UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
PROPUESTA DE ACCIONES PARA EVITAR INCIDENTES DE PHISHING AL SISTEMA INFORMÁTICO S.G.P DE UN CENTRO PENITENCIARIO DE ECUADOR
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autora:
Solórzano Coello Andrea Viviana
Tutor:
MSC. Recalde Varela Pablo Marcel

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Msc. Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA DE ACCIONES PARA EVITAR INCIDENTES DE PHISHING AL SISTEMA INFORMÁTICO S.G.P DE UN CENTRO PENITENCIARIO DE ECUADOR.

Elaborado por: Andrea Viviana Solórzano Coello, de C.I: 1310819444, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Andrea Viviana Solórzano Coello con C.I: 1310819444, autora del proyecto de titulación denominado: PROPUESTA DE ACCIONES PARA EVITAR INCIDENTES DE PHISHING AL SISTEMA INFORMÁTICO S.G.P DE UN CENTRO PENITENCIARIO DE ECUADOR. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
ANDREA VIVIANA
SOLORZANO COELLO

_____

Firma

orcid: 0000-0002-1760-8106

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Como hemos visto durante los últimos años, uno de los activos más importantes en una empresa, es la información. A continuación, se presenta una visión general del porqué se desarrolla este trabajo de máster en seguridad informática, aplicada al phishing.

Contextualización del tema

La Ingeniería Social implica la obtención engañosa de datos de individuos, con la intención de emplear dicha información en su perjuicio o en detrimento de sus grupos u empresas (Benavides y otros, 2020).

Un ataque de phishing es una forma de ingeniería social utilizada por piratas informáticos para robar credenciales a través de canales de comunicación, es uno de los métodos más utilizados para manipular a individuos para que divulguen información delicada, tal como: usuarios, contraseñas, números de tarjetas de crédito, entre otros; a través de la suplantación o simulación de una entidad confiable, que requiere la información para proceder con algún proceso lícito (Guaña y otros, 2022).

Las personas con acceso a Internet, en la actualidad, no se encuentran ajenas a caer en un ataque de ingeniería social, a diario escuchamos historias de individuos que giran en nuestro entorno, acerca de cómo sujetos inescrupulosos han robado sus ahorros de toda la vida o han realizado transacciones con sus tarjetas de crédito o débito (Koyun & Al Janabi, 2017).

Esta realidad no es ajena en los centros penitenciarios, donde los funcionarios, además de la información de índole personal -susceptible a ser vulnerada y causándoles algún perjuicio-; manejan también información digital sensible de las Personas Privadas de la Libertad (PPL), cuya información reposa y es alimentada diariamente en el Sistema de Gestión Penitenciaria (SGP) y la institución pública encargada de su mantenimiento es el SNAI. Por el carácter reservado y sensible de esta información, al caer en poder de personas inescrupulosas puede causar severas afectaciones de seguridad en el sistema penitenciario.

La vulnerabilidad al sistema puede ser aprovechada por un ciberdelincuente que utilice el phishing como herramienta para acceder a la información sensible que contiene el SGP y causar daños tanto al sistema como a las personas que se vean implicadas directa o indirectamente. Por esta razón es esencial contar con una sólida infraestructura de seguridad informática con el propósito de identificar y evitar este tipo de ataques, que impidan a los ciberdelincuentes robar credenciales mediante engaños para acceder a la información confidencial del sistema de gestión penitenciaria SGP.

Problema de investigación

Si partimos asumiendo que el punto de menor resistencia en la cadena de seguridad cibernética es el usuario final, entenderemos que el phishing es uno de los diferentes mecanismos de ingeniería social aplicable en el personal que trabaja en una cárcel.

Figura 1.

Clasificación de los ataques de Ingeniería Social

Nota: Elaboración realizada a partir de datos de (Salahdine & Kaabouch, 2019, pág. 2)

De manera continua, se reciben correos electrónicos tanto en las cuentas institucionales como personales de cada funcionario, y se han detectado casos de phishing, haciéndose pasar por entidades bancarias, de estudios e incluso estatales, mismas que al final mediante un link, llevan a un portal diseñado específicamente para obtener la información personal del funcionario elegido y de esta manera poder obtener credenciales de acceso para vulnerar el ingreso a la infraestructura informática del sistema penitenciario.

En el caso específico de vulneración al SGP, la finalidad del ciberdelincuente será obtener información sensible y de carácter reservado de las PPL que se almacena en este sistema informático; la técnica utilizada para cometer el ilícito es un ataque phishing.

¿Estableciendo una propuesta de acciones específicas que reduzcan el impacto del phishing, se pueden evitar las intromisiones de ciberdelincuentes al SGP de los centros penitenciarios del Ecuador?

Objetivo general

Establecer acciones que prevengan incidentes phishing como técnica recurrente para conseguir accesos no autorizados hacia el sistema informático SGP de un centro penitenciario del Ecuador.

Objetivos específicos

- Identificar vulnerabilidades de ciberseguridad en el sistema informático SGP de un centro penitenciario evitando daños potenciales debido a phishing.
- Implementar políticas de ciberseguridad en la infraestructura de red de un centro penitenciario.
- Elaborar un plan de capacitación continua de seguridad informática para el personal que labora en un centro penitenciario.

Vinculación con la sociedad y beneficiarios directos:

Al ser el Sistema de Gestión Penitenciaria (SGP) un sistema informático gubernamental que contiene información de las personas privadas de la libertad, información que es sensible de carácter reservada, que también detalla las actividades que realiza cada PPL en los diferentes ejes de rehabilitación, misma que sirve para ver el progreso paulatino de quienes ya cuenten con una sentencia condenatoria ejecutoriada, y que además, muestra cuando está cerca a la obtención de un beneficio penitenciario - antes de satisfacer todos los requisitos delineados en la normativa legal- es necesario que esta herramienta informática estatal, garantice la debida seguridad informática, que impida el acceso a ciberdelincuentes o a funcionarios no autorizados para el manejo de la información.

Es por esta razón que, validando la información contenida en los Objetivos de Desarrollo Sostenible, el análisis será enfocado en el objetivo número nueve, debido a su referencia con la Industria, Innovación e Infraestructuras. El apartado referente a la tecnología, sirve como guía de asesoramiento para la realización de un modelo que permita establecer políticas de ciberseguridad y control de accesos a la infraestructura de red del sistema penitenciario para prevenir ataques phishing y de esta manera proteger los datos del sistema informático SGP.

Aplicando estas mejoras que van alineadas con el Objetivo de Desarrollo Sostenible número nueve, se pueden fortalecer la infraestructura de red, mejorar la eficiencia operativa, aumentar la seguridad y promover la transparencia, garantizando así a los privados de libertad, sus familiares y ciudadanía en general, la gestión efectiva de los datos del sistema informático SGP de un centro penitenciario en el Ecuador.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se establece la descripción de los detalles del proyecto, lo que incluye la contextualización y algunos de los conceptos de seguridad informática que se emplearán.

1.1 Contextualización general del estado del arte

Un ciberataque generalmente es un intento malicioso y concertado por un individuo o gremio para violentar el sistema informático de un objetivo específico. Malware, ransomware, Denial of Service (DoS) o denegación de servicio, phishing, ataques de inyección SQL, Hombre en el medio (MitM), Exploits; son amenazas frecuentes en el ciberespacio. Los tipos de incidentes mencionados, pueden afectar desde pequeñas hasta grandes empresas, instituciones gubernamentales e incluso a personas naturales, causándoles pérdidas económicas importantes (Quirumbay y otros, 2022).

La ciberseguridad se refiere al campo que posibilita la conservación de recursos digitales de información, al encontrar riesgos que acechan la integridad de los datos manipulados, guardados y transmitidos por los sistemas interconectados de información (ISACA, 2017).

El phishing es un tipo de ataque informático, donde el objetivo principal es obtener información personal de alguien. Centra su ataque a partir de un mensaje por el cual el ciberdelincuente pretende engañar a la víctima haciéndose pasar por un posible emisor legítimo del mensaje, le solicitará datos personales y que, dependiendo de los datos que se desea conseguir, se esperaría a que los remitentes respondan al mensaje entregando sus datos personales, o bien utilizar la primera comunicación como un punto de partida para el mismo fin (Pascaner & Prandini, 2019).

A continuación, se detallan diversos tipos de ataques de phishing, sus rasgos principales y las estrategias derivadas de estos ataques destinadas a lograr la sustracción de datos.

Tabla 1.

Tipos y características de ataques phishing.

