del Estado.

Asegurar el mejoramiento continuo del programa de formación, evaluando y actualizando constantemente su contenido, a medida que van surgiendo nuevas amenazas y maneras de atacar a la seguridad informática.

Fomentar una cultura de seguridad informática, en los funcionarios de la Contraloría General del Estado, a través de campañas permanentes de prevención de ataques que amenacen la protección de activos de información.

REFERENCIAS

Awe, & Awe. (2016, 3 noviembre). Seguridad: el factor humano, el eslabón más débil. *Soporte Informático Empresas - Servicios informáticos empresas - Mantenimiento informático empresas*. https://www.awerty.net/blog/seguridad-el-factor-humano-el-eslabon-mas-debil/

AdminIberoBlogs. (2021b, noviembre 17). *¿Qué es La Seguridad de la Información y cuál es su importancia?* IBERO Posgrados | Blog. https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Castillo, L. J. E. C., & Castillo, L. J. E. C. (2020, 20 octubre). Usuario final, el eslabón más débil de la seguridad informática - Revista - Stratega Magazine. *Revista - Stratega Magazine - Stratega Magazine*. https://strategamagazine.com/usuario-final-el-eslabon-mas-debil-de-la-seguridad-informatica/

Ciberseg. (2019). Plan de concienciación de seguridad informática. *Ciberseguridad*. https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/

Augusto, V. L. C. (2017, 7 febrero). *Articulo en formato IEEE : Concienciación en Seguridad de la información*. http://repository.unipiloto.edu.co/handle/20.500.12277/2667/

De Expertos En Ciencia Y Tecnología, E. (2022, 7 diciembre). ¿Qué es la seguridad informática y cómo puede ayudarme? *VIU España*. https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Malwarebytes. (2019a). ¿Qué es el phishing? | Cómo protegerse de los ataques de phishing. *Malwarebytes*. https://es.malwarebytes.com/phishing/

Malwarebytes. (2019b). ¿Qué es el malware? Definición y cómo saber si está infectado. *Malwarebytes*. https://es.malwarebytes.com/malware/

Fases de un ataque informatico. (2014, 22 septiembre). WordPress.com. https://hilfrank.wordpress.com/fases-de-un-ataque-informatico/

¿Qué es la seguridad informática y cuál es su función? – CX Solutions. (s. f.). https://cxsolutions.mx/que-es-la-seguridad-informatica-y-cual-es-su-funcion/

Seguridad: el factor humano, el eslabón más débil. (2016). Awerty.net. https://www.awerty.net/blog/seguridad-el-factor-humano-el-eslabon-mas-debil/

Tavera, K. (2020). 7 amenazas informáticas que toda Pyme debe conocer. *Blog*. https://co.godaddy.com/blog/7-amenazas-informaticas-toda-pyme-debe-conocer/

Team, A. (s. f.). *Tipos de Vulnerabilidades y Amenazas informáticas*. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Unir, V. (2022b, octubre 13). ¿Qué es la seguridad informática y cuáles son sus tipos? *Universidad Virtual. | UNIR Ecuador - Maestrías y Grados virtuales*. https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica

Llamas, J. (2022). Seguridad informática. *Economipedia*. https://economipedia.com/definiciones/seguridad-informatica.html

Valenzuela, C. G. (2022, 14 abril). Estos son los 4 ataques más comunes que atentan contra tus contraseñas y cómo protegerte. *Computer Hoy*. https://computerhoy.com/noticias/tecnologia/estos-son-4-ataques-comunes-atentan-contrasenas-como-protegerte-1045157

xeral.net. (2017, 2 octubre). *¿Cuáles son las principales amenazas de la seguridad informática? - Vega Gestión*. Vega Gestión. https://vegagestion.es/cuales-las-principales-amenazas-la-seguridad-informatica/

Infordisa / Security Operations Center. (2021, 19 octubre). *activo de información - Infordisa / Security Operations Center*. https://www.infordisa.com/soc/glosario-definicion/activo-de-informacion/

Tituaña, A. (2017, 23 agosto). PROTEGER LA INFORMACIÓN EMPRESARIAL. *Cursosypostgrados*. https://www.cursosypostgrados.com/noticias/proteger-la-informacion-empresarial-195.html

Caser. (2023). Ataque informático. *www.caser.es*. https://www.caser.es/glosario-seguros/comercio/ataque-informatico

Méndez G. (2021, 12 marzo). Los Ciberdelincuentes: Quiénes Son, Qué Hacen Y Por Qué Lo Hacen - Acktib. *Acktib*. https://acktib.com/blog-los-ciberdelincuentes-quienes-son-que-hacen-y-por-que-lo-hacen/

El desconocimiento de los usuarios, ¿principal causa de infecciones? | WeLiveSecurity. (2023, 4 abril). WeLiveSecurity. https://www.welivesecurity.com/la-es/2017/10/19/desconocimiento-usuarios-causa-de-infecciones/

Ciberseg. (2019b). Ransomware. *Ciberseguridad*. https://ciberseguridad.com/amenzas/ransomware

What is a computer virus? (s. f.). https://lam.norton.com/blog/malware/what-is-a-computer-virus

Belcic, I. (2023a). ¿Qué es un malware troyano? Guía definitiva. *¿Qué es un malware troyano? Guía definitiva*. https://www.avast.com/es-es/c-trojan

Gusanos informáticos - Definición, reconocimiento y protección. (2020, 14 octubre). Hornetsecurity – Servicios de seguridad en nube para empresas. https://www.hornetsecurity.com/es/knowledge-base/gusanos-informaticos/

¿Qué es un keylogger? (2023, 19 abril). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/keylogger

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

R. Zieni, L. Massari and M. C. Calzarossa, "Phishing or Not Phishing? A Survey on the Detection of Phishing Websites," in IEEE Access, vol. 11, pp. 18499-18519, 2023, doi: 10.1109/ACCESS.2023.3247135.

Qué es el vishing: estafa a través de llamadas o mensajes de voz | WeLiveSecurity. (2023, 4 abril). WeLiveSecurity. https://www.welivesecurity.com/la-es/2021/05/03/que-es-vishing/

Security, P. (2022, 19 septiembre). *¿Qué es el pharming? Definición y formas de prevenirlo*. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/seguridad/pharming/

buzonuv@uv.mx. (s. f.). *Noti_infosegura: ¿Cuáles son los errores más comunes a la hora de crear una contraseña? – Seguridad de la información*. https://www.uv.mx/infosegura/general/noti_contrasenas-48/

KeepCoding, R. (2023, 27 septiembre). Ataques de contraseña | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/ataques-de-contrasena/

Correo malicioso-Portal de la UEX-Bienvenido a la Universidad de Extremadura. (s. f.). https://www.unex.es/organizacion/servicios-universitarios/servicios/siue/noticias/Correomalo/document_view

Jurado, Á., & Jurado, Á. (2023). Amenazas de seguridad física para los sistemas de información. *Canal Gestión Integrada*. https://www.inesem.es/revistadigital/gestion-integrada/amenazas-seguridad-fisica-sistemas-de-informacion/

Jiménez, M. M. (s. f.). *Vulnerabilidades que afectan la seguridad de la información*. https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

De TechTarget, C. (2013). Contraseña robusta. *ComputerWeekly.es*. https://www.computerweekly.com/es/definicion/Contrasena-robusta

González, G. (2019). Cómo utilizar la nemotecnia para crear y recordar contraseñas complejas y seguras. *Genbeta*. https://www.genbeta.com/a-fondo/como-utilizar-la-nemotecnia-para-crear-y-recordar-contrasenas-complejas-y-seguras

Arguelles, G. T. (2023, 30 abril). ¿Por qué es una mala idea reutilizar contraseñas? *Access Quality - Líderes en Servicios TI y SOC y NOC*. https://www.accessq.com.mx/porque-es-mala-idea-reutilizar-contrasenas/

McAfee. (2022). 10 consejos para protegerse en las redes sociales. *McAfee Blog*. https://www.mcafee.com/blogs/es-mx/tips-tricks/10-consejos-para-protegerse-en-las-redes-sociales/