N°	Tipo de Ataque Phishing	Características Principales
1	Deceptive Phishing	El delincuente cibernético finge ser una entidad o individuo de confianza reconocida por la víctima, con la meta de obtener datos personales o credenciales de acceso a una ubicación específica en línea.
2	Malware - Based Phishing	A través del email, se envía un tipo de software malicioso sea como archivo adjunto o mediante un enlace web incluido en el contenido del mensaje. Este contenido es diseñado para despertar el interés de la víctima, lo que lleva a descargar el software malicioso en su computadora.
3	Spear phishing	Dirigido a un pequeño grupo de individuos dentro de una compañía u entidad, el objetivo es conocido por el ciberdelincuente. Difíciles de detectar y altamente efectivos.
4	Pharming (DNS-Based phishing)	Se origina cuando la víctima accede a sitios web confiables, sin embargo, en realidad, está ingresando a sitios falsos diseñados para robar su información. Estos ataques se llevan a cabo a través de los servidores DNS, son quienes traducen los nombres de dominio de los sitios web que se visitan en direcciones IP correspondientes.
5	Spoofing de correo electrónico	Son correos electrónicos con un encabezado o dirección web que parece original. Esta estrategia es ampliamente utilizada en los ataques de phishing debido a que las personas confían en el remitente del mensaje.
6	Clone Phishing	Consiste en clonar un email de una empresa el cual ha sido recibido previamente (para otorgar una apariencia legítima) y al igual que en otros escenarios, se pide a los usuarios información confidencial. A diferencia del phishing convencional, la información en el correo electrónico original permanece sin cambios, pero se crea una duplicación.
7	Keyloggers y Screenloggers	Los ciberdelincuentes envían a las víctimas un malware que se instala en el equipo, lo que les permite monitorear las pulsaciones del teclado y transmitir la información importante a sus sistemas a través de Internet.
8	Host File Poisoning	Consiste en hacerle creer a la víctima que está iniciando sesión en el sitio web deseado. Esto se logra alterando el archivo de configuración del

		servidor desde el cual el atacante pretende obtener la información, de manera engañosa.
9	Man-in-the-Middle Phishing	Difícil de detectar. El ciberdelincuente se sitúa entre el usuario y la página web, y cuando el usuario está llevando a cabo una transacción en línea, el delincuente cibernético interviene y adquiere el control, duplicando la totalidad de los datos y credenciales del usuario y sustrayéndola. Instruye a la víctima con los pasos necesarios para evitar que sospeche.

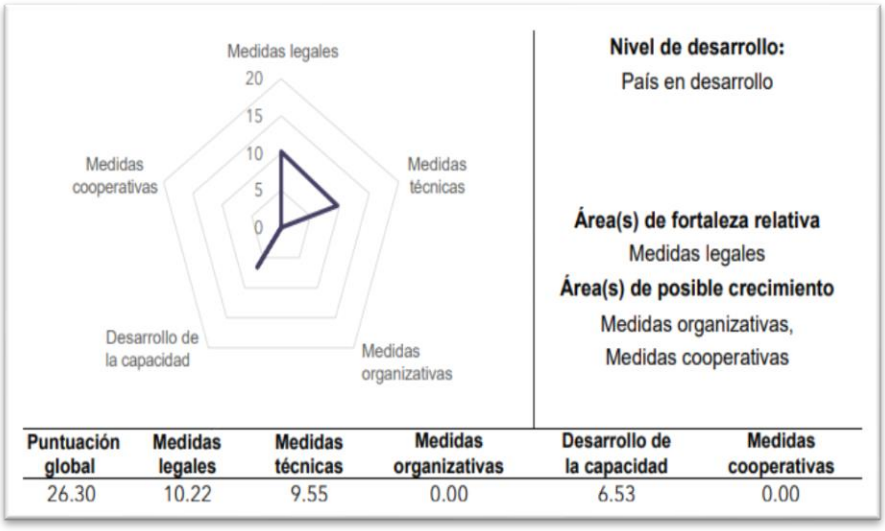
Nota: Elaboración propia con datos de (Leng Chiew, Chek Yong, & Lin Tan, 2018).

Conforme al reporte elaborado por expertos en seguridad de IBM en 2018 (OSI, 2018) el 95 % de los ataques cibernéticos se originan por errores humanos. El uso del Internet es necesario en cualquier actividad diaria, podría decirse que esencial para el desarrollo de las tareas laborales o de ocio de un individuo (Villasis, 2023).

De acuerdo con el Índice de Ciberseguridad Global (ICG) emitido por la Unión Internacional de Telecomunicaciones (UIT) en 2020, alrededor de la mitad de las naciones en todo el mundo han establecido equipos nacionales de respuesta a incidentes informáticos (EIII), señalando un aumento del 11% desde 2018. Específicamente en Ecuador, es evidente que la ciberseguridad está en sus etapas iniciales de desarrollo.

Figura 2.

Estado de la ciberseguridad en el Ecuador



Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
26.30	10.22	9.55	0.00	6.53	0.00

Nota: Índice de Ciberseguridad Global v4 (ITU Publicaciones, 2020)

El creciente uso de IA en nuestro entorno, podría servir para realizar ataques sistemáticos de phishing a cierto tipo de objetivos, como puede ser el personal de un centro penitenciario. Los

ciberdelincuentes pueden emplear la inteligencia artificial con el fin de llevar a cabo ataques de ingeniería social de forma más potente y en una mayor magnitud. Un ejemplo de esto es el perfeccionamiento de los ataques de phishing mediante el uso de métodos avanzados de generación de texto impulsados por la inteligencia artificial. Estos métodos permiten la creación de correos electrónicos que presentan un aspecto más genuino y convincente para las posibles víctimas (Rodríguez, Paya, & Peña, 2023).

El Sistema de Gestión Penitenciaria (SGP) plataforma informática bajo el cuidado del SNAI, que admite el registro de las acciones realizadas por las personas privadas de libertad desde que ingresan a un centro penitenciario como por ejemplo cambios de régimen, cumplimiento de ejes, registro de faltas disciplinarias entre otros (SNAI, 2022).

1.2 Proceso investigativo metodológico

La investigación se describe como un conjunto de pasos sistemáticos, analíticos y respaldados por pruebas que se emplean para analizar un fenómeno o dificultad. Esta investigación se ha dividido en dos enfoques principales: cuantitativo y cualitativo. Siguiendo esta línea, el enfoque cualitativo se caracteriza por la selección y análisis de datos con el fin de refinar las interrogantes de investigación o descubrir nuevas incógnitas durante el proceso de interpretación. (Hernánez, 2014, págs. 4-7).

Relacionando las explicaciones proporcionadas y los propósitos que se buscan lograr mediante este proyecto de tesina, la metodología de investigación es de carácter descriptiva y explicativa, con enfoque cualitativo (sin perjuicio que sea mixto), en virtud que se verificará teoría(s) o técnica(s) de phishing que pueden aplicar los ciberdelincuentes para obtener información personal de funcionarios de un centro penitenciario del Ecuador, que les permita generar accesos no autorizados al sistema informático SGP.

Se planea realizar un análisis documental inherente al tema de esta investigación que permitirá, desde un enfoque científico y académico, estudiar el fenómeno de phishing, analizar la reducción de accesos no autorizados al sistema informático SGP mediante técnicas de anti-phishing.

Igualmente, se recolectará información de primera mano y de manera directa a través del uso de la técnica de la entrevista, para ello se elaborará un cuestionario dirigido al recurso humano especialista del SGP en el Centro de Privación de Libertad Manabí N°4, con el propósito de evaluar amenazas y evidenciar brechas de vulnerabilidad que puedan ser detectadas por ciberdelincuentes para detener los accesos no autorizados.

1.3 Análisis de resultados

Con el propósito de establecer como válida la propuesta investigativa de que las técnicas anti-phishing son una solución acertada que permite mitigar los accesos no autorizados mediante el phishing al Sistema Informático Penitenciario (SGP), se han valorado las siguientes aristas:

La seguridad informática se describe como la destreza de los sistemas de información para conservar su resistencia, con un nivel específico de confiabilidad, frente a incidentes o actividades ilegales que podrían poner en riesgo la disponibilidad, veracidad, integridad y confidencialidad de los datos que una organización almacena o transmite. (Postigo, A., 2020, Unidad 1, P. 2).

Las instituciones públicas del Ecuador, en su afán de preservar y dar el mejor uso posible a sus activos informáticos y salvaguardar la información que generan, establecen políticas de seguridad informática el SNAI no es la excepción. Estas políticas no siempre son las más adecuadas para las instituciones que dividen sus funciones de manera central -la institución en una ciudad- y en territorio -extensiones de la institución en otras ciudades-.