Fernández, Y. (2021). La mega-guía de la privacidad y seguridad en Facebook. *Xataka*. https://www.xataka.com/basics/mega-guia-privacidad-seguridad-facebook

Seguridad en Internet: ¿Qué es el stalking? (s. f.). GCFGlobal.org. https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-el-stalking/1/

DIPLAB [DIPLAB]. (2021). *Concientización en seguridad de la información*. Laboratorio de nuevas tecnologías. Recuperado 15 de agosto de 2023, de https://diplab.hcdn.gob.ar/public/pdf/DipLab-Manual_Ciberseguridad.pdf

ANEXOS

ANEXO A

REGISTRO FOTOGRÁFICO

ANEXO B

MATRICES DE VALIDACIÓN

MATRICES DE VALIDACIÓN DE INSTRUMENTOS

Estimado validador: Soy Cristian Fernando Rodríguez Erazo CC.1002989869

Los presentes instrumentos hacen parte de la tesis de maestría titulada "*Programa de formación de seguridad informática, basado en la publicación NIST SP 800-50, para la Contraloría General del Estado - Dirección Provincial de Imbabura*".

A continuación, se presenta el sistema de objetivos de la investigación con la finalidad de proporcionar información para la evaluación de la pertinencia y coherencia de los instrumentos.

Objetivo General

Implementar un programa de formación de seguridad informática, basado en la publicación NIST SP 800-50, para la Contraloría General del Estado - Dirección Provincial de Imbabura.

Objetivos específicos

- Realizar un marco conceptual de las amenazas de seguridad informática, para la protección de activos de información en la CGE-DPI.
- Determinar el nivel de conocimiento sobre seguridad informática que poseen los servidores de la CGE-DPI.
- Diseñar el programa de formación sobre la seguridad informática, de acuerdo a las directrices de la NIST SP 800-50.
- Evaluar la efectividad del programa de formación al personal de la CGE-DPI, en base al modelo 2 de la NIST SP 800-50.

Se incluye las matrices de validación.

ENCUESTA A LOS FUNCIONARIOS DE LA CONTRALORÍA GENERAL DEL ESTADO – DIRECCIÓN PROVINCIAL DE IMBABURA

CONSENTIMIENTO INFORMADO.

Estimado Sr. Director de la Contraloría General del Estado - Dirección Provincial de Imbabura, solicitó comedidamente a usted, se sirva a responder el presente instrumento que tiene como objeto implementar un programa de formación de seguridad informática, basado en la publicación NIST SP 800-50, para la Contraloría General del Estado - Dirección Provincial de Imbabura. El resultado de esta encuesta será utilizado en el trabajo investigativo para la maestría en Computación con mención Seguridad Informática.

Variable	Indicador	Técnica	Instrumento	Preguntas
Seguridad ligada a los recursos humanos	Educación continua	Encuesta	Cuestionario	1. **¿CONOCE DE QUÉ SE TRATA LA SEGURIDAD INFORMÁTICA?** -Domino el tema -Conozco un poco -No tengo ningún conocimiento del tema
Seguridad en las operaciones	Protección contra código malicioso	Encuesta	Cuestionario	2. **¿SABE QUÉ ES UN ATAQUE INFORMÁTICO?** -Domino el tema -Conozco un poco -No tengo ningún conocimiento del tema
Seguridad en las operaciones	Protección contra código malicioso	Encuesta	Cuestionario	3. **¿CONOCE QUÉ ES UN CIBERDELINCUENTE?** -Domino el tema -Conozco un poco -No tengo ningún conocimiento del tema
Seguridad en las operaciones	Protección contra código malicioso	Encuesta	Cuestionario	4. **¿GENERALMENTE ESCANEA UN DISPOSITIVO USB CON EL ANTIVIRUS ANTES DE UTILIZARLO?** -Siempre -A veces -Nunca

Seguridad en las operaciones	Protección contra código malicioso	Encuesta	Cuestionario	5. **¿CONOCE QUE ES EL RANSOM-WARE?** -Domino el tema -Conozco un poco -No tengo ningún conocimiento del tema
Seguridad en las telecomunica-ciones	Mensajería electrónica	Encuesta	Cuestionario	6. **¿CONOCE DE QUÉ SE TRATA UN ATAQUE DE PHISHING?** -Domino el tema -Conozco un poco -No tengo ningún conocimiento del tema
Seguridad en las operaciones	Protección contra código malicioso	Encuesta	Cuestionario	7. ¿ **RECONOCE UNA PÁGINA WEB FRAUDULENTA?** -Si -No -No estoy seguro/a
Seguridad en las telecomunica-ciones	Mensajería electrónica	Encuesta	Cuestionario	8. **¿USUALMENTE VERIFICA EL RE-MITENTE DE SUS CORREOS ELEC-TRÓNICOS?** -Siempre -A veces -Nunca
Control de accesos	Responsabili-dades del usuario	Encuesta	Cuestionario	9. **¿BLOQUEA O CIERRA SU SESIÓN, CUANDO ABANDONA MOMENTÁNEA-MENTE SU ESTACIÓN DE TRABAJO?** -Siempre -A veces -Nunca
Control de accesos	Responsabili-dades del usuario	Encuesta	Cuestionario	10. ¿**GENERALMENTE GUARDA LAS CONTRASEÑAS EN: (notas, cuaderno, te-léfono, archivos de texto, fotografía)?** -Siempre -A veces -Nunca
Control de accesos	Responsabili-dades del usuario	Encuesta	Cuestionario	11. **¿REUTILIZA LA MISMA CONTRA-SEÑA PARA SUS APLICACIONES?** -Para 2 aplicaciones -Para 3 aplicaciones -Para más de 3 aplicaciones -Tengo una contraseña diferente para cada aplicación

Políticas de seguridad	Conjunto de políticas de SI.	Encuesta	Cuestionario	12. **¿LA CONTRALORÍA GENERAL DEL ESTADO CUENTA CON POLÍTICAS DE SEGURIDAD INFORMÁTICA?** -Si -No -Desconozco
Políticas de seguridad	Conjunto de políticas de SI.	Encuesta	Cuestionario	13. **¿EXISTEN DIRECTRICES EN LA CGE PARA EL USO SEGURO DE LOS EQUIPOS Y MANEJO ADECUADO DE LA INFORMACIÓN?** -Si -No -Desconozco
Seguridad ligada a los recursos humanos	Educación continua	Encuesta	Cuestionario	14. **¿CONOCE LA MANERA DE ESTABLECER LA PRIVACIDAD DE LA INFORMACIÓN DE SUS REDES SOCIALES (Ej. Facebook, Instagram, WhatsApp)?** -Domino el tema -Conozco un poco -No tengo ningún conocimiento del tema
Seguridad ligada a los recursos humanos	Educación continua	Encuesta	Cuestionario	15. **¿GENERALMENTE PUBLICA INFORMACIÓN PERSONAL EN SUS REDES SOCIALES? (Cumpleaños, lugar de trabajo, teléfono, correo, gustos, intereses, etc)** -Siempre -A veces -Nunca
Seguridad ligada a los recursos humanos	Educación continua	Encuesta	Cuestionario	16. **¿HA RECIBIDO FORMACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?** -Sí, de forma autónoma -Sí, en el trabajo -No he recibido formación sobre este tema

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

Instituto de Posgrado

INSTRUMENTO DE VALIDACIÓN

Instrucciones: En el siguiente formato, señale con una X en cada ítem, de acuerdo con los criterios de validación (claridad, coherencia, relevancia), si es necesario agregue las observaciones que considere. Al final se deja un espacio para agregar observaciones generales.