Lo que funciona en la matriz no siempre funciona en la sucursal y es en estos pequeños desajustes que aprovechan los ciberdelincuentes para obtener la información de funcionarios del SNAI que posiblemente no tengan conocimientos informáticos sólidos, terminan siendo engañados por estos profesionales del phishing y entregan sus credenciales de acceso al SGP.

Si bien, el Código Orgánico Integral Penal (COIP) impone penas de privación de libertad de tres a cinco años a los ciudadanos que cometen Phishing -Artículo 230-, no ha sido suficiente para reducir los ataques que sufren a menudo los ciudadanos con acceso al ciberespacio. En este sentido, se ha considerado de manera imprescindible en este estudio, el establecer políticas de ciberseguridad apropiadas para un centro penitenciario, ya que esto ayuda a disminuir la efectividad de los ataques mediante la técnica phishing de manera local en su infraestructura de red, y con esto se puede -entre otros riesgos informáticos- reducir el margen de robo de credenciales que permiten el acceso al Sistema Informático Penitenciario a los funcionarios mediante esta técnica.

Por otro lado, se considera indispensable el fortalecimiento del conocimiento informático del personal que trabaja en una cárcel del Ecuador, ya que si bien es cierto las credenciales de acceso al SGP son entregadas posterior a la suscripción de un acuerdo de confidencialidad, este no garantiza la entrega involuntaria de estas credenciales por parte de los funcionarios a ciberdelincuentes, que tienen experiencia en el campo del phishing, por esta razón, con el plan de capacitación continua de seguridad informática, se reduce aún más la posibilidad de que los funcionarios sean víctimas de phishing y por ende que la institución no pierda información.

CAPÍTULO II: PROPUESTA

El phishing, es una técnica bastante utilizada para conseguir información privada de los usuarios, y el personal que trabaja en un centro penitenciario en el Ecuador, no está exento de ser víctima de estos ataques cibernéticos.

2.1 Fundamentos teóricos aplicados

Ingeniería social

Siempre representa un desafío para la seguridad de todas las redes, sin importar la solidez de sus cortafuegos, enfoques criptográficos y programas antivirus; y que busca influir en personas y compañías con el propósito de que revelen información valiosa y confidencial, en beneficio de los criminales cibernéticos. En la actualidad, de los métodos más utilizados por los atacantes del ciberespacio, es la ingeniería social, la que les sirve para engañar a los usuarios informáticos (Kalnins y otros, 2017).

Ciberataque

El propósito de un ataque cibernético es aumentar la incertidumbre en el sistema de seguridad y supervisión de una entidad o país. En otras palabras, su objetivo es exponer las vulnerabilidades y deficiencias en las medidas de seguridad implementadas por estas entidades y naciones (Cano, 2020).

Además, existen ciertas técnicas de ataques dirigidos y no dirigidos, se detallan a continuación (Tchakounté y otros, 2019):

Ataques dirigidos

Esta categoría de ataque es reconocida debido a que el atacante posee un objetivo particular, ya sea por motivos empresariales o debido a una compensación financiera por llevarlo a cabo. La ejecución de este tipo de ataque demanda una investigación previa para dirigirse hacia el usuario. Este se considera el más perjudicial, ya que se desarrolla con el propósito específico de causar daño al sistema, proceso, entidad o individuo. Algunos ejemplos de esto son el spear-phishing y las botnets.

Ataques no dirigidos

Estos tipos de ataques se dirigen hacia múltiples servicios, dispositivos o usuarios. En esta modalidad, la identidad de la víctima en particular no es relevante, dado que el atacante está consciente de la existencia de dispositivos o computadoras con vulnerabilidades. Por esta razón, utilizan tácticas para aprovechar las debilidades de la red. Algunos ejemplos prominentes de este enfoque incluyen el phishing, el ataque de la fuente envenenada (watering hole) y el ransomware.

Historia del Phishing:

El término Phishing se introdujo por primera vez en 1987 durante una conferencia en la que Jerry Félix y Chris Hauck utilizaron este término en su documento titulado "Sistema de Seguridad: La perspectiva de un Hacker". En dicho documento, se abordaba un enfoque mediante el cual un individuo podría simular ser una entidad de confianza (Aldaz, 2019).

Con el pasar de los años, la técnica del phishing se ha potenciado, lo que conlleva a que cada vez sea más complejo prevenirlo o encontrar a sus autores, ya que los ciberdelincuentes no sólo utilizan el correo electrónico para captar a sus víctimas, sino que se valen de nuevas tácticas.

Etapas del Phishing

Para tener una mejor comprensión de cómo se desarrollan las etapas del phishing, utilizaremos una descripción clara acorde a lo señalado por (Benavides y otros, 2020) (P. 99).

- Planificación y configuración: Se identifica el objetivo, se recaban datos fundamentales sobre la víctima y su infraestructura. Posteriormente, se preparan los ataques mediante los canales elegidos, como sitios web, emails con enlaces nocivos, entre otros.
- Ataque de Phishing: Es donde se da la actividad real, los ciberdelincuentes envían emails falsos a la víctima, usando la base de direcciones de correo electrónico recolectadas, y proceden a solicitar información confidencial a la víctima.
- Infiltración: La víctima da clic en el enlace nocivo entonces, un malware se instala en el dispositivo que está utilizando, de esta manera el atacante accede al sistema y lo compromete según su necesidad. Existen casos que luego de dar clic en el enlace malicioso, este redirige a una página web falsa y así también obtener los datos.
- Recopilación de datos: Estando el ciberdelincuente en sistema de la víctima, recopila y extrae la información deseada.
- Extracción: Habiendo obtenido la información que deseaba, elimina toda la evidencia que pueda comprometerlo con la justicia.

Figura 3.

Etapas de un ataque de Phishing

Nota: Diseño propio

Tipos de Phishing

Phishing regular o tradicional: Este es el método más frecuente, en el cual el usuario obtiene un email en el que se le insta a dar clic en un link que conduce a un sitio web fraudulento, o bien, el propio correo le solicita que comparta información confidencial alegando una necesaria actualización de datos (Wen y otros, 2021).

Phishing basado en malware: Contiene archivos anexos en el correo recibido, estos adjuntos pueden ser software perjudicial o enlaces que dirigen a la descarga de archivos comprometidos (Ivanov y otros, 2021).

Spear Phishing: Está dirigido a una empresa o individuo específico en la organización. El agresor dispone de datos acerca de la víctima, los cuales emplea con el fin de engañar y requerir información delicada (Atmojo, y otros, 2021).

Vishing: Se lleva a cabo mediante comunicaciones telefónicas utilizando VoIP, en las cuales se le indica a la víctima que marque un número particular que aparenta ser el de una empresa legítima, con el objetivo de solicitar y divulgar su información (Hijji & Alam, 2021).

Smishing: Se envía un mensaje de texto (SMS) a los teléfonos móviles, prometiendo beneficios, premios o posibilidades de empleo. Actualmente, esta táctica se extiende a plataformas de mensajería como Facebook Messenger, Instagram, WhatsApp y Telegram (Boukari y otros, 2021).

CEO suplantador: Implica la suplantación de la dirección de email con el propósito de solicitar transferencias de fondos, dirigidas específicamente a empleados dentro de la organización (Ismail y otros, 2021).

Código Orgánico Integral Penal (COIP)

Con motivo de esta investigación, se puede mencionar algunos delitos con sus respectivos artículos, tipificados en el (COIP, 2014) con penas de privación de libertad por cometimiento de delito informático, son:

- Art. 229 Revelación ilegal de bases de datos.
- Art. 230 Interceptación ilegal de datos (Pharming y Phishing).
- Art. 232 Ataque a la integridad de sistemas informáticos.
- Art. 233 Delitos contra la información pública reservada legalmente.
- Art. 234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.
- Art. 476 Interceptación de las comunicaciones o datos informáticos.

Sistema De Gestión Penitenciaria (SGP)

Es un sistema informático destinado al sector de rehabilitación social ecuatoriana, que permite registrar diariamente las actividades que realizan las PPL, desde que ingresan a una cárcel, pasando por los ejes de tratamiento, traslados a otros centros penitenciarios, faltas de indisciplina, posibilidad de acceso a beneficios penitenciarios, entre otros.

En la resolución Nro. SNAI-SNAI-2022-0068-R se determina:

> Artículo 8. Funciones de los encargados de supervisar las áreas de ejes de tratamiento: Los funcionarios que se encuentran a cargo de los ejes de tratamiento en los CPL, sin perjuicio de las responsabilidades previstas en el Reglamento del Sistema Nacional de Rehabilitación Social, tienen que realizar en el SGP: preservar la información de manera clara, actualizada, oportuna, fiable y secuencial.

2.2 Descripción de la propuesta

El sistema informático SGP almacena y alimenta diariamente información digital sensible de las personas adultas con privación de libertad que cumplen una sentencia en los centros penitenciarios del Ecuador. Cada centro penitenciario, maneja su propia población penitenciaria, por esta razón los servidores públicos que laboran en los ejes de tratamiento en territorio, tienen sus credenciales de acceso al sistema, para poder ir actualizando las actividades que realizan los privados de libertad en el ya mencionado sistema. Estas actividades ingresadas en el SGP servirán al privado de libertad al momento de calificar para un beneficio penitenciario, que le permita recuperar su libertad antes del tiempo de su condena.

El phishing, como ya hemos revisado en esta investigación, es una forma de ingeniería social utilizada por ciberdelincuentes con el objetivo de obtener de manera no autorizada información personal a través de varios canales de comunicación, y además es uno de los métodos más utilizados para burlar a las personas para que entreguen información confidencial.

Actualmente, como se encuentra el ámbito de seguridad informática en el Ecuador, se puede decir que, el país no está fuera del radar de los ciberdelincuentes y por ende el personal que trabaja en un centro penitenciario. La información de las PPL en posesión de individuos no autorizados por el sistema de rehabilitación social, podría utilizarse en diferentes escenarios desafortunados para las partes involucradas.

Es necesario establecer acciones, políticas de seguridad y plan de capacitación continua en seguridad informática, que permitan prevenir los ataques de ingeniería social de tipo phishing, para de esta manera dejar menos espacios abiertos a los ciberdelincuentes, y así poder evitar que puedan

conseguir de los funcionarios de un centro de privación de libertad, información que les ayude a obtener las credenciales de acceso al sistema informático SGP de un centro penitenciario en el Ecuador.

Con lo expuesto, las acciones a realizar deberían ser:

- En el centro penitenciario:
  - Evaluar la infraestructura tecnológica actual (Inventario Hardware y Software).
  - Actualizar periódicamente la lista de programas instalados y sistemas operativos.
  - Concienciar sobre generar contraseñas seguras y la autenticación de doble factor.
  - Formación y concienciación del personal sobre seguridad informática.
  - Realizar copias de seguridad de manera periódica en dispositivos extraíbles.
  - Elaborar y ejecutar políticas de ciberseguridad.

Recordando que, la seguridad informática es un proceso constante y evolutivo, que en lugares tan limitados tecnológicamente como un centro de privación de libertad, cuesta su implementación, por esta razón hay que considerar que no existe una solución única o definitiva, por lo que es importante mantenernos informados e irnos adaptando a las nuevas amenazas y desafíos que puedan surgir diariamente.

Figura 4.

Ataque Phishing vía email para obtener credenciales de acceso al SGP.

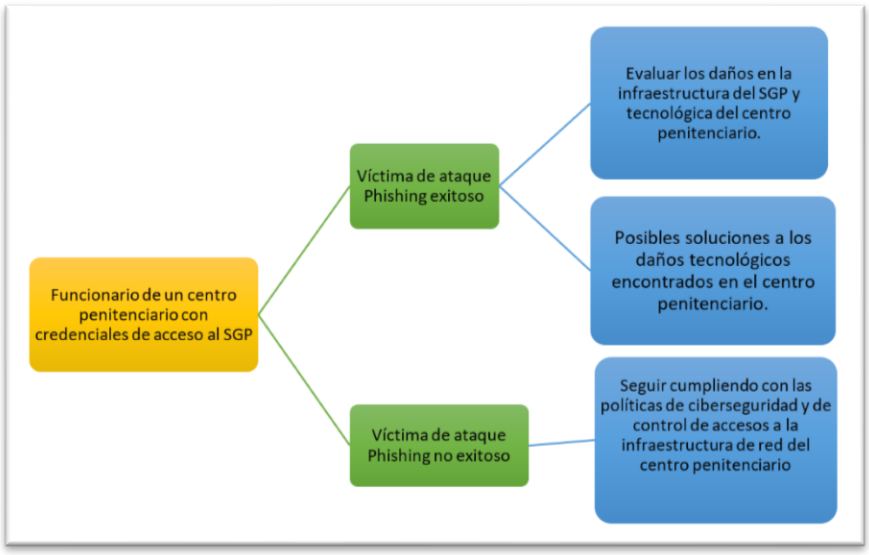
Nota: Diseño propio

Estructura general

A continuación, en la figura 5, se muestra cómo se desarrolla un ataque phishing en un centro penitenciario.

Figura 5**.**

Estructura de ataque y respuesta a phishing en un centro penitenciario



Nota: Diseño propio

a. Explicación del aporte

Para esta investigación, se tomó como muestra los equipos informáticos y el personal que realiza funciones en el Centro de Privación de Libertad Manabí N4 – El Rodeo y que tiene credenciales de acceso al sistema informático SGP.

Partiendo de las carencias informáticas actuales, como el poco conocimiento en el campo de la seguridad informática por parte de los funcionarios o computadores con limitadas características que impiden su actualización, y habiéndose demostrado que el phishing es una técnica de plagio bastante utilizada para conseguir información y que el personal que trabaja en el mencionado centro penitenciario no es ajeno a poder ser víctima de un ataque informático de éstos, es posible que por este medio se obtengan credenciales de accesos de manera no autorizada al sistema informático SGP, en tal razón, es necesario establecer políticas de ciberseguridad y de control de accesos a la infraestructura de red del sistema penitenciario para prevenir ataques phishing, así como capacitar al personal del centro penitenciario en seguridad informática para reducir las posibilidades de caer en el mencionado ataque informático.

Su funcionamiento sería de la siguiente manera, en caso de que sea exitoso un ataque phishing:

Evaluar los daños

- Verificar si hubo robo de información personal del funcionario, ya que esta información podría ser utilizada para vulnerar los accesos a la infraestructura de red.
- Comprobar si hay Infección de malware, porque podría afectar al sistema con virus, ransomware, troyanos u otro software malicioso, que provoque pérdida de información.
- Evidenciar si hubo robo de credenciales para acceso no autorizado al SGP, los ciberdelincuentes pueden obtener los nombres de usuario y contraseñas mediante formularios de inicio de sesión falsos o engañosos enviados a las cuentas de email de los funcionarios.
- Evaluar si existió o no pérdida de datos, ya que esta no solo afecta al funcionario en sus labores sino también en la reputación de la institución.

Soluciones durante un ataque phishing en el centro penitenciario

- Identificar y desconectar el dispositivo afectado, enseñar al funcionario que, si ha notado el incidente, debe desconectar inmediatamente de Internet el equipo para evitar más daños.
- Cambiar contraseñas periódicamente, asegurándose de generar contraseñas robustas, autenticación de doble factor y únicas para cada cuenta.
- Notificar a la matriz de la institución, lo antes posible para informar sobre el incidente y que tomen las medidas necesarias de seguridad.
- Escanear los equipos con antivirus institucional actualizado, esto con la finalidad de detectar y eliminar posibles amenazas y malware.
- Actualizar S.O. y aplicaciones del sistema, las actualizaciones generalmente incluyen parches de seguridad que sirven para proteger contra vulnerabilidades conocidas.
- Educar informáticamente al funcionario que ha sido víctima del phishing, esto puede ayudar a evitar que más funcionarios sean víctimas del mismo ataque.

Y en caso de que no se tengan casos positivos de afectación por Phishing en el centro penitenciario, se deben de seguir las políticas de ciberseguridad y de control de accesos a la infraestructura de red del sistema penitenciario, de la siguiente manera:

- Seguir evaluando la infraestructura tecnológica.
- Actualizar periódicamente software y sistemas operativos.

- Respaldar periódicamente en dispositivos extraíbles.
- Capacitar continuamente al personal sobre seguridad informática.
- Cumplir con las políticas de ciberseguridad propuestas.
- Concienciar del uso de contraseñas seguras y no compartir sus credenciales
- Verificar que los controles de acceso a la infraestructura de red del sistema penitenciario se estén cumpliendo.

b. Técnicas

La seguridad en la infraestructura de red de un centro penitenciario es de suma importancia para evitar incidentes como el que planteamos en esta investigación, ataques de phishing, ya que de ser exitoso uno de estos ataques cibernéticos, podrían comprometerse datos sensibles de las PPL y de funcionarios, facilitar la fuga de información o incluso poner en peligro la seguridad de las instalaciones.