Preguntas	Cumple con la claridad		Cumple con coherencia		Cumple con relevancia		Observaciones
	SI	NO	SI	NO	SI	NO	
1. ¿CONOCE DE QUÉ SE TRATA LA SEGURIDAD INFORMÁTICA?	X		X		X		
2. ¿SABE QUÉ ES UN ATAQUE INFORMÁTICO?	X		X		X		
3. ¿CONOCE QUÉ ES UN CIBERDELINCUENTE?	X		X		X		
4. ¿GENERALMENTE ESCANEA UN DISPOSITIVO USB CON EL ANTIVIRUS ANTES DE UTILIZARLO?	X		X		X		
5. ¿CONOCE QUE ES EL RANSOMWARE?	X		X		X		
6. ¿CONOCE DE QUÉ SE TRATA UN ATAQUE DE PHISHING?	X		X		X		
7. ¿RECONOCE UNA PÁGINA WEB FRAUDULENTA?	X		X		X		
8. ¿USUALMENTE VERIFICA EL REMITENTE DE SUS CORREOS ELECTRÓNICOS?	X		X		X		
9. ¿BLOQUEA O CIERRA SU SESIÓN, CUANDO ABANDONA MOMENTÁNEAMENTE SU ESTACIÓN DE TRABAJO?	X		X		X		
10. ¿GENERALMENTE GUARDA LAS CONTRASEÑAS EN: (notas, cuaderno, teléfono, archivos de texto, fotografía)?	X		X		X		

11. ¿REUTILIZA LA MISMA CONTRASEÑA PARA DOS O MÁS APLICACIONES?	X		X		X		
12. ¿LA CONTRALORÍA GENERAL DEL ESTADO CUENTA CON POLÍTICAS DE SEGURIDAD INFORMÁTICA?	X		X		X		
13. ¿EXISTEN DIRECTRICES EN LA CGE PARA EL USO SEGURO DE LOS EQUIPOS Y MANEJO ADECUADO DE LA INFORMACIÓN?	X		X		X		
14. ¿CONOCE LA MANERA DE ESTABLECER LA PRIVACIDAD DE LA INFORMACIÓN DE SUS REDES SOCIALES (Ej. Facebook, Instagram, WhatsApp)?	X		X		X		
15. ¿GENERALMENTE PUBLICA INFORMACIÓN PERSONAL EN SUS REDES SOCIALES? (Cumpleaños, lugar de trabajo, teléfono, correo, gustos, intereses, etc)	X		X		X		
16. ¿HA RECIBIDO FORMACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA? -Sí, de forma autónoma	X		X		X		

Observaciones generales:

.....

Phd. Marco Pusdá

MATRICES DE VALIDACIÓN DE INSTRUMENTOS

Estimado validador: Soy Cristian Fernando Rodríguez Erazo CC.1002989869

Los presentes instrumentos hacen parte de la tesis de maestría titulada "*Programa de formación de seguridad informática, basado en la publicación NIST SP 800-50, para la Contraloría General del Estado - Dirección Provincial de Imbabura*".

A continuación, se presenta el sistema de objetivos de la investigación con la finalidad de proporcionar información para la evaluación de la pertinencia y coherencia de los instrumentos.

Objetivo General

Implementar un programa de formación de seguridad informática, basado en la publicación NIST SP 800-50, para la Contraloría General del Estado - Dirección Provincial de Imbabura.

Objetivos específicos

- Realizar un marco conceptual de las amenazas de seguridad informática, para la protección de activos de información en la CGE-DPI.
- Determinar el nivel de conocimiento sobre seguridad informática que poseen los servidores de la CGE-DPI.
- Diseñar el programa de formación sobre la seguridad informática, de acuerdo a las directrices de la NIST SP 800-50.
- Evaluar la efectividad del programa de formación al personal de la CGE-DPI, en base al modelo 2 de la NIST SP 800-50.

Se incluye las matrices de validación.

ENCUESTA A LOS FUNCIONARIOS DE LA CONTRALORÍA GENERAL DEL ESTADO – DIRECCIÓN PROVINCIAL DE IMBABURA

CONSENTIMIENTO INFORMADO.