Con esta perspectiva, mediante la técnica de la observación, notar las debilidades tanto en los conocimientos en seguridad informática que tienen los funcionarios como en la infraestructura de red del CPL Manabí N°4, y como esto expone a su personal a ser posibles objetivos de ataques de ingeniería social, específicamente en phishing.

Con la técnica de la entrevista realizada al responsable del soporte y manejo del sistema informático SGP en el CPL Manabí N°4 se logrará tener una visión más clara de las posibles vulnerabilidades en el acceso al sistema informático SGP.

Este proyecto propone implementar políticas de ciberseguridad a la infraestructura de red de un centro penitenciario y capacitar mediante un plan continuo de seguridad informática al personal que labora en el CPL Manabí N°4, haciendo uso de bibliografía acorde a lo que se desea impartir, simulaciones, ejemplos prácticos en las capacitaciones, entre otras.

Al ser el primer centro penitenciario en el que se aplicarían estas políticas de ciberseguridad y plan continuo de capacitación en seguridad informática, y según los resultados que se consigan, este proyecto se podría replicar a los otros treinta y cinco centros penitenciarios que tiene el Ecuador, para de esta manera proteger la infraestructura de red y la información que se genera diariamente de las privados de libertad en el sistema informático SGP de los centros penitenciarios del país.

2.3 Validación de la propuesta

Se mostrarán técnicas antiphishing que ayudarán a dar soporte científico de cómo se debe proceder ante un posible ataque de phishing a los funcionarios del CPL Manabí N°4 que tienen acceso al Sistema Informático SGP.

Antiphishing

Se refieren a aplicaciones diseñadas para identificar el contenido que se introduce de manera maliciosa en páginas web, como el phishing. La relevancia de esta herramienta radica en su capacidad para restringir el acceso no autorizado a datos y material dentro de los sitios web. El antiphishing resguarda contra intentos de obtener sus contraseñas, datos bancarios y otros detalles delicados por medio de páginas web fraudulentas que se camuflan como sitios legítimos (ESET Digital Security, 2022)

Sistemas de prevención de Phishing

Su enfoque radica en prevenir que los ciberdelincuentes obtengan las cuentas de inicio de sesión para un sitio específico, incluso si la víctima ha ingresado a una página maliciosa que imita a una legítima con el propósito de robar sus datos de ingreso, se dividen en dos: sistemas de autenticación de doble factor y gestores de contraseñas (Castellanos, 2020).

Sistemas de autenticación de doble factor

Estos sistemas añaden una capa extra de protección que dificulta a los delincuentes cibernéticos el acceso a los terminales y cuentas en línea de un individuo para robar su información íntima. Incluso si el atacante tiene conocimiento de la contraseña del individuo afectado, la autenticación de doble factor sigue siendo infructuosa, evitando el acceso no consentido. Esto facilita a las instituciones un nivel extra de vigilancia en el acceso a sistemas sensibles, datos y cuentas en línea, salvaguardando esta información de eventuales ataques (Reyes, Salinas, & Mendoza, 2023).

Gestores de contraseñas

Su función implica la creación y el resguardo de contraseñas seguras y confiables para los sitios web que un usuario visita. La mayoría de estos sistemas almacenan las contraseñas de forma cifrada en el navegador del usuario y, de manera automática, completan los formularios cuando el usuario accede a los sitios utilizando las credenciales almacenadas. La principal ventaja de estos programas radica en su capacidad para generar contraseñas exclusivas, extensas, complejas y altamente resistentes a intentos de desciframiento mediante ataques de fuerza bruta (Luevanos, Elizarraras, Hirschi, & Yeh, 2018).

Políticas de Seguridad

La política de seguridad abarca un conjunto de directrices que se extienden a las operaciones del sistema y a los recursos de comunicación que son propiedad de una entidad. Estas directrices engloban aspectos como la salvaguardia física, el personal, la administración y la integridad de la red; se pueden categorizar en: defensa de recursos, autenticación, integridad, no repudio, confidencialidad, actividades de seguridad de auditoría (IBM Corporation, 2015).

Impulsar la innovación en la infraestructura de seguridad de la información que permita a cualquier institución garantizar la confidencialidad y autenticación de la información (Ortega, 2022).

Parámetros para diseñar políticas de seguridad

Se considerarán los siguientes parámetros (Departamento de Tecnología Organización Inca, 2018).

- Realizar una evaluación de riesgos en el ámbito informático con el fin de valorar los activos, permitiendo así ajustar las políticas a la situación actual de la compañía.
- Entablar encuentros con los departamentos responsables de los recursos, dado que cuentan con la experiencia y son la principal fuente para determinar el alcance e identificar las infracciones a las normas establecidas.
- Informar a todos los miembros del equipo involucrados acerca de la elaboración de las políticas, abarcando los aspectos positivos, los riesgos asociados a los recursos, activos y elementos de seguridad.
- Determinar quiénes poseen la capacidad de tomar decisiones en cada departamento, ya que son estos individuos quienes tienen un interés en proteger los activos cruciales de sus respectivas áreas.
- Realizar un seguimiento regular de los procedimientos y actividades de la empresa para permitir la actualización oportuna de las políticas en caso de cambios.
- Describir de manera precisa y clara el alcance de las políticas con el objetivo de prevenir conflictos al momento de implementar los mecanismos de seguridad en concordancia con las directrices establecidas.

2.4 Matriz de articulación de la propuesta

En esta matriz se resume cómo se vincula el producto elaborado con los fundamentos teóricos, metodológicos, estratégico-técnicos y tecnológicos que se utilizaron.

Tabla 2.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
SGP	Sistema informático que contiene información de las personas privadas de libertad desde su ingreso, cumplimiento de ejes de tratamiento, traslados, entre otros	La metodología es bibliográfica, ya que la resolución emitida permite conocer el porqué de este sistema informático.	Mediante la observación Identificar vulnerabilidades en el acceso al SGP. Mediante entrevista con el experto en el manejo del sistema informático conocer posibles brechas de inseguridad.	Con las políticas de ciberseguridad planteadas se mejora el proceso de seguridad de acceso al SGP	Fuente bibliográfica, Resolución Nro. SNAI-SNAI-2022-0068-R, 2022
Políticas de Ciberseguridad	(Carrillo, Zambrano, Zambrano, & Bravo, 2020) propone en 3 ámbitos las políticas: Auditoría interna a los métodos de las áreas de Redes, Desarrollo de Software y Documentación; Análisis de Vulnerabilidades e Identificación de	La metodología es bibliográfica, con información recabada se desarrolló la propuesta.	Mediante bibliografía, se aplican mecanismos de control para potenciar la seguridad de la infraestructura de red del centro penitenciario	Reducción de accesos no autorizados al SGP mediante la técnica de phishing.	Fuente bibliográfica y observación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
	Riesgos.				
Plan de capacitación continua en seguridad informática	Se propone, luego de realizado el diagnóstico del personal que trabaja en el centro penitenciario y notar sus carencias en conocimientos de seguridad informática.	La metodología es bibliográfica, con información que se recabó se desarrolló la propuesta.	Concienciar sobre los riesgos que implica desconocer temas de seguridad informática.	Minimizar el riesgo de ser víctima de un ataque phishing, mejorando el conocimiento informático del factor humano.	Fuente bibliográfica y observación
Seguridad Informática	(UNIR, 2021) Hace referencia a resguardar la información, cómo se la trata, con el propósito de prevenir la alteración de datos y procedimientos.	Metodología bibliográfica	Capacitaciones al personal del centro de privación de libertad.	Comprender las ventajas del conocimiento sobre posibles ataques informáticos.	Fuente bibliográfica
Phishing	(APWG, 2020) Se utilizan tácticas de manipulación psicológica para sustraer la información personal de identidad y las	Metodología bibliográfica	Técnicas para reconocer un correo electrónico phishing.		Fuente Bibliográfica

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
	contraseñas de las cuentas digitales de los usuarios.				
Antiphishing	Son sistemas diseñados para proteger a los usuarios de los ataques de phishing (Sharma, Dash, & Ansari, 2022)		Técnicas para prevenir y reducir la eficacia de un ataque phishing		Fuente Bibliográfica

Fuente: Elaboración propia

CONCLUSIONES

Establecer barreras para evitar accesos no autorizados a la infraestructura de red de la institución, se demuestra el compromiso de la entidad gubernamental en reducir posibles ataques phishing, proteger la privacidad y la integridad de los datos de los sistemas informáticos de la institución como el SGP.

Realizando de manera periódica escaneos de vulnerabilidad, de manera directa no se pudo evidenciar acceso al SGP sin autorización previa, sin embargo, se pudo identificar como vulnerabilidades indirectas -que pueden ser aprovechadas por ciberdelincuentes- las siguientes: parches para activar paquetes de ofimática o sistemas operativos, desactualización de sistema operativo, no tener un antivirus de uso institucional actualizado y permisos de navegación en las cuentas de usuario para conexión externa mediante software de acceso remoto.

Se determinó que los daños potenciales que pueden causarse en el sistema informático SGP con un ataque phishing exitoso es la pérdida o secuestro de información como, por ejemplo: identidad, delitos, boletas de encarcelación y excarcelación, registro de faltas disciplinarias y actividades realizadas para obtención de beneficios penitenciarios de las personas con privación de libertad a nivel nacional.

Con la implementación de políticas de ciberseguridad a la infraestructura de red del centro penitenciario, como por ejemplo, la autenticación de doble factor para las credenciales de acceso de los funcionarios, restricción de puertos para soporte fuera de la red de la institución, generar contraseñas seguras, mantener actualizados los sistemas con los últimos parches de seguridad o tener un antivirus institucional actualizado, entre otras políticas propuestas, la institución se prepara para los desafíos actuales en seguridad informática.

El ejecutar el plan de capacitación continua acerca de seguridad informática a los funcionarios del centro penitenciario, proporciona una cultura de seguridad informática, ya que enseña al personal a identificar y evitar ataques de phishing, indicativo de que la institución está tomando medidas para proteger datos confidenciales y personales tanto de la población penitenciaria como del personal a cargo de resguardar los sistemas informáticos en el centro penitenciario.

RECOMENDACIONES

Una institución que establece acciones concretas para prevenir ataques de phishing y asegurar sus sistemas informáticos, demuestra una preocupación real por la seguridad informática y que está tomando acciones requeridas para asegurar la protección y cohesión de los datos confidenciales y generar confianza en las partes interesadas, por esta razón se recomienda.

Se recomienda para prevenir vulneraciones en la infraestructura de red, realizar de manera periódica las siguientes acciones: actualización del software en los computadores, adquirir licencias originales para el software que así lo requiera o recurrir al software libre, generar contraseñas robustas y autenticación de doble factor, entre otras; y para mejor implementación de lo propuesto, la adquisición de computadores con nuevas y mejores características que los actuales, sería más beneficioso para la institución.

Para disminuir la posibilidad de pérdida de información del sistema informático SGP con un ataque exitoso de phishing, se recomienda establecer directrices claras sobre el uso del correo electrónico institucional y cómo los funcionarios deben actuar al recibir mensajes no solicitados, de dudosa procedencia o enlaces sitios web sospechosos.

Con base en las normas de la ISO 27001 si la institución desea garantizar la privacidad constante, la integridad y la disponibilidad de la información, además de cumplir con los requisitos legales correspondientes, para reducir significativamente el riesgo de ser víctimas de los ataques de phishing y proteger los datos generados en el sistema informático SGP de forma más efectiva, se recomienda ejecutar de manera consciente y permanente las políticas de ciberseguridad propuestas; y siempre que considere necesario, se puede restructurar el SGP o la implementación de un nuevo sistema informático que brinde mejores posibilidades de seguridad y control de accesos.

En concordancia con el Esquema Gubernamental de Seguridad de la Información (EGSI) se recomienda que, en el plan de capacitación continua para el personal del centro penitenciario, se aborden ciertos criterios que se hayan documentado previamente y que detallen -para cada clase de riesgo- qué medida se debe tomar y la importancia o urgencia con la que el funcionario debe reaccionar. Este tipo de nociones se pueden replicar las veces que se considere necesario, ya que el reforzamiento en los conceptos ayudará a que la información sea repetida más veces y por más personas, lo cual será beneficioso para los funcionarios y por ende para la institución.

BIBLIOGRAFÍA

Aldaz, W. (2019). VULNERABILIDADES DE SEGURIDAD INFORMÁTICA EN LA ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO" A TRAVÉS DEL PHISHING. *Universidad Tecnológica Israel*.

APWG. (2020). *Phishing Activity Trends Report.* Obtenido de 4th Quarter San Francisco: A.P.W. Group, 2020: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

Atmojo, Y., Susila, M., Hilmi, M., Rini, E., Yuningsih, L., & Hostiadi, D. (2021). A New Approach for Spear phishing Detection. *IEEE*. doi:10.1109/EIConCIT50028.2021.9431890

Benavides, E., Fuertes, W., Sanchez, S., & Nuñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Revista Ciencia y Tecnología OJS, 13*(1), 97–104. doi:https://doi.org/10.18779/cyt.v13i1.357

Boukari, B., Ravi, A., & Msahli, M. (2021). Machine Learning detection for SMiShing frauds. *IEEE*. doi:10.1109/CCNC49032.2021.9369640

Cano, J. (2020). ¿Por qué los ciberataques son inevitables?: Prácticas y capacidades claves de la ciberseguridad empresarial. *Voces diversas y disruptivas en tiempos de Revolución, 4*, 223-248. doi:10.29236/sistemas.n157a6

Carrillo, J., Zambrano, N., Zambrano, T., & Bravo, M. (2020). Proceso de Ciberseguridad: Guía Metodológica para su implementación. *Revista Ibérica de Sistemas e Tecnologias de Informação, (E29)*, 41-50. doi:http://www.risti.xyz/issues/ristie29.pdf

Castellanos, P. (2020). Ataques tecnológicos de ingeniería social en sistemas de red. "Anti-phishing Web con Machine Learning". *Universidad Nacional de Educación a Distancia (España)*. doi:http://e-spacio.uned.es/fez/view/bibliuned:master-ETSInformatica-II-Pcastellanos

COIP. (2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL.* La Asamblea Nacional del Ecuador. doi:https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Departamento de Tecnología Organización Inca. (2018). *Políticas de seguridad informática (PSI).* Obtenido de Centro Inca: https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

ESET Digital Security. (2022). *[KB3100]*. Obtenido de ¿Cómo funciona el Anti-Phishing en ESET Smart Security y ESET NOD32 Antivirus?: https://support.eset.com/es/kb3100-como-funciona-el-anti-phishing-en-eset-smart-security-y-eset-nod32-antivirus

Guaña, J., Sánchez, A., Chérrez, P., Chulde, L., Jaramillo, P., & Pillajo, C. (2022). Ataques informáticos más comunes en el mundo. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 87-100.

Hernánez, R. (2014). *Metodología de la investigación Sexta edición.* McGraw-Hill/Interamericana Editores S.A. de C.V.

Hijji, M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic:Challenges and Prospective Solutions. *IEEE Access, 9*, 7152-7169. doi:https://doi.org/10.1109/ACCESS.2020.3048839

IBM Corporation. (2015). *Política y objetivos de seguridad*. Obtenido de La política de seguridad: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

ISACA. (2017). *www.isaca.org*. Obtenido de Fundamentos de Ciberseguridad Guía de Estudio, Segunda Edición: www.isaca.org/cyber

Ismail, S., Alkawaz, M., & Kumar, A. (2021). Quick Response Code Validation and Phishing Detection Tool. *TEEE llth IEEE Symposium on Computer Applications 8 Industrial Electronics (ISCAIE)*, 261-266. doi:10.1109/ISCAIE51753.2021.9431807

ITU Publicaciones. (2020). *Índice Mundial de Ciberseguridad*. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

Ivanov, M., Kliuchnikova, B., Chugunkov, I., & Plaksina, A. (2021). Phishing Attacks and Protection Against Them. *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering.* St. Petersburg, Moscow: ElConRus. doi:10.1109/ElConRus51938.2021.9396693

Kalniņš, R., Puriņš, J., & Alksnis, G. (2017). Security evaluation of wireless network access points. *Applied Computer Systems., 21*(1), 38-45. doi:10.1515/acss-2017-0005

Koyun, A., & Al Janabi, E. (2017). Social Engineering Attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST), 4*, 7533-7538.

Leng Chiew, K., Chek Yong, K., & Lin Tan, C. (2018). A Survey of Phishing Attacks: Their Types, Vectors and Technical approaches. *Expert Systems With Applications ScienceDirect , 106*, 1-20. doi:https://doi.org/10.1016/j.eswa.2018.03.050

Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J.-h. (2018). Analysis on the Security and Use of Password Managers. *IEEE Xplore*. doi:DOI 10.1109/PDCAT.2017.00013

Ortega, S. (2022). ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE. *Universidad Tecnológica Israel*.