Estimado Sr. Director de la Contraloría General del Estado - Dirección Provincial de Imbabura, solicitó comedidamente a usted, se sirva a responder el presente instrumento que tiene como objeto implementar un programa de formación de seguridad informática, basado en la publicación NIST SP 800-50, para la Contraloría General del Estado - Dirección Provincial de Imbabura. El resultado de esta encuesta será utilizado en el trabajo investigativo para la maestría en Computación con mención Seguridad Informática.

Variable	Indicador	Técnica	Instrumento	Preguntas
Utilidad percibida	Satisfacción	Encuesta	Cuestionario	1. **Por favor, califique el nivel de satisfacción para la Organización del programa** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho
Utilidad percibida	Satisfacción	Encuesta	Cuestionario	**2. Por favor, califique el nivel de satisfacción para la Temas abordados en el programa** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho
Utilidad percibida	Satisfacción	Encuesta	Cuestionario	**3. Por favor, califique el nivel de satisfacción para la Material del programa** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho
Utilidad percibida	Satisfacción	Encuesta	Cuestionario	**4. Por favor, califique el nivel de satisfacción para la Conocimiento del instructor** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho

Facilidad percibida	Calidad	Encuesta	Cuestionario	5. **¿Qué tan fácil fue entender los términos que usaba el instructor?** Muy difícil Difícil Neutral Fácil Muy fácil
Utilidad percibida	Satisfacción	Encuesta	Cuestionario	6. **¿Cree que la duración del programa fue lo suficientemente buena como para satisfacer sus expectativas de formación?** Si No Prefiero no decir
Utilidad percibida	Importancia	Encuesta	Cuestionario	7. **¿Se explicó claramente el objetivo del programa previo a su inicio?** Si No Prefiero no decir
Utilidad percibida	Calidad	Encuesta	Cuestionario	8. **¿El programa de formación le proporcionó aprendizajes prácticos y teóricos?** Si No Prefiero no decir
Utilidad percibida	Importancia	Encuesta	Cuestionario	9. **¿Considerando su experiencia completa con el programa, recomendaría replicar el programa de formación a los servidores de la CGE a nivel nacional?** Lo recomendaría No lo recomendaría
Utilidad percibida	Importancia	Encuesta	Cuestionario	10. **¿Tiene alguna sugerencia o comentario que ayude a mejorar el programa?**

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

Instituto de Posgrado

INSTRUMENTO DE VALIDACIÓN

Instrucciones: En el siguiente formato, señale con una X en cada ítem, de acuerdo con los criterios de validación (claridad, coherencia, relevancia), si es necesario agregue las observaciones que considere. Al final se deja un espacio para agregar observaciones generales.

Preguntas	Cumple con la claridad		Cumple con coherencia		Cumple con relevancia		Observaciones
	SI	NO	SI	NO	SI	NO	
1. **Por favor, califique el nivel de satisfacción para la Organización del programa** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho	X		X		X		
2. **Por favor, califique el nivel de satisfacción para la Temas abordados en el programa** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho	X		X		X		
3. **Por favor, califique el nivel de satisfacción para la Material del programa** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho	X		X		X		
4. **Por favor, califique el nivel de satisfacción para la Conocimiento del instructor** Muy insatisfecho Insatisfecho Neutral Satisfecho Muy Satisfecho	X		X		X		

5. **¿Qué tan fácil fue entender los términos que usaba el instructor?** Muy difícil Difícil Neutral Fácil Muy fácil	X		X		X		
6. **¿Cree que la duración del programa fue lo suficientemente buena como para satisfacer sus expectativas de formación?** Si No Prefiero no decir	X		X		X		
7. **¿Se explicó claramente el objetivo del programa previo a su inicio?** Si No Prefiero no decir	X		X		X		
8. **¿El programa de formación le proporcionó aprendizajes prácticos y teóricos?** Si No Prefiero no decir	X		X		X		
9. **¿Considerando su experiencia completa con el programa, recomendaría replicar el programa de formación a los servidores de la CGE a nivel nacional?** Lo recomendaría No lo recomendaría	X		X		X		
10. **¿Tiene alguna sugerencia o comentario que ayude a mejorar el programa?**	X		X		X		

Observaciones generales:

.....

Phd. Marco Pusdá