Pascaner, D., & Prandini, P. (2019). Efectividad de campañas anti-phishing. *XIII Simposio de Informática en el Estado (SIE 2019) - JAIIO 48.* Salta. Obtenido de http://sedici.unlp.edu.ar/handle/10915/89725

Postigo Palacios, A. (2020). *SEGURIDAD INFORMÁTICA (EDICIÓN 2020).* Ediciones Paraninfo. doi:https://books.google.com.ec/books?hl=es&lr&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=pol%C3%ADticas+de+seguridad+inform%C3%A1tica&ots=-H1Vpq7Th6&sig=NnpWOshC0eSo-g0snsYrfOD2M0Q&redir_esc=y#v=onepage&q=pol%C3%ADticas%20de%20seguridad%20inform%C3%A1tica&f=false

Quirumbay Yagual, D. I., Castillo Yagual, C. A., & Coronel Suárez, I. A. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE, 9*(1), 57- 65. doi:http://dx.doi.org/10.26423/rctu.v9i1.671

Reyes, A., Salinas, J., & Mendoza, A. (2023). Modelode Autentificaciónde Doble Factor. *Revista Innovación y Software, 4*(1), 82-95. doi:https://revistas.ulasalle.edu.pe/innosoft/article/view/81/99

Rodríguez, V., Paya, C., & Peña, B. (2023). Estudio criminológico del ciberdelincuente y sus víctimas. *Cuadernos de RES PUBLICA en derecho y criminología.*(1), 95–107. doi:https://doi.org/10.46661/respublica.8072

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet MDPI*, 2-17. doi:https://doi.org/10.3390/fi11040089

Sharma, P., Dash, B., & Ansari, M. (2022). Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms. *International Journal of Advanced Research in Computer and Communication Engineering, 11*(7), 153-160. doi:10.17148/IJARCCE.2022.11728

SNAI. (2022). *Resolución Nro. SNAI-SNAI-2022-0068-R.* Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes Infractores.

Tchakounté, F., Nyassi, V., & Udagepola, K. (2019). True Request–Fake Response: A New Trend of Spear Phishing Attack. *Journal of Network Security, 7*(3), 1-17. doi:https://www.researchgate.net/publication/338634278_True_Request-Fake_Response_A_New_Trend_of_Spear_Phishing_Attack

UNIR. (15 de 06 de 2021). *¿Qué es la seguridad informática y cuáles son sus tipos?* Obtenido de https://ecuador.unir.net/: https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

Villasis, M. (2023). ANÁLISIS DE BRECHAS DE SEGURIDAD EN REDES LPWAN: SIGFOX Y LORAWAN EN BASE A LA NORMA ISO 27001:2013. *Universidad Tecnológica Israel*.

Wen, H., Fang, J., Wu, J., & Zheng, Z. (2021). Transaction-based Hidden Strategies Against General Phishing Detection Framework on Ethereum. *IEEE International Symposium on Circuits and Systems (ISCAS)*. doi:10.1109/ISCAS51556.2021.9401091

ANEXOS

ANEXO 1

POLITICAS DE CIBERSEGURIDAD PARA EL CPL MANABI N°4

1. **Políticas de acceso a los equipos y red institucional:**

- Las credenciales de acceso al computador y al Internet que tendrán los funcionarios, serán diferenciadas, la política de accesos será acorde a las funciones que desempeñan.
- Solo el personal responsable de ejes de tratamiento, podrá tener acceso al sistema informático SGP, pero solo a los módulos correspondientes a su campo de trabajo.
- Todas las cuentas sin distinción alguna, tendrán que utilizar autenticación de dos factores para reforzar la seguridad de las cuentas.
- Restricción de puertos para soporte remoto fuera de la red institucional.

2. **Concienciación del personal:**

- Ejecutar el plan de capacitación continua sobre seguridad informática al personal del centro penitenciario.
- Informar de manera periódica vía correo electrónico, sobre las mejores prácticas y cómo reconocer posibles amenazas informáticas, como el phishing.
- Instar al personal a que accedan a páginas con https.

3. **Monitoreo continuo:**

- Implementar sistemas de monitoreo de seguridad automáticos en la red para identificar actividades inusuales o maliciosas en tiempo real.

4. **Actualizaciones y parches:**

- Mantener todos los sistemas y software actualizados con los últimos parches de seguridad para evitar la explotación de vulnerabilidades previamente documentadas o encontradas gracias al monitoreo continuo de los sistemas.

5. **Gestión de contraseñas:**

- Establecer políticas estrictas de gestión de contraseñas, estas incluyan la creación de contraseñas seguras, robustas y su cambio obligado de manera periódica.

6. **Segmentación de redes:**

- Dividir la red en segmentos para limitar la propagación de amenazas y mantener separados los sistemas considerados críticos de los sistemas menos sensibles.

7. **Respaldo de datos:**

- Realizar copias de seguridad periódicas de los datos considerados críticos y almacenarlos en ubicaciones seguras y separadas de la red principal.

8. **Respuesta a incidentes:**

- Desarrollar un plan de respuesta a incidentes minucioso, que establezca el paso a paso, en caso de una violación de seguridad informática.
- En caso de incidente, realizar la notificación de las áreas afectadas y la cooperación de las autoridades pertinentes.

ANEXO 2

PLAN DE CAPACITACIÓN DE SEGURIDAD INFORMÁTICA PARA EL PERSONAL ADMINISTRATIVO Y DE SEGURIDAD DEL CPL MANABI N°4

Considerando que el personal del CPL Manabí N°4 posee un conocimiento limitado en cuanto a seguridad informática, es esencial aumentar la conciencia y su preparación ante amenazas cibernéticas.

Objetivo Principal:

Mejorar el conocimiento y las habilidades del personal del CPL Manabí N°4 con respecto a la seguridad informática para reducir el riesgo de amenazas cibernéticas.

Duración:

El plan de capacitación es continuo y estará distribuido en varias semanas, acorde a los espacios que brinde la autoridad local para la convocatoria del personal.

Módulo 1: *Introducción a la seguridad informática*

Objetivos:

- Comprender la importancia de la seguridad informática.
- Reconocer las amenazas comunes en línea.

Contenido:

- ¿Qué es la seguridad informática?
- Razones para preocuparse por la seguridad informática.
- Amenazas cibernéticas comunes: malware, phishing, ingeniería social.

Módulo 2: ***Contraseñas seguras y autenticación***

Objetivos:

- Aprender a crear contraseñas seguras.
- Comprender la importancia de la autenticación de dos factores.

Contenido:

- Cómo crear contraseñas fuertes.
- Importancia de no reutilizar contraseñas.
- Introducción a la autenticación de dos factores (2FA).

Módulo 3: Correo electrónico y phishing

Objetivos:

- Identificar correos electrónicos de phishing.
- Saber cómo actuar frente a correos electrónicos sospechosos.

Contenido:

- ¿Qué es el phishing?
- Cómo reconocer correos electrónicos de phishing.
- Qué hacer si se recibe un correo electrónico sospechoso.

Módulo 4: Uso seguro de dispositivos y redes

Objetivos:

- Comprender cómo proteger dispositivos y redes.
- Reconocer riesgos al conectarse a redes públicas.

Contenido:

- Actualizaciones y parches: por qué son importantes.
- Conexiones seguras a redes Wi-Fi.
- Riesgos de redes públicas y cómo protegerse.

Módulo 5: Seguridad en redes sociales y en línea

Objetivos:

- Conocer los riesgos y la privacidad en las redes sociales.
- Aprender sobre el uso seguro de la web.

Contenido:

- Configuración de privacidad en redes sociales.
- Riesgos de compartir información personal en línea.
- Sitios web seguros y no seguros.

Módulo 6: Buenas prácticas de seguridad informática

Objetivos:

- Adquirir conocimientos prácticos para mantenerse seguro en línea.
- Aprender a mantener la seguridad de manera continua.

Contenido:

- Respaldo de datos: por qué es importante.
- Actualizaciones y parches continuos.
- Evitar la descarga de software no confiable.

Módulo 7: Evaluación y simulación de amenazas

Objetivos:

- Poner en práctica lo aprendido mediante ejercicios de simulación.
- Evaluar la comprensión y la capacidad para identificar amenazas.

Contenido:

- Ejercicios prácticos de identificación de correos electrónicos de phishing.
- Simulaciones de amenazas cibernéticas y cómo responder.

Evaluación final: Prueba de seguridad informática

Objetivo:

- Evaluar el conocimiento adquirido por el personal administrativo y de seguridad del CPL Manabí N°4.

Contenido:

- Prueba escrita sobre conceptos clave de seguridad informática.

Es necesario precisar que, el plan de capacitación puede adaptar el contenido de los módulos según las necesidades y características que se vayan notando en el personal del centro penitenciario. Remarcando que la repetición y el refuerzo de los conceptos impartidos, siempre serán esencial para garantizar la retención y aplicación de lo aprendido en este plan de capacitación de seguridad informática.

Entrevista 1

UNIVERSIDAD TECNOLÓGICA ISRAEL
Maestría en Seguridad Informática
2023

El objetivo del presente instrumento es conocer desde la óptica del responsable del manejo y soporte en el CPL Manabí N°4 del Sistema de Gestión Penitenciaria SGP, sus apreciaciones acerca de lo relacionado con la seguridad en el acceso al mencionado sistema informático.

Datos personales

Nombre y Apellido:	Orly Gioberty Cevallos Menéndez			
Título Académico:	Economista	**Otro(s) Títulos Académicos**	**Magister**	**PHD**
			X	
Cargo del funcionario:	Líder Estadístico del Centro de Privación de Libertad MANABI # 4 – EL RODEO			
Fecha de la entrevista:	16 agosto de 2023			

Banco de preguntas

1. **¿Cuál es su experiencia y formación en sistemas informáticos?**

   R: Soy Tecnólogo Programador de Sistemas, y Analista de Sistemas, otorgados por la Universidad Técnica de Manabí.

   Tengo 24 años de trabajar en el sistema penitenciario del Ecuador. Desde el 01 marzo de 2019 me encuentro cumpliendo funciones como Líder Estadístico en el Centro de Privación de Libertad MANABI # 4 – EL RODEO, es decir, conozco el manejo del Sistema de Gestión Penitenciaria (SGP) desde esa fecha hasta la presente.

2. **¿Cómo se mantiene actualizado en cuanto a las últimas tendencias y avances en sistemas informáticos?**

   R: A través de la lectura y seguir publicaciones en Internet en avances tecnológicos.

3. **¿Tiene conocimientos en seguridad informática?**

   R: Actualmente un poco desactualizado, ya que el campo en que me desempeño es muy amplio, por lo que realice estudios en otras áreas como Tributación y Finanzas,

Economía, además mi actual ocupación es llevar el control de los ingresos y salidas de personas privadas de la libertad (PPL) a través del manejo del Sistema de Gestión Penitenciaria (SGP), que por cierto, cuenta con varios módulos entre ellos a citar, Dactiloscopia, Jurídico, Educativo, Laboral, Trabajo Social, etc.

4. **¿Conoce qué es la ingeniería social?**

   R: Tengo entendido que es cuando se obtiene información confidencial de los usuarios de manera ilegal.

5. **¿Ha escuchado o conoce qué es la técnica informática phishing?**

   R: El phishing es una técnica de ingeniería social que consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario.

6. **¿Considera Usted que el acceso al Sistema de Gestión Penitenciaria SGP es seguro?**

   R: Bueno. Según la experiencia que tengo desde el 01 marzo de 2019 en el manejo del Sistema de Gestión Penitenciaria (SGP) hasta la presente fecha, es que la Base de datos del Sistema SGP fue hackeada en una ocasión. Desconozco las mejoras que se hayan implementado en seguridad informática después de este ataque a la DATA del Sistema SGP, ya que esto se lo realizó en la Planta Central del Servicio Nacional de Atención Integral a personas adultas privadas de la libertad y a Adolescentes infractores (SNAI). A partir de este último suceso, no hemos tenido otro intento de hackeo en la DATA de este Sistema informático hasta la presente fecha, y se podría decir, que hasta el momento el acceso al Sistema de Gestión Penitenciaria si es seguro.

7. **Cree Usted que el personal del Centro Penitenciario que tiene acceso al SGP, ¿posee conocimientos informáticos necesarios para reconocer un email phishing?**

   R: Lamentablemente mi respuesta es que no poseen conocimientos informáticos necesarios para poder reconocer un email phishing. Funcionarios desde la Planta Central SNAI se activan inmediatamente para comunicar a través de un correo electrónico institucional oficial a todos los servidores públicos que laboran en el SNAI a fin de que ignoren esta clase de email phishing.

8. **Desde su experiencia, ¿considera usted que los funcionarios con acceso al SGP colocan contraseñas seguras a su cuenta de acceso?**

   R: Lamentablemente mi respuesta es que no colocan contraseñas seguras a su cuenta de acceso al Sistema de Gestión Penitenciaria (SGP), son demasiado predecibles.

9. **¿Considera que es necesaria la capacitación en seguridad informática al personal del CPL Manabí con acceso al SGP?**

   R: Mi respuesta es rotunda, SI.

10. **Si tuviera la posibilidad de hacerlo, ¿Cómo mejoraría la seguridad en el acceso al SGP?**

    R: Para poder tener acceso al Sistema de Gestión Penitenciaria (SGP) antes se ingresaba con la misma clave de acceso que se enciende el computador de escritorio (trabajo), es decir, eran las mismas. Actualmente han cambiado el URL para poder tener acceso al Sistema SGP que es el siguiente https://192.168.1.33/?db=sgp# y la clave es dada por el personal de la Dirección de Tecnologías de la información y comunicación del SNAI, a los funcionarios que nos encontramos en territorio (es decir, en los Centros de Privación de Libertad del país). Cambiar la forma de acceso al sistema.

Firmado electrónicamente por:
ORLY GIOBERTY
CEVALLOS MENENDEZ

_____

Firma

ANEXO 4

Validación de la propuesta

Propuesta de acciones para evitar incidentes de phishing al sistema informático S.G.P de un centro penitenciario de Ecuador.

Evaluador: Christian Hernán Rosero Solís.
Ingeniero en Sistemas Informáticos.
Director Nacional de la Dirección de Tecnologías de la Información y Comunicaciones del Servicio Nacional de Atención Integral a Personas Privadas de la Libertad y a Adolescentes Infractores.

He revisado la propuesta de titulación de la Ing. Andrea Viviana Solórzano Coello, respecto al cumplimiento de las acciones para evitar incidentes de phishing al sistema informático S.G.P de un centro penitenciario de Ecuador y considero que la propuesta acompañada de las nuevas adquisiciones tecnológicas que ha realizado la institución, es adecuada para ser ejecutada en el CPL Manabí N4 El Rodeo.

Observaciones: Esta propuesta de acciones para evitar incidentes de phishing al sistema informático Sistema Gestión Penitenciaria (SGP) de un centro penitenciario de Ecuador, demuestra el compromiso con la privacidad y la ética en el cuidado y tratamiento de la información digital generada en el mencionado sistema informático. Con la implementación de estas medidas, se contribuye con el fortalecimiento de la relación de confianza entre las partes involucradas en el sistema de rehabilitación social del Ecuador.

La interesada puede hacer uso de este documento para sus fines académicos pertinentes.

Atentamente;

Ing. Christian Hernán Rosero Solís,
Director de Tecnologías de la Información y Comunicación,
Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes.

ANEXO 5

Validación de la propuesta

Propuesta de acciones para evitar incidentes de phishing al sistema informático S.G.P de un centro penitenciario de Ecuador.

Evaluador: Odilo Eusebio Ipiales González.
Ingeniero en Sistemas Informáticos.
Responsable del funcionamiento del S.G.P.
Analista de la Dirección de Tecnologías de la Información y Comunicaciones del Servicio Nacional de Atención Integral a Personas Privadas de la Libertad y a Adolescentes Infractores.

He revisado la propuesta de titulación de la Ing. Andrea Viviana Solórzano Coello, respecto al cumplimiento de las acciones para evitar incidentes de phishing al sistema informático S.G.P de un centro penitenciario de Ecuador y considero que la propuesta acompañada de las nuevas adquisiciones tecnológicas que ha realizado la institución, es adecuada para ser ejecutada en el CPL Manabí N4 El Rodeo.

Observaciones: Esta propuesta de acciones para evitar incidentes de phishing al sistema informático Sistema Gestión Penitenciaria (SGP) de un centro penitenciario de Ecuador, demuestra el compromiso con la privacidad y la ética en el cuidado y tratamiento de la información digital generada en el mencionado sistema informático. Con la implementación de estas medidas, se contribuye con el fortalecimiento de la relación de confianza entre las partes involucradas en el sistema de rehabilitación social del Ecuador.

La interesada puede hacer uso de este documento para sus fines académicos pertinentes.

Atentamente;

Firmado electrónicamente por:
ODILO EUSEBIO IPIALES GONZALEZ

Ing. Odilo Eusebio Ipiales González
Analista de Tecnologías de la Información y Comunicación,
Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes.