UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Comunicación y Artes Contemporáneas

La comunicación estratégica como herramienta para prevenir ataques de seguridad informática.

.

Martín Sebastián Garzón Yánez

Comunicación

Trabajo de fin de carrera presentado como requisito
para la obtención del título de
LICENCIADO EN COMUNICACIÓN

Quito, 16 de diciembre de 2024

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Comunicación y Artes Contemporáneas

HOJA DE CALIFICACIÓN
DE TRABAJO DE FIN DE CARRERA

Trabajo de titulación de Comunicación

Martín Sebastián Garzón Yánez

Nombre del profesor, Título académico **María José Enríquez Cruz, PhD en Comunicación**

Quito, 16 de diciembre del 2024

© DERECHOS DE AUTOR

Nombres y apellidos: Martín Sebastián Garzón Yánez

Código: 00216996

Cédula de identidad: 1727470336

Lugar y fecha: Quito, 16 de diciembre del 2024

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

RESUMEN

El presente trabajo tiene como objetivo ofrecer una perspectiva única de cómo la comunicación estratégica funciona como una herramienta eficaz para prevenir y mitigar ataques de seguridad informática. Hoy en día, las vulneraciones a los sistemas digitales son cada vez más comunes; los ciberdelincuentes emplean distintos métodos de hackeo, y con éxito, engañan a los individuos porque se aprovechan de su desconocimiento. Dado a que la seguridad informática parte del principio de corregir vulnerabilidades, este marco teórico busca brindar diferentes soluciones a través de la correcta aplicación de la comunicación organizacional y en crisis a una de las vulnerabilidades más grandes en un sistema informático, el usuario. Como metodología, se realizó una revisión bibliográfica y cualitativa donde se reúne el conocimiento de varios expertos en las diferentes áreas de comunicación e informática para combinarlos y ofrecer una respuesta ante la dificultad planteada desde un punto de vista comunicacional.

De igual forma, se planificó, diseñó y ejecutó una campaña de Comunicación con acciones internas y externas cuya naturaleza busca proliferar el mensaje de prevención en los usuarios. Dicha iniciativa consiguió tres aliados estratégicos donde ejecutar charlas sobre ciberseguridad y se logró la instrucción en ciberseguridad de más de 50 colaboradores en total. También, se consiguió un espacio en 4 medios de comunicación donde se informó sobre prácticas de seguridad informática y se elaboró una página de protección cibernética en la red social Instagram que consiguió 207 seguidores. Por otra parte, la campaña se juntó con otras iniciativas y se realizó un evento que recibió bastante acogida con más de 60 asistentes. El trabajo concluye con el uso de una campaña de comunicación como un artilugio valioso para la seguridad informática, donde la adecuada transmisión de mensajes internos sirve para construir rutinas consideradas con la integridad digital de la empresa. Así, las charlas deben ser informativas, dinámicas y pertinentes para no aburrir a los funcionarios y transmitir

correctamente el mensaje de cuidado y desconfianza en entornos informáticos. Este tema, debido a su utilidad, trasciende y es útil para todo tipo de audiencias, por ende, es importante cada estrategia de comunicación y su adaptación a cada medio para alcanzar al mayor número de usuarios posibles.

Palabras clave: comunicación, ciberseguridad, hacking, crisis, información, mensajes, organización.

ABSTRACT

The present work aims to offer a unique perspective on how strategic communication functions as an effective tool to prevent and mitigate cyber security attacks. Nowadays, breaches of digital systems are increasingly common; cybercriminals employ various hacking methods and successfully deceive individuals by taking advantage of their lack of knowledge. Since cybersecurity is based on the principle of correcting vulnerabilities, this theoretical framework seeks to provide different solutions through the proper application of organizational and crisis communication to address one of the biggest vulnerabilities in an IT system: the user.As a methodology, a bibliographic and qualitative review was conducted, gathering the knowledge of various experts in communication and IT fields to combine and offer a solution to the proposed issue from a communication standpoint. Similarly, a communication campaign was planned, designed, and executed with internal and external actions aimed at spreading the message of prevention among users. This initiative secured three strategic allies to deliver cybersecurity talks and successfully trained more than 50 employees on cyber security. Additionally, space was secured in four media outlets to report on IT security practices, and a cybersecurity protection page was created on Instagram, which gained 207 followers. Furthermore, the campaign joined other initiatives, resulting in an event that was well-received with more than 60 attendees.

The work concludes that the use of a communication campaign serves as a valuable tool for cybersecurity, where the proper transmission of internal messages helps build habits aligned with the company's digital integrity. Therefore, the talks must be informative, dynamic, and relevant to avoid boring employees and to effectively convey the message of caution and vigilance in digital environments. This topic, due to its utility, transcends and is useful for all types of audiences; hence, every communication strategy and its adaptation to each medium is crucial to reach as many users as possible.

Keywords: communication, cybersecurity, hacking, crisis, information, messages, organization.

TABLA DE CONTENIDO

INTRODUCCIÓN

La ciberseguridad es una interdisciplina multidimensional que engloba un conjunto de técnicas, métodos y procesos tecnológicos con el objetivo de proteger a sistemas, ordenadores, redes de telecomunicaciones, datos importantes, accesos no autorizados y ataques informáticos. Se busca asegurar la disponibilidad, confidencialidad e integridad de los sistemas (Jove et al., 2023). Dado el acelerado ritmo en el que progresan las tecnologías de la información en una sociedad digitalizada y conectada, las amenazas contra los usuarios son cada vez más latentes y frecuentes, por lo que los ciberataques afectan aún más a nuestra sociedad y pueden generar pérdidas desastrosas en todos los sectores. Ahora bien, la Comunicación es otra ciencia cuya importancia hace que sea visible y vital en todas las áreas de conocimiento desarrolladas por la humanidad, su incidencia en la ciberseguridad no es la excepción. Así, una de las maneras para perpetrar un ataque informático es a través de técnicas que involucran a la misma Comunicación, lo que también se le conoce como Ingeniería Social. Este último término se refiere a los métodos de engaños y suplantaciones empleadas para estafar a los usuarios y conseguir acceso a contraseñas, datos, información confidencial, la identificación de elementos vulnerables de la seguridad informática de un sistema y, de esta manera, utilizar lo obtenido en contra del vulnerado de forma directa o indirecta (Ibarra, 2018). Entonces, mi tema para tesis es el uso de la comunicación como una herramienta para prevenir y lidiar con ataques de seguridad informática; el siguiente texto busca justificar dicha cuestión a través de la explicación de su pertinencia, relevancia, aporte teórico e implicaciones de sostenibilidad.

En primer lugar, el tema tiene una gran relevancia y se relaciona con unos de los principales retos y peligros de nuestro mundo digitalizado. Como se mencionó antes, el avance tecnológico que ha ocurrido durante el siglo XXI es exponencial y debido a este adelanto, los

dispositivos computarizados y espacios virtuales son cada vez más imprescindibles para nuestro desarrollo diario. Por esta razón, hoy en día los ataques cibernéticos son cada vez más recurrentes y se han convertido en una de las principales amenazas a las que nos enfrentamos como usuarios. Además, las empresas son un blanco notorio y buscado por los ciberdelincuentes que emplean diferentes métodos para vulnerarlas. Por lo tanto, América Latina se ha convertido en un objetivo atractivo para los piratas informáticos y durante el 2022 se registraron 360.000 millones de intentos de hackeo, el ransomware (secuestrar los datos de los usuarios y pedir una paga para que estos sean recuperados) se posicionó como la amenaza más frecuente. Según expertos, en la región no existe una educación y conciencia adecuada por parte de los usuarios en cuanto a la prevención de estos problemas, lo que facilita el trabajo del hacker al momento de realizar sus intrusiones (Castro, 2023). Además, de acuerdo con un informe de ciberseguridad de IBM, el costo promedio de una filtración de datos en Latinoamérica llega a cifras de USD 2,6 millones, lo que nos indica que un ataque informático supone pérdidas millonarias extremas para las organizaciones. El usuario es el eslabón más débil en un sistema informático y la Ingeniería Social conoce y se aprovecha ampliamente de este principio para perpetrar ataques. Al usar la propia comunicación estratégica para manipular a las personas en función de que lleven a cabo una determinada acción, el hacker se aprovecha de la falta de conocimiento de los usuarios y logra conseguir su cometido gracias a su buen y mal intencionado manejo de la transmisión de información. De acuerdo con un Informe de Investigación de Violaciones de Datos de Verizon (DBIR) de 2021, el 85% de las violaciones de datos requieren un ser humano para iniciarse; y adicionalmente, el 70% de las organizaciones en Latinoamérica permiten que sus empleados trabajen desde dispositivos personales lo que facilita que se produzcan hackeos a los empleados por la Ingeniería Social y que estas infecciones se expandan a todos los espacios de la empresa (Gutiérrez, 2022). Entonces, el tema tiene que ver con el uso de la propia comunicación para fortalecer a este

punto frágil en el sistema y cobra aún más relevancia cuando Ecuador es el tercer país de América Latina que sufre más intentos de ciberataques según cifras de Kaspersky en el 2023. Es cada vez más recurrente escuchar que una empresa ecuatoriana sufrió un grave hackeo que, o bien la paralizó y generó significativas pérdidas, o directamente produjo su quiebre y cierre definitivo. Por ende, la importancia de mi tema está relacionada con la generación positiva de un impacto social y laboral a través de la comunicación para prevenir ataques de Ingeniería Social.

Por otra parte, se busca demostrar cómo la incidencia de la comunicación es fundamental al momento de cometer un hackeo. Como se mencionó antes, gracias al posicionamiento de mensajes estratégicos cuyo foco es la persuasión, los piratas informáticos han logrado que las personas expongan sus datos, propaguen infecciones de malware y otorguen acceso a sistemas restringidos. Entonces, por qué no utilizar la propia comunicación para informar a los usuarios y educar a las empresas con herramientas para afrontar estas amenazas. A través de una campaña estratégica, se puede levantar conciencia a las personas para prevenir que se sigan ejecutando los diversos tipos de ataques informáticos que necesitan de un click de un usuario desinformado e ingenuo. A pesar de que se han publicado y explorado muchísimas estrategias para enfrentarse a los hackers, el combate contra la ciberdelincuencia ha tenido un enfoque más ubicado en aspectos plenamente informáticos (acciones relacionadas con la actualización de software, corrección de vulnerabilidades, fortalecimiento de barreras de ciberseguridad, etc.); pero este tema no ha sido tratado bajo una perspectiva comunicacional y esto es lo que le convierte en algo novedoso. Se ha conceptualizado a las técnicas de Ingeniería Social en libros, investigaciones y papers, pero siempre se lo analiza de acuerdo con los conocimientos de las áreas de las ciencias de la computación. En el libro llamado “Ingeniería Social, El Arte Del Hacking Personal” escrito por Christopher Hadnagy, se explora

un poco más la importancia de la comunicación para prevenir los ataques informáticos, pero también se involucran elementos más técnicos que pueden ser poco comprensibles por algunas audiencias. Entonces, existe la oportunidad de crear campañas que capaciten a los usuarios y los mensajes transmitidos sean más claros y enfocados a un público con un menor grado de conocimientos en informática. Asimismo, se puede encontrar una declaración reciente con un manual que incluye estrategias de ciberseguridad del Ministerio de Telecomunicaciones; sin embargo, el tema de la concientización puede aún ser complementado a través de los conocimientos en comunicación estratégica para beneficiar y proteger a organizaciones públicas y privadas. Así, es pertinente explorar a la prevención y confrontación de ataques informáticos desde el punto de vista de la comunicación. Todavía existe la necesidad de desarrollar campañas de comunicación interna y externa relacionadas con la seguridad cibernética. Se estaría generando una instrucción, a través de herramientas comunicacionales, para usuarios, incluyendo a trabajadores de empresas. Adicionalmente, para las organizaciones, la comunicación en crisis jugará un papel fundamental para hacerle frente a una amenaza informática inesperada porque esta permite delinear estrategias con acciones tácticas para interactuar correctamente con los diferentes stakeholders y coordinar esfuerzos defensivos durante dicha situación. De esta manera, se aportaría a la teoría de la comunicación social, en crisis y organizacional en materias de seguridad cibernética con un mejor entendimiento de esta interdisciplina.

Por último, el tema se alinea con el objetivo desarrollo sostenible número nueve que equivale a industria, innovación e infraestructura. En este caso, lo que se investigará tiene relación con la construcción de infraestructuras informáticas resilientes y con el fortalecimiento de la ciberseguridad de las empresas. Existe incidencia con la industria de la tecnología y con su desarrollo, donde cada día el software y el hardware crecen más con nuevos elementos, al

mismo tiempo de que las amenazas se incrementan. Por lo tanto, este trabajó tendrá que ver con cómo innovar a la comunicación en las industrias para prevenir y lidiar con la inseguridad informática. Partiendo desde lo antes mencionado, las industrias, empresas y organizaciones son un blanco cada vez más visible para los hackers. Por ende, este trabajo tiene como propósito aportar con el desarrollo de la seguridad en las entidades donde múltiples colaboradores trabajan con un determinado fin, ya sea de lucrar o no. El objetivo es repercutir positivamente en la industria de la tecnología, cuya relevancia afecta directamente a la sociedad. Por consiguiente, se aplicará a la comunicación para desarrollar un sector industrial de software y hardware más seguro y con prácticas tan conscientes como éticas.

Como conclusión, la comunicación demuestra su importancia y versatilidad cada vez más y cada día que pasa en cada ámbito de la humanidad. En este caso, se la puede utilizar con fines negativos, para perjudicar y robar, pero también tiene el poder de contrarrestar dichas malas intenciones y crear una sociedad más segura e informada. Con esto dicho, podemos ver el poder de la comunicación y su inminencia para construir, por ende, los buenos debemos ser más y tenemos que utilizar cada herramienta a nuestro favor para transformar al mundo en uno mejor donde la tecnología sea un medio de desarrollo y no de malicia. Así, mi tema es relevante, novedoso, pertinente y trae consigo nuevos aportes teóricos que apoyarán a los comunicadores, trabajadores, gerentes y a los propios usuarios.

CAPÍTULO 1:

1.1 ¿Qué es un ataque cibernético?

Emprendido por uno o varios delincuentes informáticos, un ataque cibernético consiste en una vulneración a un determinado equipo tecnológico donde se saca provecho y se utiliza una debilidad o error en el software, hardware o en los individuos que pertenecen al entorno informático. Debido a esto, se puede conseguir beneficios de manera ilegal mientras que se impacta negativamente a la seguridad de un sistema (Moya et al., 2022). Dado que con el paso del tiempo, en la actualidad la mayoría de las actividades de índole comercial, social, cultural, económica y gubernamental se producen en el ciberespacio; las empresas a nivel global deben enfrentarse a amenazas cibernéticas y los problemas que suponen las vulneraciones informáticas que sitúan directamente en jaque a la integridad de las actividades de las organizaciones. Los avances en la computación también han supuesto el origen de nuevos vectores de ataque acompañadas de más modalidades cuyo peligro supone una transformación de las tecnologías de la información e Internet en medios donde existe el riesgo tanto para personas como para grupos (Mieres, 2009).

Los motivos de los ciberpiratas pueden variar, pero normalmente sus fines son económicos. También se asaltan a los sistemas por fines políticos, sociales, estatales, éticos y en múltiples ocasiones, los atacantes simplemente buscan obtener información sensible para determinados fines personales. Ahora, las causas técnicas para que se produzcan los atentados cibernéticos son varias y parten del principio de sacarle partido a una equivocación o lo que se denomina como “explotación”. Estas fallas pueden ser el resultado de códigos de programación que no están correctamente construidos y producen problemas, lo que también se conoce como bugs. Las limitaciones tecnológicas de software o hardware del sistema también suponen un problema porque producen saturación de datos u otro tipo de eventualidades. Otro tipo de

deficiencias gravísimas y extremadamente comunes son los errores humanos causados por la falta de educación informática y desconocimiento de los usuarios. Por esta razón, es importante tipificar y clasificar a los ataques informáticos más comunes según su función y acción.

Para empezar, las vulneraciones computacionales suceden en los espacios virtuales de los propios usuarios, empresas y organizaciones. Pueden ser proliferados y esparcidos a través de Internet porque este entorno es global y conectado, entonces, se convierte en el medio principal para muchos ciberdelincuentes. Las infraestructuras de redes corporativas y sistemas financieros en contextos electrónicos también son blancos extremadamente recurrentes porque tienen datos e información valiosa y confidencial. Los bancos y plataformas que funcionan para el pago en línea también son objetivos que recurren a varios métodos para conseguir saberes financieros para ejecutar fraudes. Los Gobiernos e Instituciones Estatales son otro tipo de conjuntos muy afectados por los piratas dada la relevancia de la seguridad nacional y por el alto número de datos sensibles que estos mantienen. Por último y no menos importante, todos y cada uno de los usuarios de las plataformas del ciberespacio también se encuentran en riesgo de ataques; ya sean personalizados y específicos, o pensados para afectar a múltiples individuos, las personas están en el punto de mira de los hackers y la incidencia de vulneraciones informáticas es cada vez mayor.

1.2 Tipos de ataques cibernéticos más frecuentes:

Ahora, se enumeran las categorías de ataques cibernéticos más frecuentes que atentan contra los usuarios, las entidades comerciales y compañías. En primer lugar, tenemos al malware, que es una manera general de nombrar a múltiples versiones malignas de un código de programa. Corresponde a un software cuyo fin es afectar procesos o datos para conseguir accesos no autorizados en un sistema o red. Este término se emplea de manera general y comprende a cualquier tipo de programa computacional que ejerza un impacto no deseable y

malicioso. Luego tenemos al Virus que tiene que se puede encontrar en páginas en línea como portales de apuestas, videojuegos en la web, sitios de compras, ventas, pornografía, blogs, motores de búsqueda, redes sociales, etc. La característica de esta clase de software malintencionado es que lo podemos hallar en sitios en los cuales el tráfico es elevado porque existe una alta frecuencia de visitas, los internautas navegan muy comúnmente estas webs con distintas necesidades. Cada virus informático está específicamente construido para proliferarse sin control y provocar daños graves a los datos. Por lo que se les puede comparar con plagas virtuales como si de patógenos se tratasen, se transmiten desde un huésped contra otro. Los troyanos son otra clase de malware muy común y que ha protagonizado innumerables complicaciones tecnológicas graves. Corresponde a un software malicioso que finge tratarse de procesos legítimos con el objetivo de lograr una entrada no autorizada en la computadora o dispositivo móvil de la víctima. De esta forma, el atacante procede con diferentes acciones maliciosas como apoderarse y controlar el equipo alterado, robar información, descargar materiales maliciosos adicionales, entre otras. Pueden aparentar ser archivos comprimidos, audios, actualizaciones, apps para el celular, instaladores de software, etc. Ahora, el spyware es otra clase de código informático perjudicial que también corresponde a una de las funciones del Troyano una vez que la vulneración informática es exitosa. Es instalado de manera totalmente oculta en el ordenador de la víctima y con esta estrategia de hacking, se controla a escondidas la actividad del usuario. Su función es recoger información y datos sobre la persona en cuestión o la empresa en donde trabaja sin el conocimiento, y mucho menos el consentimiento, para posteriormente enviar dichos detalles a un tercero. Es uno de los riesgos informáticos más comunes que están presentes en la red que atenta contra las empresas y los cibernautas de manera constante. Este tipo de malware recopila y difunde información sensible a analistas de datos, anunciantes o usuarios con algún interés particular. Además de penetrar sin autorización el contenido de cámaras y micrófonos, mediante este programa dañino, los

espías pueden acceder a diferentes códigos de seguridad, contraseñas, credenciales de tarjetas de créditos, etc. Uno de los peligros más comunes para las organizaciones hoy en día es el ransomware, es otro modelo software nocivo que tiene como meta el secuestrar los datos de un usuario u organización a través del cifrado de la información (transformar el contenido legible por claves de criptográficas) y así demandar un pago como condición que permitirá que el damnificado vuelva a tener acceso a su sistema. De la misma manera, se emplea el ransomware para robar los datos muy delicados de las organizaciones y se pide una compensación económica muy considerable para que la información no se haga pública para la comunidad, autoridades o competencia. Por lo tanto, la dirección de estos métodos de pirateo informático se enfoca en impactar a las corporaciones para entorpecer o frenar sus operaciones; esto instaura un dilema para los gerentes que se debaten en realizar la paga respectiva y tener fé en que los hackers cumplan su parte, o por otro lado no desembolsar y hacer el intento de emprender formas para restablecer las operaciones empresariales (Guaña et al., 2019). Cuando sucede una crisis por ransomware, normalmente las empresas no tienen un largo tiempo para mitigar, remediar o evitar el ataque y restablecer el sistema, tampoco poseen estrategias que gestionen las relaciones públicas si se da el caso de que se produzca una filtración de datos masiva. Otro malware sumamente recurrente y uno de los más reconocidos es el phishing, una técnica que busca, con fines maliciosos, conseguir detalles potencialmente muy significativos de la víctima. Se trata de obtener nombres de usuarios, contraseñas, información de las tarjetas de crédito, elementos privados, datos médicos, etc. Es transmitido a través de comunicaciones de correos electrónicos y mensajes con tonos engañosos y persuasivos. Las formas de perpetración a los sistemas que se acaban de tratar son métodos estandarizados, muy útiles y comprobados que los hackers emplean para vulnerar un sistema. Las habilidades de los ciberdelincuentes son muy bastas y técnicas, pero una de las aptitudes más fundamentales que poseen estas personas es la capacidad de provocar, identificar y tomar partido de los errores de

sus víctimas para lograr su cometido. Como se mencionó antes, los puntos sensibles de las infraestructuras informáticas son varias, pero el eslabón más débil de estos sistemas puede ser el propio usuario (Moya et al., 2022).

1.3 La vulnerabilidad más grande de un sistema:

El phishing y todos los tipos de ataques informáticos que se explicaron anteriormente necesitan de una vulnerabilidad fundamental para que estos tengan éxito y puedan ser iniciados, el error humano. Los piratas informáticos engañan y persuaden negativamente a los usuarios a través de múltiples estrategias donde se explota el miedo y desconocimiento para conseguir que el individuo cometa una falla comprometedora que otorgue ventajas claves al hacker. Para que la víctima sea afectada por un malware, el éxito de este código maligno radica en la simulación, es decir, se crea el impulso para el usuario para que ejecute el archivo y permita la ejecución de las funciones del programa malicioso sin darse cuenta (Muñoz, 2021). Sin siquiera saberlo, el afectado da el primer paso clave a que se vulnere su propio sistema al caer en el requerimiento de abrir dicho software malintencionado, abre una puerta trasera en su sistema para la entrada de virus, troyanos, spywares, ransomware y muchas otras averías en los sistemas. En el phishing, las intenciones son provocar que las víctimas realicen clic o inicien sesión en sitios web que en realidad son clonados. Por ejemplo, se copian páginas de inicio de sesión de los sistemas propios de las empresas, de sitios bancarios, redes sociales y espacios de correos electrónicos (Facebook, X, Instagram, Gmail, Outlook, etc.). Cuando los usuarios entran a la URL enviada por el hacker, el portal en línea original es redireccionado a un dominio falso controlado por el pirata. Entonces, si la víctima intenta iniciar sesión o transmitir algún tipo de información en estas direcciones web, el perjudicado otorga información sensible y secreta como contraseñas, detalles de la tarjeta de crédito, identificaciones del usuario, direcciones, correos electrónicos, teléfonos celulares, fechas de nacimiento, etc. Con el paso

del tiempo, estas metodologías que usan los ciberdelincuentes han progresado constantemente, su mejoría está relacionada con la personalización, las vulneraciones informáticas son hechas a la medida según el tipo de víctima y las motivaciones del ciberpirata. En las empresas, los objetivos pueden ser personas de alto nivel o quienes tienen un valor alto, por ejemplo, ejecutivos, jefes de recursos humanos, miembros de la junta directiva, etc. Por ende, los piratas emplean maneras más avanzadas de ataques de phishing contra estos públicos, a esto se le conoce como whaling, que implica vulnerar computacionalmente a líderes jerárquicos o de elevado perfil en una organización a través del engaño informático. También, el spear-phishing apunta a personas específicas en las compañías y son aún más personalizados, pueden ser miembros del equipo de TI (Tecnologías de la Información), finanzas, producción, gestión, nuevos empleados, entre otros (Guaña et al., 2019). Otros tipos de phishing tienen que ver con la creación de códigos QR que son fraudes, si estos son escaneados con teléfonos, el hacker podrá explotar vulnerabilidades propias del teléfono e introducir código maligno en el mismo para acceder y dominarlo. El pop-up es otra forma de ejecutar el phishing sorpresivamente, se lo lleva a cabo a través del empleo de ventanas emergentes o cuadros de diálogo que pueden ser creíbles o engañosos, se persuade a los usuarios a que introduzcan sus credenciales y datos personales de manera repentina y sobresaliente. Por último, el vishing es otro método relacionado con la realización de una llamada telefónica en la cual se falsifica la identidad de una persona, empresa o trabajador con el fin de conseguir información personal o entrada a algún dispositivo (Álvarez, 2022).

Según estadísticas del 2022, El Informe sobre Delitos en Internet del FBI reportó que se denunciaron un total de 800.994 de crímenes informáticos, siendo los ataques de phishing la modalidad más frecuente con 300.497 de denuncias notificadas. Estos generarían un aproximado de 10.300 millones de dólares en pérdidas para las empresas (Guaña et al., 2019).

Entonces, de acuerdo con estas cifras, el 90% de las intrusiones en contra de datos son debido a los ataques de phishing. Esto quiere decir que los atacantes asumen una identidad creíble al momento de emitir un mensaje y los usuarios están cada vez más desprevenidos, lo que hace que caigan en diferentes tipos de engaños. Ahora, en el auge de la inteligencia artificial, los hackers pueden recurrir a algoritmos de educación automática para realizar un análisis de grandes masas de datos, lo que les permite crear mensajes aún más personalizados y convincentes. Pueden ser comunicados falsos de instituciones de confianza como bancos, marcas, empresas grandes, entidades sin fines de lucro, etc. Los ciberdelincuentes pueden producir contenidos relevantes para el contexto y mensajes persuasivos para explotar vulnerabilidades más específicas o aprovecharse de situaciones coyunturales. Por ende, los usuarios y las corporaciones necesitan prestar más atención y esfuerzos a su seguridad informática (Álvarez, 2023).

1.4 Ingeniería Social:

Pero el phishing y todas sus estrategias de vulneración similares parten de un concepto básico fundamental e indispensable para su éxito y funcionamiento, un principio denominado como Ingeniería Social. Este último término se define como el conjunto y ejecución de técnicas empleadas por los piratas informáticos para engañar al usuario a través de la comunicación persuasiva y así que este individuo con permisos de sistemas informáticos de un sistema revele información sensible y conceda acceso al ciberdelincuente. Comprende el conjunto de usos del lenguaje oral, escrito y visual para estafar a las personas y explotar el hueco de seguridad más frágil en la informática, que como se mencionó antes, es el propio usuario. Dependiendo del hacker, se pueden aplicar distintas herramientas tecnológicas e incluso, encuentros cara a cara donde el pirata consigue la información necesaria. Según López y Salvador (2015), se debe reconocer que “no solamente el usuario de los sistemas está expuesto a sufrir un ataque de

Ingeniería Social; el mismo personal de seguridad informática está expuesto e igual de vulnerable" (p. 39). Si lo pensamos bien, la Ingeniería Social se aplica en situaciones normales; cuando una adolescente convence a sus padres de que le dejen salir en la noche; el momento en que un empleado persuade a sus superiores de conseguir un aumento de salario; cuando un vendedor quiere concretar la venta de su producto estrella para un cliente interesado. Cuando se recurre al lenguaje persuasivo y la comunicación con una planificación por detrás con un fin determinado, puede ser una manera de emplear la Ingeniería Social. Así, tiene usos gubernamentales o dentro del mundo del Marketing, por lo que es una acción bastante común que lamentablemente los estafadores y delincuentes combinan con la informática para vulnerar sistemas computacionales (Hadnagy, 2011). El atacante, antes de ejecutar su plan de Ingeniería Social, primero realiza un diagnóstico y recolección de la información básica y visible de sus víctimas para perfilarlas y simplificar la planificación de su estrategia de engaño persuasivo, además de que determina qué posible método de hacking usar.

Es importante definir las formas de Ingeniería Social adicionales al phishing, como el baiting, una técnica que maneja la psique humana; ocurre cuando un pirata informático configura un dispositivo que contenga un malware, como una memoria USB, y persuade al atacado para que conecte dicho aparato en su computadora y revise su contenido, en ese momento se estaría inyectando el código maligno en el sistema. El pretexting es otro elaborado procedimiento donde el pirata crea un buen escenario o pretexto para robar los datos de sensibilidad del afectado, apunta a ganarse la confianza de la víctima (contrario del phishing que normalmente desea inducir miedo) para lograr el éxito. Cuando el hacker crea una buena relación personal con el atacado según la información que el pirata investigó antes, se le conoce como farming, se aplica lenguaje positivo mientras que se socializa con el blanco para que este no se espere el hackeo. El quid pro quo es otro método basado en que el atacante finge

beneficiar o ayudar al usuario a cambio de datos confidenciales determinados, por ejemplo, el ciberdelincuente se hace pasar por alguien del equipo de soporte técnico y brinda un apoyo falso a la víctima mientras que le pide que revele información clave como contraseñas, números de cuentas bancarias, etc. Pueden existir aún más enfoques de la Ingeniería Social dado a que depende mucho de cómo el hacker emplee el lenguaje y qué tan hábil sea este al momento de emplear la comunicación.

1.5 Problema en Ecuador y América Latina:

Entonces, en función de que los diferentes tipos de malware, troyanos, virus, ransomware y otros tipos de código maligno tengan éxito, es necesario el uso inteligente de la Ingeniería Social. Por consecuencia, en la mayoría de los casos se puede afirmar que los programas malintencionados mencionados anteriormente dependen de que el usuario caiga en estas trampas. El 85% de violaciones a datos necesitan de un ser humano para iniciarse según un informe de Investigación de Violaciones de Datos de Verizon (DBIR). Además, el 70% de las organizaciones en Latinoamérica autorizan que sus empleados laboren desde sus dispositivos personales; esto facilita que se den más hackeos, donde la base es la Ingeniería Social, en contra de empleados con el fin de llegar a afectar a toda una empresa (Gutierrez, 2022).

América Latina se ha transformado en un blanco llamativo para los hackers. Durante el 2022, se notificaron 360.000 millones de atentados informáticos solo en este continente, el ransomware fue el ataque con mayor incidencia cuya cantidad fue de 60%. De acuerdo con expertos, el retorno progresivo a la normalidad luego de la pandemia ha sido la causa principal de nuevos mensajes fraudulentos de Ingeniería Social. Esto, sumado con la adición de la Inteligencia Artificial para creación de contenidos para automatizar estafas, ha incrementado la frecuencia de ataques informáticos de phishing para el 2023 (Kaspersky, 2023). Los delitos

informáticos continúan con más persistencia y una alarmante progresión, las amenazas a los dispositivos móviles están en aumento. Además, los países latinos con más ciberataques son Brasil, México y Ecuador, seguidos de Colombia, Argentina, Perú y Chile (Cañizares, 2023). En Ecuador, durante el año pasado se registraron aproximadamente 12 millones de ataques cibernéticos en el país, una cifra menor a la del 2022, pero que denota que aún debemos trabajar en la creación de una cultura de ciberseguridad más fuerte porque los piratas vulneran sistemas de maneras cada vez más sofisticadas.

Entonces, es importante mencionar delitos informáticos previos ocurridos en nuestro país en función de enfatizar la importancia de la seguridad computacional en las organizaciones y en el día a día de los usuarios. Durante el 16 de abril del 2022, la plataforma de trámites digitales del Municipio de Quito fue anulada temporalmente debido a un ataque informático que afectó entre el 15% al 20% del servicio momentáneamente. Se vulnero el sistema y se secuestraron los datos a través de un ransomware cuyo propósito era ingresar a los datos municipales. Fue un ataque estratégico dirigido a información estratégica de la institución que dejó paralizada la actividad de múltiples trámites y funcionarios debido a la encriptación de sistemas y componentes relevantes (Swissinfo, 2022). A finales del propio 2022, la Universidad San Francisco de Quito fue víctima de una vulneración en sus sistemas informáticos, lo que les produjo que el establecimiento frene y tenga que postergar múltiples actividades importantes como el inicio de clases para el 2023. Nuevamente, el tipo de malware que afectó a la USFQ fue un ransomware, un colaborador interno de Tecnologías de la Información pudo haber sido engañado y caído en un phishing que infectó al resto del sistema. A pesar de que la universidad cuenta con algunas sofisticadas medidas de ciberseguridad en cuanto a software y hardware, fue el usuario que inocentemente abrió la puerta y concedió acceso a los hackers. Sin embargo, el equipo de TI pudo restaurar el orden y rescatar los datos,

pero se frenó la cotidianidad de múltiples colaboradores en momentos claves de la operación de la organización (Samson y Bayas, 2023). El Banco del Pichincha corresponde a otra entidad ecuatoriana que ha sido golpeada por la ciberdelincuencia. El 18 de febrero del 2021, la empresa bancaria comunicó que existió un acceso no autorizado en los sistemas de un proveedor que brindaba los servicios de mercadeo respecto al programa Pichincha Miles. En este primer incidente, los piratas emitían correos electrónicos fraudulentos y comunicaciones en nombre del Banco de Pichincha a los clientes de este programa, con el objeto de conseguir la información requerida para efectuar transacciones no legítimas (El Comercio, 2021). Meses después, el 11 de octubre de ese mismo año, el Banco notificó que su servicio en canales electrónicos cayó por 72 horas y afirmó que se debía a incidentes de ciberseguridad. La institución afirmó que la intrusión de meses pasados persistía y posteriormente se señalaron a los intrusos, Hotarus Corp. Se dice que este conjunto comprometió la información personal de miles de consumidores del Grupo Diners y del propio banco. En un principio, el grupo pedía un pago millonario para que se rescaten los datos, pero este pago nunca se dio y los hackers filtraron las bases de datos en foros de internet, mientras tanto, el Banco afirmaba que no existía esta filtración (Díaz, 2021). En el 2021, la Corporación Nacional de Telecomunicaciones (CNT) pasó por una crisis muy aguda relacionada con un duro ataque informático. La empresa pública fue afectada a través de un ransomware y un virus que alteró las recargas, facturación, activaciones y más funciones clave. Se vulneraron elementos como la red, el sitio, sistemas informáticos internos y las bases de datos. Pese a que no exista mucha información oficial respecto a cómo se logró la intrusión a CNT, muchos presumen que se debe a que un funcionario mordió el anzuelo de un phishing con Ingeniería Social y esto provocó la infección y crisis del sistema; otros no descartan que también se trató de la explotación de fallas en los códigos de programación de los sistemas. El atentado golpeó a múltiples servicios de CNT, como a los centros integrados de atención al cliente, se dieron malestares de los usuarios al

momento de hacer reclamos, pagos o acceder a las prestaciones por las cuales pagaban (Dávalos, 2021). A inicios del 2021, las plataformas computacionales de la Armada Ecuatoriana, es decir, el Sistema de Gestión Marítima o Sigmar, sufrió una intrusión por delincuentes informáticos. Sigmar engloba una numerosa base de datos relacionada con embarcaciones y trabajadores que recorren los mares territoriales. Esta incluye nombres de armadores, pescadores y patrones costaneros, también posee matrículas de aquellas embarcaciones y su característico geoportal informático que permite realizar una gestión marítima visualizable en tiempo real. A pesar de que no se secuestraron los datos, el geoportal poseía información clave que podría comprometer la seguridad marítima del Estado, por lo que el peligro en esta situación fue extremadamente grave. Así, podemos ver las múltiples consecuencias existentes en el caso de que se produzca un ciberdelito. Se pueden producir crisis empresariales de alta magnitud de índole bancaria, municipal, monetaria, seguridad nacional, etc. Por ende, es importante saber cómo manejarlas y prevenirlas para evitar repercusiones mayores en las que se paralicen actividades y se pierdan millones.

CAPÍTULO 2:

2.1 Definición de Seguridad Informática:

Ahora, es pertinente mencionar algunas de las maneras de cómo se contrarrestan los ataques que vulneran los sistemas virtuales, qué acciones y mecanismos existen para dar una oportunidad de defensa al usuario ante la creciente amenaza de los delitos cibernéticos. La seguridad informática es un grupo de estrategias, acciones, prácticas, técnicas y herramientas diseñadas especialmente para defender la confidencialidad, disponibilidad e integridad de los datos junto a la información guardada por los diferentes sistemas informáticos (Arango, 2023). Es el acto de proteger a las personas y organizaciones de ciber-atentados con procesos y buenas prácticas que identifican y obran defensivamente en contra de las amenazas o accesos no

autorizados. Según el experto en seguridad informática, Axel Orihuela (2022), cuando se habla de una estrategia de resguardo informático “no solo se debe considerar las herramientas tecnológicas, sino que hay que involucrar al ser humano en la prevención y detección de amenazas de ciberataques” (p. 15). En las empresas, se pretende proteger a los activos de la información digital de la corporación, a la par que se vela por la infraestructura computacional. Así, la protección de espacios digitales toma en cuenta las normativas de salvaguarda que se deben tomar en cuenta con el fin de evitar el sufrimiento y compromiso que una vulneración cibernética supone.

2.2 Pilares fundamentales:

La seguridad informática está compuesta por cuatro pilares fundamentales; el primero se refiere a la confidencialidad, a su vez esto tiene que ver con la protección de la información para que esta no sea revelada a personas que no poseen autorización, como ejemplo, podemos nombrar a los datos de identificación personal, tarjetas de crédito, credenciales de acceso, etc. Esta información es confidencial y no puede ser divulgada a cualquier persona. Como segundo pilar tenemos a la integridad que se trata de la protección de la información para que esta no sea alterada por las personas cuyo nivel de autorización no les permite esta práctica; por ejemplo, un individuo sin permiso que cambia lo que contiene un archivo informático puede causar daños de la integridad de los sistemas y, posiblemente, provoque una pérdida de datos. El tercer pilar es la disponibilidad, se refiere a la capacidad de los usuarios con aprobación para acceder a la información cuando sea necesario; en función de ilustrar esto, se puede plantear un escenario en el que un sitio web está siendo afectado por un ataque de denegación de servicio (saturación de peticiones o interacciones con el portal en línea que genera una sobrecarga de datos y altera el funcionamiento correcto), los afectados estarán imposibilitados en el acceso a este espacio virtual y los datos no se encontrarán disponibles. La autentificación es el cuarto

pilar que se define por la certeza existente en la información gestionada y se garantiza que la identidad del emisor de un mensaje o programa sea legítima; por ejemplo, si un colaborador interno de una institución envía un ejecutable a un empleado, dicho archivo está libre de código malicioso y existe la seguridad de que su creador no posee malas intenciones. Ahora, para cumplir los objetivos de seguridad informática, debemos tomar en cuenta los planos técnicos en los que se trata la infraestructura de datos, legales (países cuya ley obliga el planteamiento de medidas de ciberseguridad) y los humanos, particularmente empleados y directivos, que deben ser formados en ámbitos de defensa cibernética. Asimismo es necesario tomar en cuenta los esquemas organizativos que tienen que ver con las normas, procesos, buenas prácticas de actuación, planes y políticas de seguridad (Arango, 2023).

2.3 Tipos de seguridad informática:

De acuerdo con las diferentes clases sistemas y sus estructuras, la seguridad informática también puede ser tipificada. Tenemos a la seguridad del hardware, esta tiene que ver con la clase de dispositivos utilizados para escanear un sistema o para controlar el tráfico en la red (actividades en línea que impliquen transmisión de datos entre aparatos conectados en una red). Por ejemplo, pueden ser los firewalls o cortafuegos de hardware, dispositivos físicos diseñados para controlar (también existen códigos de software que actúan como firewalls) y filtrar dicho tráfico, estos están configurados para bloquear el paso de datos según que incumplan normas predefinidas, es decir, un cortafuego acciona al bloquear el traspaso de un virus dañino colgado y circulando en estos ciberespacios. La seguridad en el software tiene que ver con la integridad de las aplicaciones, programas y códigos especificados contra ataques de los hackers, el

objetivo es que cualquier clase de software siga trabajando correcta y eficientemente a pesar de que existan estos riesgos. Entonces, es de crucial importancia que se garantice la seguridad de estos datos a través de su autenticación, verificación y actualización constante. Los desarrolladores de programas informáticos trabajan en esta rama desde hace relativamente poco, los errores en los códigos van desde fallos en la introducción, defectos de diseño, malas respuestas ante errores cuando los usuarios utilizan los programas, etc. La defensa cibernética del software tiene que ver con el aprovechamiento de la ejecución de ingeniería en desarrollo y la aplicación de medidas de corrección y protección constante desde el comienzo de la propia implementación. El tercer tipo de seguridad informática se remite al bienestar de la red cibernética (dispositivos electrónicos interconectados que están en comunicación y se enlazan entre sí gracias a una red digital que los une), es toda acción y práctica que proteja a la red. La eficiencia de delinear un modelo de seguridad de interconexión radica en adoptar medidas contra las amenazas y métodos utilizados por los piratas por los cuales estos últimos se introducen en las tecnologías conectadas (Santos, 2022). Dado el auge de la tendencia de almacenar información en la nube, también se destinan esfuerzos a asegurar lo guardado en este espacio cibernético, lo que incluye la seguridad de esta infraestructura y contenido. Además, la seguridad de la identidad es otro tipo de manera de protección fundamental que tiene que ver con el minucioso cuidado de la identidad digital de los colaboradores y clientes, por lo que se toma en cuenta el control del acceso y las formas de autentificación de los usuarios (Arango, 2023).

2.4 Conciencia de las prácticas de seguridad informática y su necesidad:

Tal como se vio en el capítulo anterior, la necesidad de la seguridad informática para las empresas va en aumento. Ecuador es un territorio cada vez más atractivo para hackers malintencionados y por ello, es de vital importancia incrementar el nivel de conciencia de los

usuarios sobre cómo se ejecutan los hackeos y cuáles son las prácticas de ciberseguridad que lograrían evitar un posible ataque. En el 2022, se realizó una prueba de hacking con ingeniería social en manera de simulación, el fin era evaluar la seguridad informática en el Gad Municipal (prefectura) de la provincia de Santa Elena. A través de ataques controlados, se determinó una representativa vulnerabilidad en los empleados porque estos cayeron en los engaños de phishing; también se evidenció que la entidad debe tomar medidas más serias de seguridad y, por lo tanto, poner un énfasis especial en la mejoría de los esfuerzos en la protección cibernética (Campoverde, 2022). Otro experimento realizado en el 2020, consistió en la vulneración gestionada para aumentar la sensibilidad respecto a los ataques contra usuarios. En este ensayo, se hizo un ataque simulado en el cual se emplearon tácticas de ingeniería social donde un blog falso era empleado para recolectar datos susceptibles como información de sistemas operativos, direcciones IP y credenciales a un grupo de personas en Internet. Lo encontrado por esta investigación fue que solo el 2% de los participantes logró identificar el objetivo real de las técnicas de ingeniería social incluidas en el blog y esto denota el bajo grado de conciencia que existe respecto al uso del phishing, la ingeniería social y las diferentes maneras que previenen o mitigan ataques informáticos (Benavidez et al., 2020).

En efecto, es pertinente realizar una descripción de las múltiples prácticas de ciberseguridad que pueden ser implementadas en las organizaciones con el fin de precautelar la integridad informática de los sistemas. Cada una de las estrategias que se mencionan a continuación deben componerse en un método unificado que constituye el plan de seguridad digital íntegro de una entidad o agrupación. De entrada, se deben utilizar las diferentes herramientas de hardware y software concebidas para la defensa de la integridad de la información y la tecnología, como cortafuegos, software de detección de malware, antivirus, servidores protegidos, etc (Arango, 2023). Estos son instrumentos técnicos cuyo

funcionamiento debe ser gestionado por los expertos en informática dentro de las organizaciones porque se necesita una configuración adecuada y pertinente de cada implemento para asegurar su correcto funcionamiento. Así nos dirigimos al siguiente punto, realizar la actualización del software junto a los sistemas operativos de manera constante, esto es fundamental para prevenir pirateos porque las renovaciones de los códigos incluyen mejoras en la ciberseguridad y parches o correcciones a las vulnerabilidades encontradas, por lo que se le complica el trabajo para el delincuente debido a que se le cerró una ventana de oportunidad de vulneración y sus posibilidades serán más limitadas (Postigo, 2020).

La adopción de contraseñas seguras es otra práctica imprescindible de la ciberseguridad, estos códigos de acceso cifrados son una medida de protección básica implementada para defender a los sistemas informáticos de intrusiones. Sin embargo, las contraseñas pueden ser "adivinadas" por múltiples metodologías de los hackers, una de ellas se le conoce como fuerza bruta, esta técnica implica el probar todas las combinaciones posibles de caracteres para descifrar una contraseña en base a la información que el usuario da a conocer públicamente. Por ejemplo, si un usuario configura una contraseña con su nombre combinado con la fecha de su nacimiento, será muy fácil para el ciberdelincuente poder encontrar cuál es la clave de acceso al sistema de la empresa. Si por el contrario, la persona establece una contraseña segura, donde las letras sean aleatorias mientras que combina guiones medios o bajos, mayúsculas, número aleatorios y otros caracteres, será mucho más complicado el proceso de descifrado para el hacker y puede tomar muchísimo tiempo. Entonces, es fundamental usar este tipo de códigos secretos y cambiar su contenido constantemente para evitar la adivinación por parte de los atacantes, esto constituye en una medida básica, simple y rápida, pero poderosa que puede salvaguardar la confidencialidad de un sistema. Los ciberdelincuentes pueden centrarse en atacar individualmente a las cuentas personales de redes

sociales de los trabajadores, así, componen un ataque informático individual en el que pueden descubrir las credenciales del colaborador a través de sus perfiles privados, infectar el dispositivo de uso laboral con un troyano y progresivamente, acceder a la información sensible de la empresa. Por ende, las contraseñas fuertes es una medida básica pero poderosa que puede ser complementada con más metodologías de defensa.

Para incrementar aún más el refuerzo de las contraseñas, existe la autenticación de dos factores, una forma cibersegura adicional que pide a los usuarios que proporcionen una segunda manera para autenticarse además de la contraseña. Por ejemplo, puede ser un código de seguridad que se envía a un teléfono con el fin de que existan dos pasos importantes, si el hacker logra descifrar la clave de acceso de la víctima, aún hay una barrera más que es complicada de superar y protege la integridad informática del usuario. Otro caso en el que corroboramos la efectividad de esta medida es cuando se utiliza un phishing sofisticado para engañar a un empresario y éste, accidentalmente, concede la información de acceso requerida por el delincuente para entrar a los sistemas de una entidad financiera. Sin embargo, no podrá acceder directamente a lo vulnerado porque la doble autenticación no se lo permite y alerta al afectado que su contraseña ha sido determinada, por consiguiente el vulnerado opera rápidamente para cambiar sus credenciales y reforzar la seguridad.

Manejar cortafuegos es otra acción de defensa digital que, como se dijo antes, bloquea todo tráfico no autorizado y constituye una protección a los sistemas de ataques externos. Corresponde a la barrera de seguridad entre una red privada interna frente a los peligros del mundo exterior. La implementación de firewalls actualizados mitiga riesgos y conserva un entorno de navegación seguro. Al utilizar cortafuegos, cuando los colaboradores internos utilizan internet como herramienta, se reduce el riesgo de entrada de un malware dentro del sistema de su red. Añadiendo a los conceptos anteriores, la medida de cifrar los datos también

es empleada para velar por la confidencialidad de la información que se guarda en los sistemas informáticos. Se trata de transformar los activos digitales, caracteres y cifras en un formato no legible para cualquier persona que no tenga acceso a la clave de encriptación.

Efectuar copias de seguridad de manera regular corresponde a otro protocolo de seguridad informática que debe ser normal y muy incentivado, tanto para los usuarios comunes como para los integrantes de una organización. Hacer copias consiste en respaldar toda la información y proteger los datos en caso de pérdida o daño en el sistema. Por ejemplo, cuando la Universidad San Francisco de Quito sufrió la vulneración informática, la práctica regular de producir copias de seguridad fue el paso fundamental que permitió a la institución la superación de esta crisis por ransomware. Por ende, es fundamental efectuar copias de seguridad con regularidad y almacenarlas en lugares seguros cuya exposición e incidencia a ataques informáticos sea muy baja. Si un ciberdelincuente llega a capturar los datos de una empresa, esta última podrá seguir operando gracias a las copias realizadas previamente y podrá conseguir algo de aire al momento de lidiar con este ataque.

Establecer un conjunto de procedimientos y reglas relacionadas con la seguridad informática es crucial para el éxito de las otras prácticas de protección digital. Es la iniciativa de instaurar políticas claras y específicas que proporcionen un marco de acción y comportamiento para los colaboradores internos de una organización. Se formalizan conjuntos de acciones que definen las maneras en la que la entidad puede protegerse y manipular sus datos interna y externamente. El punto fundamental aquí es velar y asegurarse de que todos los trabajadores internalicen dichas políticas y las ejecuten al pie de la letra con el propósito de precautelar la integridad informática de la compañía. Es importante incluir una combinación de medidas de seguridad que fortalezcan la protección correcta de los sistemas y los datos guardados ahí.

2.5 ISO 27001 y cultura de seguridad informática en las empresas:

Partiendo de lo anteriormente dicho, el Sistema de Gestión de la Seguridad de la Información o SGSI es una manera de nombrar las prácticas ciberseguras. Este último se implementa formalmente basándose en la norma ISO 27001 que, a su vez, es una certificación de un estándar internacional donde se establece como requisito la implementación, mantenimiento y actualización periódica del SGSI. Con un carácter obligatorio, las empresas con esta acreditación deben establecer políticas generales y específicas de la seguridad de la información, controles criptográficos, de acceso, gestión de claves de cifrado, transferencias de datos, información de los dispositivos móviles, proveedores, políticas de escritorio, para teletrabajo, respaldo para la información, desarrollo seguro, reglamentos de protección de datos personales. Además, debe definir controles e instrumentos tecnológicos de protección de información importante y sensible (Hernández, 2019).

Es fundamental complementar las estrategias de ciberprotección con una cultura de seguridad informática. Esta última puede ser definida como un sistema de significados, creencias, prácticas y valores compartidos por todos los miembros de la organización con el fin de focalizar las actividades relacionadas con precautelar la integridad y protección de la información de la empresa (Robbins et al., 2017). La cultura de seguridad informática funciona para que los colaboradores sigan los lineamientos y políticas de defensa de datos, mientras que obren correctamente para orientar a la entidad a un mejor nivel de protección integral. También, las instituciones con esta cultura poseen respuestas más rápidas, eficaces y apropiadas frente a los incidentes que afecten a los activos informáticos porque se involucran políticas, actividades, procesos, estructuras, recursos tecnológicos y humanos para enfrentarse a los ataques de ciberdelincuentes y los empleados tienen un valioso conocimiento que marca una diferencia al momento de lidiar con hackeos. Para crear, introducir, llevar, mantener y actualizar una cultura

de seguridad informática se debe trabajar con los empleados que como se dijo antes, son los principales blancos de las vulneraciones digitales. Cada uno de los colaboradores internos debe ser educado y concientizado sobre las medidas de protección de datos que la organización toma, las amenazas latentes a las que está expuesta y sobre casos de hackeos anteriores. En las normas ISO 27001 se sugiere que la institución debe proporcionar todos los recursos necesarios para la adecuada operación del Sistema de Gestión de Seguridad de la Información. Esto incluye el emprender capacitaciones y recomendaciones constantes sobre un plan de concientización dirigido a todos los funcionarios de la empresa, se tiene que garantizar una adecuada instrucción en ciberseguridad para aumentar las posibilidades de prevención (Organización Internacional de Normalización, 2022). El personal tiene que ejecutar su trabajo con una conciencia de protección de información y mientras que siguen las diferentes normas de defensa digital establecidas por la agrupación.

Así, la comunicación organizacional interna juega un papel clave en el proceso de concientización y para fomentar la integración de la cultura corporativa de la seguridad informática. Primero porque es la herramienta usada para informar a los funcionarios sobre las estrategias de ciberseguridad adoptadas, los tipos de amenazas y las prácticas junto con las políticas adoptadas por la corporación. También tiene que ver con la educación y entrenamiento de los empleados para mejorar su comprensión y sensibilizarlos sobre la forma en que sus acciones y responsabilidad puede asegurar o afectar la integridad de los datos de la empresa. Adicionalmente, los colaboradores aprenden a identificar las amenazas y tienen conocimiento sobre cuáles son los protocolos de acción para reaccionar adecuadamente a dichos peligros. De esta manera, quienes trabajen en el negocio o institución pueden responder ante un intento de ataque phishing porque tienen el entendimiento e información pertinentes para reconocer este tipo de engaño; asimismo, crean contraseñas seguras y fuertes que imposibilitan que los

hackers adivinen los códigos de acceso y entren indeseadamente en un sistema; realizan respaldos con frecuencia y almacenan su trabajo constantemente en caso de que una vulneración informática; saben qué protocolos tomar y cómo actuar en caso de un ataque informático. Entre los tópicos que se pueden difundir en las capacitaciones o talleres que se imparten a los colaboradores como parte esencial de la estrategia de ciberseguridad son: ideación de contraseñas seguras y pasos para defenderlas; detección y evasión de phishing e ingeniería social; prevenir la descarga e instalación de malwares; fundamentos de cómo detectar vulnerabilidades en el software y los sistemas operativos; cómo elaborar copias de seguridad del trabajo; procedimientos de actualización del software; protección de los dispositivos personales como el teléfono; cuidado de la integridad de la nube; cómo seguir e implementar las políticas de seguridad informática en la organización (Arango, 2023).

2.6 Casos de éxito:

La implementación de estrategias de seguridad informática ha traído consecuencias positivas para las organizaciones porque se logran prevenir los ciberdelitos, responder adecuadamente ante estos y mitigar sus efectos. En una empresa privada de telecomunicaciones de Lima, Perú, se realizó una propuesta educativa enfocada en el levantamiento de conciencia en seguridad informática en los colaboradores para que ellos tengan la posibilidad de enfrentar ataques de ingeniería social y no realizar acciones incorrectas. Dentro de este proyecto se incluía un direccionamiento orientado a la cultura de pertenencia para que los empleados cumplan los protocolos de protección digital debido a su sentimiento de defensa a su lugar de trabajo. Se generó un espacio de aprendizaje inmersivo donde los funcionarios debían resolver simulaciones relacionadas a casos de ciberseguridad en base a los conocimientos presentados de la estrategia de aseguramiento de datos. Como parte del programa, se puso en marcha un plan piloto que demostró el funcionamiento de las estrategias de seguridad informática en un

entorno de entrenamiento similar a uno real. Por lo tanto, la iniciativa confirmó que los empleados pueden ser adiestrados para preocuparse por las amenazas existentes al interactuar en internet y sus conocimientos permitirían prevenir vulneraciones a la integridad de los sistemas informáticos (Orihuela, 2022).

KnowBe4, cuya traducción al español es “conoce antes”, es otra iniciativa emprendida por grandes expertos en seguridad informática que busca la capacitación masiva de los empleados de las empresas. Se trata de una plataforma en línea que las organizaciones pueden contratar donde los funcionarios pueden acceder para estar debidamente preparados para enfrentarse a los ataques más frecuentes de piratería e identificar señales de ataque. En este espacio existen planes de educación para los usuarios con bibliotecas con mucho contenido como módulos interactivos, juegos de ciberseguridad, infografías, vídeos, exámenes, etc. Igualmente, con el propósito de determinar el aprendizaje de los beneficiarios del proyecto, se les envía ataques de phishing mensuales de manera automatizada. Este servicio analiza los resultados con informes y gráficos de alto nivel donde se puede evidenciar el aprendizaje de los empleados de la empresa que accede a este proyecto. Así, permite medir el nivel y estado de la cultura de seguridad de la corporación para abordar los puntos débiles y solucionarlos (Fárfan, 2023). Los resultados obtenidos por estudios indican que esta herramienta ha logrado resultados positivos, donde los empleados entrenados han demostrado que esta es una buena manera de transmisión de conocimiento y mejora los comportamientos, actitudes y aumenta la responsabilidad. Por consiguiente, este caso enseña que cada vez existen más complementos para las agrupaciones que funcionan para apoyar a esta creciente necesidad de formación de ciberseguridad (Leite et al., 2023).

En el año 2013, la herramienta que permite programar y gestionar el contenido de redes sociales llamada Buffer sufrió una vulneración informática. Múltiples usuarios reportaron que

vieron cómo sus cuentas vinculadas con esta plataforma publicaban mensajes de spam a través de sus páginas comerciales. Así, la empresa emitió un comunicado a través de X en donde anunció que sufrió un pirateo y que mitigarán lo sucedido lo antes posible. Debido a que esta aplicación posee el acceso a los perfiles de múltiples compañías, esto significaba un problema sumamente grave donde una parte de la información más sensible estaba en juego. Dado a que los colaboradores internos de Buffer poseían una buena noción de principios de seguridad informática, supieron cómo actuar y la importancia de la respuesta inmediata, tanto para mitigar el daño informático como para emitir comunicados apropiados que administren la crisis correctamente y se evite agravar la situación. Primero determinaron que las contraseñas y la información de pago de los usuarios no fue comprometida. Entonces, el equipo de Buffer coordinó una estrategia de ciberseguridad conjunta con un enfoque de minimización de agravios donde brindaban asesorías personalizadas a los usuarios para superar totalmente al ataque de los delincuentes. Enseñaron a los afectados a cómo borrar las publicaciones de spam realizadas por los piratas y también reforzaron las defensas digitales a través del equipo de programación (Gonzáles, 2013).

Estos ejemplos funcionan para entender la importancia de las estrategias y prácticas de seguridad informática, a la par que el establecimiento de una cultura sólida con el fin de lidiar con las vulneraciones y ataques emprendidos por los ciberdelincuentes. Para desarrollar los protocolos de ciberprotección pertinentes, la comunicación es una herramienta fundamental. Entre sus funciones, se puede destacar que permite la creación de dicha cultura organizacional dominante a través de la transmisión de símbolos, normas y utilización para que las campañas estratégicas promuevan las políticas de defensa informática. La comunicación sirve para educar y levantar conciencia en los colaboradores, entonces, estos últimos se acatan a las normas y adoptan prácticas de prevención o acción contra ataques. También, es un medio fundamental

por el cual se puede lidiar con una crisis interna y externa si se produce una situación de hackeo en la empresa ya que se configuran mecanismos de respuesta anticipados o permite una buena adaptabilidad que coordinará una respuesta adecuada. Por consiguiente, las iniciativas de ciberprotección se apoyan ampliamente de teorías de comunicación organizacional y en crisis con el fin de enfrentarse a los retos actuales de la seguridad informática.

CAPÍTULO 3:

3.1 Comunicación Interna e información a los colaboradores:

En cada uno de los escenarios relacionados con seguridad informática, la transmisión y el intercambio de la información entre cada uno de los stakeholders es fundamental. Esto tiene que ver con las maneras de hacer saber a los colaboradores cuál es la misión, visión, valores, filosofía, historia, sistemas y el modelo del negocio de la corporación; pero al mismo tiempo, se debe dar aviso sobre las amenazas que atentan contra la integridad de la empresa y los antecedentes de este tema, en caso de existir. A la par, hay que informar a los colaboradores cómo proteger y combatir una potencial crisis relacionada con pirateos informáticos. Una vez comprendidos los múltiples mecanismos que protegen los sistemas y los datos digitales en una organización, es ampliamente necesaria la transmisión adecuada y estratégica de este conocimiento dentro de la entidad. Así, la comunicación se convierte en un valioso móvil que puede preservar y responder en varias materias, donde la seguridad informática no es la excepción. Dado que la ingeniería social es una técnica de transmisión de información que integra la sugestión psicológica, la apelación a diferentes sentimientos como el miedo, la falta de conocimiento y diferentes maneras de persuasión, es pertinente utilizar a la propia comunicación para revertir estas vulnerabilidades humanas. El acto de comunicar a los empleados puede darles saberes suficientes para no morder el anzuelo de los cibercriminales y

perseverar la integridad informática de la institución, lo que marca una diferencia sustancial. Por ende, la Comunicación Interna juega un papel clave para conformar una metodología de protección donde se parte desde el principio de informar a los funcionarios para prevenir y mitigar ataques.

La Comunicación Interna es contar a la organización lo que la organización está haciendo (Capriotti, 1998). Constituye de una serie de estrategias, medios y formas por las cuales la propia empresa transmite información a todos sus stakeholders internos. Así, a los colaboradores se les insta ser partícipes de lo que se hace en la entidad y esto mejora su sentimiento de pertenencia mientras que adquieren información importante sobre múltiples actividades relacionadas con la empresa. Es importante dar voz y herramientas para los funcionarios con el fin de que estos respondan con feedback, entonces, el flujo de información es bidireccional, ya sea de forma horizontal o ascendente y descendente. También, la correcta interacción facilita para la productividad y el buen ambiente de trabajo. Es clave y fundamental que todos los miembros de la corporación participen en las actividades a raíz de la actividad comunicativa; esto significa que los funcionarios tienen que sentirse involucrados dentro del proceso del intercambio de información donde se consideran a sí mismos como miembros activos y no como simples receptores (Capriotti, 1998).

Entonces, la Comunicación Interna gestiona todo tipo de procesos dentro de la empresa y otorga la forma de la cultura organizacional porque moldea los múltiples modos de relación e interacción. El adecuado y estratégico flujo de la información dentro de la entidad es una herramienta fundamental de la administración porque se trabajan culturas y vínculos que pueden resultar en consecuencias positivas o negativas para la organización (Cuenca & Verazzi, 2020). La eficiencia de la Comunicación Interna se encuentra en la capacidad de ejecutar planes y políticas con metas bien definidas por parte del departamento de

comunicación en conjunto con las otras áreas. Así, se establecen las tácticas, protocolos y principios que conducen a que la organización sea guiada por los mecanismos adecuados (Egas & Yance, 2018). Adicionalmente, algunas variables determinantes para el éxito de la Comunicación Interna tienen que ver con la confianza, los empleados deben creer en los directivos, deben considerarles como interlocutores válidos para intercambiar mensajes relevantes que facilitan el sistema de organización y cumplimiento de tareas. A partir de esta credibilidad con sus superiores, se logrará que los colaboradores internos sean leales y se ajusten a los objetivos en beneficio de la empresa. Los funcionarios tienen que sentir libertad y empoderamiento en la toma de decisiones para solucionar los problemas a los que ellos se enfrente, esto debe estar acompañado con sentimientos de responsabilidad, respeto y conciencia sobre siempre velar por el bienestar de la entidad. Por ende, esto hace que los componentes de la entidad se preocupen más por la protección de la integridad de su empresa y tomarán acciones relacionadas con la defensa de la misma para preservar el bien de su entorno de trabajo.

3.2 En relación con la seguridad informática:

Que los empleados tengan la sensación de que sus opiniones, preocupaciones y feedback son reconocidos también es un elemento decisivo que nos indica la efectividad de la Comunicación Interna. Gracias a esto, los funcionarios pueden avisar sobre cualquier eventualidad o riesgo que hayan identificado, y al mismo tiempo, tiene la posibilidad de ofrecer retroalimentaciones valiosas en base a insights para mejorar los sistemas de protección y acción de la organización (Capriotti, 1998).

Si integramos a los objetivos de Comunicación Interna junto a las acciones de ciberseguridad, podemos establecer que el intercambio de comunicados entre todos los colaboradores internos compone de una herramienta que facilita la existencia de una cultura de

ciberseguridad. Así, se plantea una serie de mensajes estratégicos internos, también conocida como campaña, cuyo primer objetivo es generar un vínculo fluido entre empleados (del mismo departamento o de diferentes subdivisiones) para notificar una determinada amenaza informática o avisar de que un sistema ha sido hackeado a los diferentes departamentos y a los superiores. Por otra parte, se deben definir metas de instrucción y capacitación relacionados con la seguridad informática a través de las constantes acciones de comunicación interna. Por ejemplo, un objetivo relacionado esto puede ser la iniciativa de realizar sesiones de formación cada cierto periodo de tiempo donde se refuercen los mensajes que incentiven las prácticas de protección de datos, esta es una de las acciones de capacitación que la estrategia de Comunicación Interna debe incluir en su planificación integral. En niveles de funcionalidad, los objetivos deben enfocarse en conseguir una operación dinámica y ágil entre todos los colaboradores para accionar de tal forma que se prevenga o reaccione ante un ataque informático. De esta forma, las diferentes áreas se coordinarán entre ellas para preparar actividades consistentes que respondan pertinentemente ante las necesidades de ciberprotección de la entidad. Igualmente, hay que velar por la correcta ejecución de las prácticas informáticas responsables y el respeto a las políticas establecidas respecto a este tema a través de la Comunicación Interna. Esto nos lleva a los propósitos motivacionales, en los cuales se anima, estimula, incentiva y dinamiza la labor de los miembros de la empresa en materia de seguridad informática. La comunicación aquí sirve para involucrar a los funcionarios y hacerles saber sobre su importante papel en la preservación de la integridad digital de la organización, al mismo tiempo que se crea un clima de trabajo en el cual predominan las prácticas diligentes y comprometidas con la defensa informática. Es importante trazar finalidades en las que se logre la aceptación e integración de los empleados a los valores, filosofía, metas y procedimientos de la organización en cuanto a protocolos de ciberseguridad, donde los funcionarios sientan que deben cuidar el bienestar de organización como si se tratara

de un tema personal muy importante. Así, no pasarán por alto los pequeños detalles que pueden marcar la diferencia en el éxito o el fracaso de un hacker intentando vulnerar a la corporación.

3.3 Estrategias de Comunicación Interna enfocadas a la seguridad informática y la prevención:

Luego de que se establezcan las políticas claras de protección de datos y de los sistemas informáticos, la comunicación dentro de la agrupación empresarial se encargará de transmitir adecuadamente cada una de estas medidas para moldear los comportamientos de los empleados y crear este sentido de responsabilidad donde se sigan las normas. Como punto de partida, determinar los objetivos de comunicación y los efectos que se quieren lograr a través de los esfuerzos de la campaña interna proporciona una brújula a las acciones de difusión. Cuando se establecen las metas, se sabe que aquello que queremos conseguir es el levantamiento de conciencia y una correcta educación en materia de seguridad informática con el fin de prevenir atentados contra la integridad digital de la entidad empresarial. Posteriormente, se tiene que delimitar a los receptores de los comunicados a compartir. En el contexto organizacional y dependiendo de la estructura de la compañía, en este caso, tenemos a los altos cargos a quienes se les debe informar de la misma manera que al resto de funcionarios, independientemente de su posición. Es importante decir que el tono y las estrategias de comunicación para emitir el mensaje funciona de la misma manera para cada parte de la corporación. No obstante, siempre será importante realizar adaptaciones a la divulgación según el caso y los contextos que pueden ser especiales en algunas situaciones. Luego de identificar los objetivos, públicos, el tono y el mensaje, como primera estrategia de Comunicación Interna, se puede comenzar con la emisión de una serie de avisos cuidadosamente pensados destinados a la sensibilización, a esto se le denomina campaña como campaña de comunicación interna. Se trata de los movimientos de comunicación estratégica que apuntan a la formación de una cultura corporativa de seguridad informática que es responsable y mantiene prácticas ciberseguras que defienden a la empresa

frente a ataques de hackers. El propósito principal de este tipo de campañas de comunicación interna es el de resaltar la importancia de la ciberprotección y el cumplimiento de las múltiples políticas establecidas para precautelar el resguardo de los datos y sistemas. Así, los colaboradores conocerán las normativas y las penalizaciones en caso de no cumplirlas; además, entenderán las prácticas de la organización para proteger su funcionamiento informático. Se comunicaría a los usuarios de la empresa de sus responsabilidades y tareas frente a la defensa cibernética. Por ejemplo, los empleados deben saber que en caso de que exista un intento de hackeo o un mal funcionamiento de un sistema, se debe reportar al departamento especializado en gestionar la seguridad informática de manera técnica. Para comunicar esto, se pueden colgar infografías relacionadas con estas políticas colocadas en puntos visibles de la infraestructura en las sedes de la empresa, o pegar pequeños papeles en forma de ayudamemoria donde se detallen las políticas de ciberseguridad.

Ahora, se explicarán los componentes de un modelo de una campaña de comunicación interna. Primero se trata de la transmisión del mensaje base que corresponde a la necesidad de enseñar las prácticas ciberseguras a los funcionarios y explicarles en qué consiste cada una. De esta manera, cada uno de los componentes del grupo sabrá cómo actuar en beneficio de la integridad digital de la organización y aumentará las probabilidades de prevenir un ciberataque. Entonces, lo que se deberá compartir a través de los múltiples canales internos de la empresa y los diferentes formatos (dependiendo de la entidad) es cómo las actividades y juicios de los empleados aportan o perjudican a la entidad. En primer lugar, es vital informar los roles y responsabilidades de cada uno de los colaboradores a través de la comunicación, esta última se tiene que fusionar con el plan integral de ciberseguridad desarrollado por los expertos en el área técnica de la defensa digital. Entonces, se debe clarificar y responder las siguientes preguntas a través de la campaña de información interna: quién es el responsable del diseño de

la planificación, quienes lo implementan, cuál es la responsabilidad de cada parte en el plan, cuáles son los objetivos, cuáles son las políticas que se deben seguir, qué prácticas se tienen que respetar, cuáles son los canales de información de este plan. Por consiguiente, el cuerpo del plan de ciberseguridad se relaciona con la comunicación de las rutinas, técnicas y procedimientos de defensa informática (Hueca et al., 2020). En cuanto a la primera práctica, esta corresponde a informar y dar aviso a los usuarios sobre su deber de elaborar contraseñas seguras para proteger sus sistemas. Además, la comunicación aporta con una explicación sobre cómo definir un código de acceso sólido y difícil de descifrar donde el lenguaje no es técnico y es entendible para todas las audiencias. Otra práctica que se tiene que transmitir es el análisis minucioso de un archivo antes de abrirlo o la revisión de la procedencia de un dispositivo USB antes de introducirlo al ordenador. Es pertinente enseñar a los empleados a pensar dos veces antes de realizar algo o dar click en un ejecutable y analizar la procedencia de cualquier software o hardware que tenga que llegue a los sistemas, ya sea en los dispositivos de la empresa o los aparatos personales. Promover que los colaboradores se cuiden en su navegación a través de internet es otra práctica que la comunicación debe hacer énfasis, de esta manera se evita que los usuarios indaguen ingenuamente en páginas que puedan contener material digital dañino. En las políticas, se puede incluir cuáles son las páginas de la web que están restringidas y que los empleados no pueden visitar cuando emplean sus dispositivos de trabajo.

Por otro lado, la siguiente forma de ciberseguridad consiste en incentivar a que los trabajadores empleen los programas de antivirus dispuestos por la organización para verificar el contenido de los códigos en un programa, lo que filtra las aplicaciones malignas. Estos últimos detectan el malware y adoptan correctivos técnicos para eliminarlos, de esta forma, se facilita la protección digital (Arévalo et al., 2020). Manejar los softwares de limpieza de amenazas informáticas es una tarea sencilla de explicar porque las interfaces de estos

programas son amigables con el usuario y sumamente didácticas, la comunicación interna se encarga de transmitir el conocimiento a los funcionarios sobre qué aplastar y cómo hacerlo en caso de que se intente hackear un sistema. Además, se conduce a que los empleados utilicen los antivirus para analizar archivos y detectar peligros de manera oportuna. Cuando cada elemento de la empresa sabe manejar los antivirus correctamente, la seguridad incrementa y a través del efecto incitador de la estrategia de comunicación, las prácticas ciber-responsables proliferan la integridad de los datos. Ahora, para contrarrestar la técnica del hackeo individual a través de la sugestión psicológica, la persuasión y la desinformación, es posible emplear a la propia comunicación como medida de seguridad. Por esta razón, se previene que los funcionarios caigan en las técnicas de ingeniería social cuya función es engañar a los colaboradores y conducirlos a que realicen acciones que abren puertas a los hackers.

Esto nos lleva al uso de la comunicación para la enseñanza relacionada con instruir a cada uno de los colaboradores en conceptos y nociones básicas de seguridad informática; a través de esto, se pueden identificar y diferenciar múltiples clases de ataques por sí solos sin la necesidad de un programa de reconocimiento o un antivirus. Al tener conocimientos de estos principios, los funcionarios no estarán desprevenidos y sabrán cómo reaccionar ante las amenazas. En cuanto a las estrategias de comunicación para la instrucción, se puede anticipar al personal a través de la realización de una muestra con ejemplos de cómo son los ataques de phishing, cuáles son las técnicas de engaño y persuasión más creíbles que se emplean comúnmente. Asimismo, se les indicaría en maneras dinámicas y didácticas cómo se ven los intentos de vulneración por ingeniería social y en qué casos se usan, los mensajes estarán enfocados en la pedagogía. Es pertinente diferenciar que la conciencia y la educación son dos factores diferentes en esta estrategia de comunicación, mientras que la conciencia se refiere a la información teórica que ofrece una noción de las definiciones básicas de seguridad

informática, la educación constituye la acción práctica del empleado al momento de enfrentarse a un riesgo cibernético que podría comprometer la integridad de los sistemas. Así, es importante combinar ambos factores con el objeto de acentuar un conocimiento preventivo, defensivo y proactivo que proteja a la organización (Hueca et al., 2020). Por último, es pertinente adaptar el mensaje base sobre la promoción de las prácticas de seguridad informática en distintas fases. La primera es la expectativa, en la cual se anuncia superficialmente que se emprenderán esfuerzos que solucionen los problemas de ciberdefensa existentes en la organización. En la siguiente etapa se trata de informar constantemente a los colaboradores sobre las prácticas y políticas de seguridad informática, a la par que se les entrena para que adopten estas rutinas a su accionar diario con el fin de prevenir y mitigar un ataque informático. Luego se realizaría un periodo de recordación en el que se acentúan los mensajes transmitidos en las fases previas de la campaña para solidificar la certeza de que los trabajadores internalizaron los comunicados previos.

Ahora, cuando ya se han identificado todos los mensajes a compartir, es importante utilizar los medios de comunicación interna adecuados dentro de la empresa para llegar a las audiencias de manera eficiente. Estas herramientas de transmisión de la información deben ser seleccionadas en base al uso de los múltiples tipos de canales de difusión empleados por la organización; pero de igual manera, el comunicador puede ser creativo y aportar con ideas innovadoras para transferir el conocimiento, siempre y cuando, el medio se adapte naturalmente y respete la esencia de la corporación. Como punto de partida, para seleccionar dichos conductos de comunicación interna, se tiene que responder la pregunta de qué canales están activos en la entidad y quién tiene acceso a ellos. Dado que toda la organización por igual debe interpretar, conocer y poner en práctica la cultura de seguridad informática en la organización, la comunicación debe ser oblicua o transversal como descendente. Se tiene que

dar entre los niveles jerárquicos junto a las demás áreas de la corporación en una manera perpendicular, entonces, se modifican los comportamientos generales de todo el conjunto en beneficio de la protección de los sistemas digitales y se da un énfasis general en cada parte estructural de la organización. Pero, adicionalmente poseerá un movimiento descendente, es decir, los superiores tienen que difundir las prácticas de ciberseguridad a sus subordinados para que se refleje liderazgo y control desde arriba, lo que aumenta la posibilidad de éxito en cuanto a la mitigación más débil del sistema, el propio funcionario de cualquier jerarquía que por ingenuidad, cae en las trampas de los delincuentes (Brandolini & Frigoli, 2009). Por ello, es necesario primero dirigir las capacitaciones a los componentes de los niveles más altos, para que estos transmitan este ejemplo a las partes más bajas de la estructura organizacional. Por otra parte, porque en el caso de los canales de difusión de una campaña de seguridad informática para un negocio pueden ser varios, estos deben ser formales y generar una impresión de seriedad; mediante esto, los empleados relacionan a la campaña con la responsabilidad y el rigor de la ciberprotección, lo que evitará que se tomen a la ligera la relevancia del tema. En base a los medios de comunicación interna más empleados actualmente, a continuación se presentarán diferentes ideas de cómo emplearlos para transmitir las prácticas de ciberseguridad en la entidad. El correo electrónico es uno de los medios más empleados dentro de las empresas para compartir comunicados e información importante, los colaboradores de los cargos más elevados pueden informar sobre las iniciativas de la campaña de seguridad informática a los demás empleados. Al mismo tiempo que tendrían la responsabilidad de compartir correctamente las políticas de ciberseguridad a través de este medio. Por medio de los emails, se puede informar sobre las próximas actividades de la campaña y ejecutar las fases expectativas, informativas y de recordación. Se pueden crear vídeos, piezas gráficas, ilustraciones y materiales audiovisuales de información respecto a las rutinas que se están impulsando sobre la estrategia de defensa cibernética. Las redes sociales

corporativas es otro medio que puede ser empleado para divulgar sobre las prácticas, políticas e iniciativas de la campaña, se mostraría de una manera rápida y didáctica sobre qué acciones de seguridad informática los empleados deben seguir, además de que es un elemento eficiente para conseguir feedback por parte de los públicos. Otra manera aún más ágil de favorecer el traspaso de la comunicación de las reglas, prácticas y enseñanzas ciberseguras a los colaboradores mientras se consigue retroalimentación, es mediante los chats internos. A través de los contenidos precisos pero con mensajes valiosos; los empleados pueden seguir aprendiendo y reforzando sus conocimientos sobre protección digital. La emisión de comunicados escritos y contenido impreso visual también es otro método de compartición de la información que funciona para solidificar los mensajes. Es una buena idea el colocar infografías pedagógicas que encapsulan los conceptos de ciberprotección en puntos visibles dentro de las sedes de la organización, de esta manera, los funcionarios pueden revisar y leer sobre la seguridad informática y sus procedimientos que se están aplicando en la entidad. Junto a los gráficos informativos, es posible imprimir manuales individuales para cada colaborador en donde se les comunique todo sobre la defensa digital y se les incentiva las prácticas que prevengan ataques cibernéticos. Estas guías escritas también tienen la capacidad de incluir un instructivo concebido por expertos en comunicación junto a informáticos altamente cualificados sobre qué hacer en caso de que exista un ataque exitoso que no se haya podido prevenir. En este texto se debe detallar tanto acciones técnicas como comunicativas internas y externas para que los empleados tengan un marco teórico previo en caso de una amenaza materializada. Como siguiente punto, se tienen mencionar a las propias capacitaciones presentadas en forma de eventos donde prime la educación y entrenamiento práctico. En función de impartir el conocimiento formalmente sobre la prevención de pirateos informáticos y acción contra éstos, se deben formar convenios con otras empresas de seguridad informática para invitar a expertos en el área a la organización que faciliten un plan de formación y

preparación práctica destinada a los trabajadores. Estos eventos estarían acompañados por reuniones donde se informan sobre temas de seguridad informática o videoconferencias según la facilidad y disponibilidad de los colaboradores. Todos los procedimientos mencionados anteriormente corresponden a métodos de comunicación tradicionales basados en los medios de difusión más recurrentes en las organizaciones, sin embargo, existen maneras creativas de transmitir la información.

Los mensajes pueden ser comunicados de muchas maneras y los responsables tienen una gran variedad de canales y formatos a su disposición, una de las alternativas más creativas puede ser la gamificación. Consiste en dinámicas de juego que potencian la transmisión del conocimiento para los colaboradores y crean cohesión en el grupo, lo que favorece al fortalecimiento de la cultura corporativa (Márquez, 2023). En el caso de la enseñanza de prácticas de ciberseguridad, se pueden diseñar juegos de diferentes tipos. Por ejemplo, la creación de desafíos de conocimiento con preguntas y respuestas relacionadas a las actividades, políticas y responsabilidades de la protección digital, se otorgan puntos y remuneraciones a los empleados que respondan acertadamente. También, es posible organizar rompecabezas y desafíos vinculados con el entendimiento de la cultura de ciberseguridad para facilitar la comprensión de las rutinas de defensa de datos. Transformar la capacitación en una experiencia jugabilística es otra alternativa en la cual los funcionarios pueden avanzar niveles según cómo completan módulos de aprendizaje sobre temáticas puntuales de seguridad informática (Fábregas & Tejedor, 2021). Este tipo de metodologías de instrucción y comunicación son dinámicas e innovadoras que entretienen y motivan a los funcionarios porque se sienten empoderados (Cáseres, 2019). Como idea, se pueden realizar simulaciones de phishing y preguntar a los empleados si es un intento de hackeo o no, entonces, se reforzará el conocimiento a la par que se crea un vínculo entre los públicos y la seguridad cibernética

(Aldawood & Skinner, 2019). Cabe recalcar que esta estrategia tiene que estar fundamentada en los demás esfuerzos de comunicación interna y capacitaciones, donde los participantes apliquen su pensamiento crítico, habilidades de resolución de problemas y conocimientos teóricos para responder cuestionamientos que simulan la realidad en un entorno seguro (Mio & Ventura, 2019).

3.4 Concepto de comunicación en crisis aplicado en la seguridad informática:

Ahora, en caso de que el ataque informático sobrepase la barrera de prevención constituida por la estrategia de comunicación interna de prevención, se debe aplicar los conceptos en un contexto de crisis. Cada organización puede estar expuesta a sufrir un ataque exitoso que ponga en peligro el equilibrio natural y la imagen de la institución, pero gracias a la sólida cultura corporativa y la pertinente aplicación de las estrategias de transmisión de la información internas, hay caminos para mitigar y solventar este peligro. Entonces, la comunicación en crisis son las diferentes estrategias de la transmisión de la información a los públicos internos (colaboradores) y externos (opinión pública) de una organización con el objetivo de enfrentar y reaccionar ante un acontecimiento inesperado que compromete la imagen y funcionamiento normal (Yaguache, 2019). En este caso, uno de los sucesos imprevistos ya fue contemplado y corresponde a una vulneración cibernética.

3.5 Estrategias de manejo de la crisis:

Ante todo, se tiene que identificar el objetivo principal de los esfuerzos de la gestión de crisis, en este caso, la meta básica es proteger la reputación e imagen interna y externa de la organización mientras que se destinan acciones para solventar la crisis informática lo antes posible. Muchas veces, las crisis también representan oportunidades para mejorar fallos y potenciar la comunicación de la empresa, en caso de identificar estas ventanas abiertas, se deben aprovechar (Fernández et al, 2016). Para arrancar, la administración de comunicación

necesita de la participación de todos los públicos internos que actúan con resiliencia como un soporte firme frente a la turbulencia producida por la crisis. La estrategia de comunicación en crisis parte del principio de ofrecer respuestas rápidas según las prácticas promovidas en la fase de anticipación de amenazas informáticas y defensa contra estas. Los empleados deben saber cómo actuar, responder y qué estrategias se tomarán en función de mitigar los daños de la emergencia. Por ello, la etapa de prevención de comunicación interna dispuesta previamente crea una cultura de seguridad que solidifica a los grupos y estos están prevenidos y tienen lineamientos sobre qué hacer cuando se produce un ataque exitoso. Así, emprenderán las prácticas enfocadas en la mitigación cuyo aprendizaje fue inculcado anteriormente mediante talleres de aprendizaje, esfuerzos de comunicación, uso del manual de crisis, etc. Este último será de gran utilidad porque los empleados se basarán en lo mencionado aquí para corregir los desperfectos originados por la crisis y enfrentarla bajo lineamientos útiles. De tal forma, la sólida y correcta transmisión de mensajes internos es una de las formas a tolerar y, progresivamente, aliviar la crisis. Como acciones técnicas que se tienen que comunicar a los empleados no encargados oficialmente de la seguridad informática para atenuar la dificultad, se podría pedirles que usen los antivirus para encargarse de la desinfección rápida de los equipos de la entidad, restaurar los respaldos que se habían realizado con anterioridad, reportar cada fallo y mencionarles los desperfectos a los encargados de tecnologías de la información y al equipo de seguridad informática también es crucial.

La formulación de un comité de crisis es fundamental, este debe estar organizado por responsables en todos los niveles y expertos en informática. Esta agrupación direcciona las actividades y compone reacciones ante la crisis, entonces, administran cotidianamente el problema. Elaborar matrices donde se evalúen los riesgos a modo de anticipación es una gran opción, además, se deben especificar los niveles de alarma y los tipos de respuesta. Gracias a

la etapa de anticipación y la cultura de seguridad, se pueden elaborar planes generales y específicos para cada situación (Islas & Hernández, 2012). Entonces, el comité tomará las decisiones y comunicará internamente lo que se realizará.

Ahora, para la gestión de comunicación para los públicos externos involucrados, es importante anticipar que los usuarios consumidores experimenten retrasos, fallas en el sistema y problemas determinados. Por lo tanto, cada funcionario deberá responder rápida y precisamente mientras que soluciona las necesidades del cliente mientras que se adelanta ante posibles escenarios relacionados con el entorno informático (Marín, 2009). En cada uno de los casos, la transparencia es un valor clave, se tiene que evitar manipular la verdad, admitir los errores y demostrar que se están tomando acciones rápidas desde la empresa para responder ante la vulneración a través de la comunicación. Acompañado de la emisión de disculpas públicas y reconocimiento de los errores, cada paso que se dé para solventar la crisis tiene que ser indicado mediante los medios que informan hacía el exterior. Con el objetivo de recuperar la confianza, es importante transmitir que las prácticas de prevención también funcionaron para mitigar el ataque informático y que la entidad reforzará aún más sus esfuerzos de defensa en base a los aprendizajes adquiridos. Por consiguiente, el seguimiento poscrisis estará relacionado con cada uno de los esfuerzos de solidificación de la transmisión del mensaje que la empresa ha aprendido de sus errores, a la par que trabaja duro para recuperar la credibilidad de sus clientes. La comunicación en crisis proporciona puertas con salidas útiles para proteger, no solo la integridad informática de la organización, sino también su imagen y reputación; sin embargo, esta se basa en una buena estrategia de transmisión interna y de las buenas prácticas de los colaboradores.

CAPÍTULO 4: HUMAN FIREWALL

4.1 Presentación de la campaña de Comunicación y pertinencia:

Para comenzar, la campaña de Comunicación Interna a realizar es de suma importancia, no solo para las organizaciones y sus colaboradores, también para todos los usuarios como tal. Ecuador se encuentra en un contexto donde la inseguridad es un problema sumamente recurrente y una de las maneras más comunes de robar a las personas es digitalmente. Las organizaciones son el blanco predilecto de los ciberdelincuentes, a pesar de que estos últimos cuentan con múltiples técnicas para vulnerar sistemas, casi siempre los ataques inician a través de la Ingeniería Social. Tal es así que, según cifras del 2023, el Phishing es el método responsable del 91% de casos de ataques informáticos y el usuario es el primer vector de ataque, es decir, la primera barrera de ciberseguridad que los hackers intentarán vulnerar para acceder al sistema será al usuario (Secureframe, 2023). Para fortalecer este escudo informático, se deben utilizar campañas de comunicación que empoderen a los colaboradores a ser responsables con sus prácticas cibernéticas. Al mismo tiempo, se busca eliminar el exceso de confianza y las acciones impulsivas que pueden producir catástrofes para las personas y las empresas en donde se desenvuelven. Es muy importante informar y prevenir sobre cómo los ciberdelincuentes utilizan, malintencionadamente, la comunicación persuasiva para lograr que los usuarios les concedan acceso ingenuamente. Esto se logra a través de la propia comunicación bien intencionada, cuya función será reforzar una coraza constituida por los propios funcionarios que no son presas de los mensajes sugestivos de los hackers y no permiten que ingresen malwares informáticos ni entregan información sensible sin darse cuenta. A pesar de que existen múltiples organizaciones que utilizan grandes esfuerzos de comunicación para entrenar a sus colaboradores para prevenir el Phishing y la Ingeniería Social como Pronaca o Banco

Pichincha, aún se puede trabajar con más empresas pequeñas, medianas y grandes en función de reforzar la ciberseguridad y corregir los errores humanos que producen vulneraciones. Este trabajo constituye uno de los primeros pasos en cuanto a cómo utilizar la comunicación interna para prevenir ciberataques. De manera académica, esto es un preámbulo para muchos más trabajos y campañas que recurrirán a la transmisión de mensajes estratégicos que informen a los usuarios sobre acciones responsables que les protejan frente a una amenaza que cada día cobra más fuerza.

4.2 Enfoque sostenible (objetivos de desarrollo sostenible):

La campaña está vinculada con el Objetivo de Desarrollo Sostenible número 9, industria, innovación e infraestructura. Esto porque tiene que ver con la innovación de la comunicación y sus estrategias en las industrias en función de evitar ciberataques. Además, el tema se trata de la combinación entre temas de tecnología junto a la comunicación y concientización de cómo usar plataformas correctamente. La informática crece cada día con nuevos desarrollos de software y hardware; pero al mismo tiempo, las amenazas también aumentan con nuevas tácticas de engañar al usuario a través de la persuasión y las herramientas tecnológicas utilizadas para estafar. Por ejemplo, ahora es posible utilizar la inteligencia artificial para engañar a los usuarios. Entonces, es vital relacionar la campaña junto a este ODS y enfocar las prácticas de comunicación interna dentro de organizaciones para evitar vulneraciones informáticas.

4.3 Enfoque social de la campaña:

El problema social que la campaña busca solucionar es el exceso de confianza e ingenuidad de los usuarios que resulta en delitos informáticos. Pero al mismo tiempo, se busca mitigar el mal uso de la comunicación estratégica para desinformar, persuadir y estafar. Como se mencionó antes, Ecuador es uno de los países más atacados informáticamente,

además, vive en un contexto de inseguridad y la desinformación ya ha causado graves problemas anteriormente. Los pirateos informáticos explotan múltiples tipos de fallos en los sistemas y la falta de educación en temas de ciberseguridad por parte de los usuarios es uno de esos errores. Aquí la comunicación ayuda a la protección informática para conquistar el error humano mediante la instrucción.

4.4 Enfoque comunicacional de la campaña:

La campaña manejará un enfoque de Comunicación Interna dentro de organizaciones. Igualmente, las acciones consisten en informar, concientizar, enseñar y empoderar a los colaboradores múltiples prácticas de ciberseguridad a través de charlas. Aquí se mostrará cómo identificar y prevenir el Phishing y la Ingeniería Social a través de pautas y consejos, se comunicarán ejemplos de casos reales donde se demostrarán formas de darse cuenta sobre cuándo un mensaje es real o falso. Además, se proporcionarán más acciones de ciberseguridad que son simples, poderosas y muy cotidianas. Una de ellas consiste en asegurarse de estructurar contraseñas seguras que sean difíciles de adivinar. También es importante que los colaboradores comprendan la importancia de usar e invertir en antivirus para asegurar sus sistemas; y, no confiar en cualquier información que provenga de internet, es importante corroborar cada dato a pesar de que suene real. Por ende, el mensaje que se busca transmitir es el de desconfiar, que en este tema, la duda es el poder del usuario porque lo protege, entonces, es muy pertinente dejar a los colaboradores con esta información para prevenir ciberataques. Debido a la pertinencia de la iniciativa y porque todos pueden ser presas de estas trampas sin distinción, la campaña trascienden en cuanto audiencias se refiere y se expande, no solo a funcionarios internos de corporaciones, sino todos debemos aprender sobre ciberseguridad para poder defendernos.

4.5 Investigación cualitativa para la campaña:

Se llevó a cabo una investigación cualitativa para comprender la profundidad de la combinación de las áreas de Comunicación Organizacional junto a la Ciberseguridad. Dado que se emplea la Ingeniería Social en contra de los usuarios para que cometan errores que llevan a la vulneración de sistemas de empresas, es pertinente recolectar los datos mediante técnicas cualitativas para conocer perspectivas a profundidad. Se delimitó el espacio del estudio a Ecuador, principalmente Quito. Los hallazgos se convierten en una hoja de ruta para ejecutar una campaña de comunicación interna que trascienda externamente para reforzar la seguridad informática. Partiendo de que Ecuador es un país muy atacado informáticamente, con mucho trabajo de defensa por desarrollar y que el error humano siempre se da, se emplearon múltiples métodos de investigación cualitativa.

La primera técnica de indagación fueron las entrevistas conducidas a diferentes expertos de ciberseguridad y un especialista en comunicación interna. Se prepararon múltiples preguntas concretas para cada uno de los expertos y se manejó la indagación como una conversación. El propósito era obtener insights, conocimiento particular, la pertinencia del tema y conseguir ideas sobre cómo ejecutar la campaña en base a experiencias de los consultados. El primer entrevistado fue Fabían Hurtado, profesional en Seguridad Informática y CEO de Ecforensics, una empresa de servicios, capacitaciones y soluciones de Seguridad Informática. El siguiente consultado fue Gustavo Cusot, experto en comunicación interna y coordinador de la carrera de Comunicación Organizacional en la Universidad San Francisco de Quito. El objeto de esta entrevista fue determinar la perspectiva comunicacional de este especialista para estructurar la campaña y las estrategias, entonces, fusionar los conceptos de comunicación interna y ciberseguridad en el contexto empresarial. Marco Rivadeneira junto a Juan Carlos Gómez, ambos cabezas principales de Greenetics, organización de seguridad informática, también fueron consultados. La entrevista estuvo

enfocada en conocer ideas para la campaña, cómo se llevan las capacitaciones de ciberprotección, a qué departamentos dirigirlas. la importancia de la ciberseguridad, más insights y hacer una alianza estratégica. Fausto Vasco, experto en Informática y director del departamento de Tecnologías de la Información de la USFQ también fue entrevistado, se le preguntó sobre el ataque contra la Universidad en el 2022, cómo lo mitigaron, cuáles son las prácticas ciberseguras que deben primar en los usuarios y qué tipo de instituciones y empresas son las más vulnerables.

Debido a que los grupos focales guían las discusiones de un grupo de personas, lo que permite conocer una mayor diversidad de perspectivas con varios matices, se empleó esta metodología para la investigación cualitativa. Se realizó el grupo focal a algunos funcionarios expertos en informática y se indagó sobre la importancia de las capacitaciones a los colaboradores internos, a qué sectores dirigir la campaña y la pertinencia de la comunicación interna para generar conciencia. Asimismo, una parte importante de la investigación fue la escucha activa en podcasts, vídeos y reportajes, además, se mantuvo una conversación con un funcionario del SERCOP, experto en redes y telecomunicaciones que me reveló más insights importantes como preámbulo para la creación de la campaña. La revisión del trabajo de Seguridad Informático de las empresas a partir de las publicaciones en redes sociales como Linkedin también fue otra de las tácticas de indagación utilizadas para analizar la percepción de la ciberseguridad por parte de las organizaciones. También se analizó el contenido sobre Hacking Ético y potenciales estafas compartido en redes sociales como Facebook, Instagram y YouTube con el objetivo de entender y determinar qué tipo de publicaciones se realizan y definir el tono de la ciberseguridad y los tipos de usuarios que postean sobre esto. Igualmente, se elaboró un monitoreo de medios de comunicación en Ecuador para precisar cómo los medios tratan al tema y qué se ha dicho previamente, con este conocimiento, se

puede definir una estrategia para lograr que los medios cubran las acciones realizadas durante la campaña.

Resultados de las entrevistas:

En primer lugar, los resultados de las entrevistas proporcionaron insights y conocimientos muy útiles para emprender la campaña de comunicación interna. Fabían Hurtado destacó que la Ingeniería Social es un ataque sumamente recurrente porque principalmente se aprovecha del error humano, incluso la gente experta puede ser presa de esta técnica por un descuido ya que caen por ego, emocionalidad y curiosidad. Las empresas están principalmente expuestas al Spear Phishing, ataques muy elaborados y direccionados que requieren de una investigación previa de las víctimas y de los puntos débiles de la organización. Cuando ingresan al sistema de las entidades víctimas, pueden capturar equipos y crear botnets, es decir, computadoras infectadas que expanden malwares y escalar privilegios para vulnerar sectores más específicos. Fabian hizo mucho énfasis al decir que los usuarios son muy cómodos y confiados, tienen contraseñas fáciles de adivinar, guardan su información en espacios informáticos vulnerables, utilizan la misma credencial para acceder a todas las plataformas y no se anticipan ante los potenciales riesgos existentes en la red. Mencionó que la seguridad no es infinita y que siempre existirán brechas, pero se puede trabajar mucho para reducir al máximo posible las amenazas informáticas. En cuanto a la comunicación interna, recalcó que es una herramienta sumamente importante para conformar una barrera de defensa para las organizaciones, señaló que la transmisión de información y las capacitaciones a los colaboradores deben ser incisivas y constantes, como un entrenamiento destinado a eliminar el exceso de confianza. Al mismo tiempo, hay que ser muy estrictos con las prácticas y la seguridad de las redes, los respaldos y las políticas. Por último, Fabian reveló que Windows es uno de los sistemas operativos más atacados mientras

que Linux es más complicado de vulnerar y se necesita mayor esfuerzo; entonces, si una empresa comienza a emplear este último, se agrega una poderosa capa que repele a los ciberpiratas.

Gustavo Cusot compartió su experticia en comunicación interna y explicó cómo se debería ejecutar una campaña de comunicación dentro del entorno laboral. Primero, se tiene que explicar a los colaboradores el concepto de ciberseguridad mientras que se les indica ejemplos concretos sobre los riesgos que corre la empresa en el ámbito informático. Al hacer esto, el comunicador debe asegurarse que los mensajes sean transmitidos de una manera real y tangible para implicar a los funcionarios, alertarles que cualquiera de ellos puede equivocarse y producir un ataque informático dentro de la organización. Entonces, se debe crear responsabilidad y empoderamiento en los colaboradores a través de la campaña con información poderosa, interesante y precisa, esta puede estar orientada a la indicación del por qué y cómo se previene. Gustavo puntualizó en no saturar a los funcionarios con mensajes repetitivos porque puede producir una respuesta negativa, en vez de esto, es importante que la comunicación impacte a un gran nivel a través de estrategias dinámicas y creativas. En cuanto a las herramientas, se deben emplear capacitaciones para enseñar y concientizar con contenido claro, sin abusar del uso de tecnicismos para no confundir ni aburrir. Como punto de partida, es inminente que la gerencia esté convencida de la pertinencia y sea capacitada en el tema, este sector transmitirá las prácticas correctas a los colaboradores y son cruciales para comunicar el mensaje de manera sólida. Si la gerencia está convencida, esto bajará como cascada para los funcionarios.

El equipo de Greenetics conformado por Marco y Juan Carlos también compartieron información sumamente valiosa para el desarrollo de la campaña, destacaron que las personas carecen de conocimiento sobre cómo se manifiestan y perpetran los ataques cibernéticos. La

falta de instrucción en esto es lo que lleva al exceso de confianza, los usuarios no se toman el tiempo para revisar los correos, enlaces, páginas e imágenes que les llegan. Debido a esto, el Phishing e Ingeniería Social son las técnicas más antiguas y usadas; además, en el entorno corporativo, se falsifican y suplantan páginas de pago y sitios de inicio de sesión fraudulentos de la propia empresa para lograr que el funcionario introduzca sus credenciales. Por ende, se debe construir una cultura de seguridad de la información en toda la organización facilitada por los esfuerzos de comunicación interna. Juan Carlos y Marco recalcaron que para proteger a la empresa se necesitan dos mitades, la primera de concientización por parte de los usuarios y la segunda está conformada por las herramientas técnicas informáticas. También, al igual que Gustavo, enfatizaron en la importancia de que la gerencia esté involucrada y sepa de los riesgos de los ataques informáticos para que la comunicación interna funcione de la mejor manera. Las capacitaciones deben ser entretenidas y despertar interés, por ende, el equipo de Greenetics propuso, en base a su experiencia, que en las charlas concientización pueden incluir una sección en la cual se instruye a los colaboradores sobre cómo piratear e indicarles hackeos en entornos controlados en tiempo real. Mencionaron que es importante realizar este tipo de iniciativas en Ecuador por los antecedentes existentes, el país no posee una estrategia nacional de ciberseguridad y las empresas aún deben trabajar en muchos aspectos. Adicionalmente, Ecuador se ha visto involucrado en temas políticos relacionados con el Hacking, como el caso Assange y el narcotráfico tiene buena presencia en este territorio. Por último, Marco y Juan Carlos manifestaron que invertir en ciberseguridad es como contratar un seguro financiero, donde los usuarios conocedores y preparados son una barrera de defensa importantísima con una cultura que se forma con el tiempo.

Fausto Vasco también reveló impactantes hallazgos sobre la ciberseguridad y la comunicación interna, primero, corroboró que la Universidad San Francisco de Quito fue

víctima de un Ransomware ejecutado a través de la introducción de un archivo infectado en la red. Se presume que la persona que infectó los equipos fue víctima de una técnica de Ingeniería Social, entonces, hubo un secuestro de la información crucial que permitía el funcionamiento de algunos sistemas. Esto ocurrió el 26 de diciembre del 2022, el equipo de Tecnologías de la Información tuvo que levantar todos los sistemas de la USFQ nuevamente y casi desde cero. Fausto fue claro al decir que la Ingeniería Social es una de las formas más accesibles de vulnerar un sistema y que la comunicación interna y la concientización es una de las primeras líneas de defensa porque la comunidad informada reacciona positivamente y en defensa propia de los sistemas. Así, es importante enseñar a los funcionarios a reconocer engaños provenientes de ciberdelincuentes, entrenarlos para que verifiquen los correos electrónicos que les llegan y los archivos ejecutables que pueden abrir; asimismo, recordarles que no es común que te pidan el nombre de usuario ni la clave de acceso. Otras buenas prácticas mencionadas por Fausto son el reconocimiento de mensajes falsos que ingresan a los celulares, usar el factor doble de autentificación y nunca confiarse porque los ciberpiratas están a la orden del día, atacando a sectores como bancos, hospitales, universidades, cooperativas, etc.

Grupos focales:

Entre los resultados obtenidos por los grupos focales se puede destacar que nuevamente aparecen las capacitaciones como herramienta crucial de una estrategia de comunicación interna coordinada con la ciberseguridad. Los funcionarios también dejaron en claro que es fácil vulnerar páginas webs de pequeñas empresas cuyas barreras informáticas son muy básicas porque no destinan fondos a esta área. También dijeron lo cerca que está el tema para los colaboradores, contrario a lo que muchos pueden pensar que hackear depende de conocimientos puramente técnicos de informática, la Ingeniería Social emplea el uso de la

psicología y comunicación persuasiva para cometer un atentado de ciberseguridad. Por ende, los funcionarios tienen que reconocer estos métodos de pirateo y la comunicación interna facilita el espacio por el cual compartir los mensajes con la capacidad de reforzar las enseñanzas que resultan en comportamientos propios de culturas ciberseguras.

Conversación con colaborador del área de sistemas de SERCOP:

La conversación con un colaborador del Servicio Nacional de Contratación Pública reveló que esta entidad, por ser estatal, siempre se encuentra recibiendo y repeliendo ataques. Puntualizó que la comunicación interna sí es un aditamento esencial para la ciberseguridad en función para conformar la barrera protectora del usuario. Mencionó que la gente es confiada, por ejemplo, tienen muchas cuentas y datos sensibles que son complicados de memorizar almacenados en lugares de fácil acceso, si los hackers logran entrar al sistema de la víctima, podrán determinar las credenciales muy fácilmente. Por lo tanto, una práctica cibersegura es anotar en una libreta las contraseñas y cuentas, sin necesidad de guardar la información de inicios de sesión en las páginas web para acceder rápidamente. De igual manera, una forma de ciberseguridad es evitar mostrar nombres de familiares, mascotas, direcciones, fechas de nacimiento, gustos, entre otras, esto se debe a que se está entregando algunos datos a los hackers para descifrar contraseñas.

Etnografía:

La etnografía consistió en revisar el material compartido por las empresas respecto a la ciberseguridad y entender cómo es el trabajo de las mismas en esta área. Se publican casos de éxito, testimonios y las instituciones educativas promocionan capacitaciones especiales y cursos donde se enseña más sobre seguridad informática a partir de ciertos requisitos. Los bancos sí brindan espacios de concientización y alertas en sus redes sociales, por ejemplo, en Instagram, Banco del Pichincha comparte sobre qué es el Phishing y cómo no caer en estos

mensajes y realiza esfuerzos de Comunicación Interna para instruir a sus colaboradores en materia de ciberseguridad como charlas y eventos con juegos interactivos. Por otra parte, las corporaciones también ejecutan peritajes para comprobar la protección de sus sistemas, auditan para encontrar sus puntos débiles y entre estos, el usuario es muy frecuente. Emplean pirateos autorizados en ambientes controlados a sus propios equipos y utilizan la Ingeniería Social constantemente para determinar si los colaboradores son fácilmente persuadidos. Posteriormente, recurren a la estadística para evaluar cuantitativamente los resultados de las auditorías de ciberseguridad y tomar acciones en base a esto.

Análisis de Contenido:

En el análisis de contenido en redes sociales, se exploraron las publicaciones de seguridad informática y cómo puede aparecer la Ingeniería Social en estas plataformas. Entonces, se identificó que pueden existir perfiles falsos, anuncios maliciosos, comentarios por parte de usuarios malintencionados, estafas, etc. Por ejemplo, en los grupos de Facebook se ofrece ayuda, a cambio de dinero, para que los usuarios recuperen sus cuentas de redes sociales que han sido vulneradas o han perdido sus credenciales. Esta es una oportunidad para los engañadores porque pueden obtener dinero de las víctimas, no hacer el trabajo en cuestión y los usuarios son engañados porque optaron por este servicio como resultado de su desesperación. Existen perfiles de Instagram donde los usuarios les gusta promover el estereotipo de cómo es un hacker: figura encapuchada oculta en un cuarto oscuro que utiliza múltiples computadoras con programas muy sofisticados, casi como hacer magia. Además, este tipo de cuentas comparten contenido educativo sobre el uso de aplicaciones de hacking e historias sobre vulneraciones con motivos éticos. Es importante mencionar que incluso quienes quieren aprender a hackear por una motivación determinada pueden ser víctimas de ataques de Ingeniería Social. Esto se debe a que los ciberpiratas venden códigos y

aplicaciones que “hackean” pero realmente son softwares malignos que infectan los dispositivos de los usuarios. Hay cuentas falsas que ofrecen recuperación de perfiles, servicios de pirateo independiente y publican comentarios respecto al tema, sin embargo y presumiblemente, esto también se trata de estafas contra los usuarios que pueden caer ingenuamente. Por otro lado, hay comunidades que comparten contenido sobre el Hacking Ético, disciplina que refuerza la ciberseguridad a través de ataques supervisados para monitorear la fortaleza de los sistemas defensivos y anticiparse contra amenazas informáticas. En estos grupos se transmiten mensajes con un tono más profesional, donde predomina la educación y el deseo de aprender para prevenir. Por último, en un podcast, se escuchó a un experto destacar que los usuarios no podemos “incontinencia clickaera”, es decir, pensar dos veces antes de darle click a un ejecutable, también destaca la importancia de ayudar y capacitar al usuario.

Monitoreo de medios:

Con el fin de determinar la estrategia de medios para la campaña, esta metodología de investigación consistió en determinar con qué frecuencia los medios de comunicación hablan sobre ciberseguridad en Ecuador. Se encontró que la regularidad con la que los medios replican este tema es muy habitual, particularmente, en épocas del año donde el movimiento económico es alto y las estafas ocurren reiteradamente. Además, durante el contexto de los apagones de octubre-diciembre del 2024, los medios de comunicación se encuentran activamente informando y desmintiendo sobre correos falsos de Phishing e Ingeniería Social vinculados con la Corporación Nacional de Electricidad (CNEL). Los temas que combinan ciberseguridad junto política también son asuntos muy reproducidos por los medios, junto con casos de empresas, públicas y privadas, que han sido víctimas de vulneraciones informáticas. De igual manera, se busca informar a la ciudadanía y los usuarios de prácticas

ciberseguras que evitarán que sufran pirateos en sus dispositivos; al analizar este tipo de contenido, se puede deducir que los medios buscan generar valor a sus audiencias y mantenerlas protegidas de los ciberataques. Por lo tanto, a modo de refuerzo, es pertinente continuar difundiendo mensajes que generen conciencia acerca de la ciberseguridad en las personas y sobre su papel fundamental en la defensa de sus sistemas propios y de sus organizaciones de trabajo. Dado que la coyuntura de este tema es alta, existe una buena oportunidad de colaborar con los medios de comunicación para compartir prácticas ciberseguras que contrarresten las técnicas de Ingeniería Social.

4.6 Diseño, planificación y ejecución de la campaña:

Nombre:

El nombre de la campaña es “Human Firewall”. Se la nombró así para combinar un término de ciberseguridad junto al usuario, la campaña trata de crear un escudo y fortalecer la barrera humana de los sistemas informáticos. Un firewall o cortafuegos es un sistema de seguridad informática de red que actúa como una barrera protectora, bloquea los malwares provenientes de internet y del exterior para mantener los dispositivos y sistemas informáticos seguros. El objetivo del nombre es vincular a los usuarios con este procedimiento y pared de ciberseguridad para crear un escudo humano que funcione como un firewall frente a la Ingeniería Social. Esto quiere decir que los usuarios están prevenidos, se protegen y evitan cometer errores frente a intentos de ciberataques que utilicen la persuasión y sugestión.

Concepto de campaña y logotipo:

Human Firewall es una campaña de Comunicación Interna que utiliza las capacitaciones y estrategias de educomunicación dentro de las organizaciones para conformar una barrera de defensa constituida por los colaboradores. El concepto fundamental de la campaña es enseñar a los funcionarios a estar protegidos según tres ejes. El primero se relaciona con cómo identificar posibles amenazas de Phishing e Ingeniería Social e inculcar la desconfianza frente a mensajes sugestivos como medida de defensa. El segundo eje tiene que ver con la promoción de hábitos ciberseguros como la utilización de contraseñas fuertes y el uso de la autenticación de dos pasos en todas cuentas. El tercer punto busca promover prácticas simples pero eficientes de responsabilidad digital como el uso activo de antivirus, la desconfianza de códigos QR y de contenidos producidos en internet a través de la inteligencia artificial, también conocidos como deepfakes. Se ilustran los conceptos bajo temáticas de tecnología e informática, desde la tipografía hasta las decoraciones de los artes gráficos, se

maneja la computación y su entorno como protagonistas de la campaña. Esto se debe a que la gente identifica a la ciberseguridad como un tema de tecnología; y, en función de crear impacto y recuerdo en los colaboradores y que estos últimos sigan las definiciones de la campaña con mayor familiaridad, se emplean ilustraciones con temas informáticos como conceptos principales. Además, el símbolo del escudo es un elemento gráfico muy importante para la campaña porque simboliza la protección y guardia frente a las ciber-amenazas.

El logotipo diseñado para la campaña representa, nuevamente, el escudo tecnológico utilizado por los usuarios para bloquear ataques informáticos. Así, el isotipo constituye una analogía del concepto de cortafuegos cuya llama funciona para añadir dinamismo al logotipo. Los colores escogidos mayormente son el azul y el celeste, esto con el propósito de representar a la tecnología con colores y seguir con el concepto planteado anteriormente. De igual forma, el escudo tiene toques de informática y decoraciones que vinculan a esta herramienta de protección con un instrumento tecnológico. En cuanto a la tipografía, se busca demostrar innovación y computación a través de las formas de los caracteres, además de contiene rojo con el objetivo de contrastar las palabras. De esta manera, el logotipo de Human Firewall simboliza un escudo protector informático frente a los ciberdelincuentes.

Figura 1: Logotipo de Human Firewall

4.7 Mapa de públicos:

Human Firewall se dirige a un público principalmente corporativo y esto depende de la estructura organizacional de cada empresa. Es decir, la campaña de Comunicación Interna apunta a generar impactos en empresas y organizaciones a través de la concientización de múltiples grupos de colaboradores. A continuación se realizará un mapeo de públicos.

Alta dirección:

Alta dirección:	
Perfiles:	Gerentes y directores
Preocupación:	Mantener la seguridad y proteger los activos estratégicos de la organización.
Objetivo con este sector:	Asegurar que comprendan la importancia de ciberseguridad y hacer que promuevan la campaña dentro de la organización.
Canales y métodos de comunicación:	Reuniones ejecutivas, charlas, comunicaciones directas por correo o presentaciones, contenido audiovisual.
Mensaje:	“Invertir en la ciberseguridad es como invertir en un seguro, se ahorran pérdidas millonarias y el potencial quiebre de la organización. La alta dirección debe entender la importancia de la prevención de los ataques de Ingeniería Social para transmitirlo a los demás”.

Tabla 1: Mapeo de alta dirección

Departamento de TI y personas vinculadas a este sector:

Tecnología de la Información y vinculados	
Perfiles:	Especialistas en TI, ingenieros de sistemas, analistas de ciberseguridad.
Preocupación:	Implementación y supervisión de protocolos de seguridad, minimización de riesgos cibernéticos, soporte técnico, y cumplimiento con estándares de seguridad.
Objetivo con este sector:	Apoyar la campaña desde el punto de vista técnico y asegurar que las herramientas y recursos de ciberseguridad estén disponibles para todos los empleados.
Canales y métodos de comunicación:	Reuniones técnicas para revisar contenidos de la charla, comunicación a través de correos electrónicos y WhatsApp, charlas de refuerzo.
Mensaje:	"Todos podemos ser susceptibles a un ataque de Ingeniería Social, mantengamos la guardia en alto. Es hora de configurar un firewall humano en contra de los ciberataques".

Tabla 2: Mapeo de TI

Departamento de Comunicación Interna y Recursos Humanos:

Comunicación Interna y RRHH	
Perfiles:	Comunicadores organizacionales y especialistas en Recursos Humanos de las organizaciones.
Preocupación:	Resolver problemas relacionados con la comunicación y con el personal, prevenir malentendidos y capacitar a los colaboradores para que estén protegidos de los pirateos.
Objetivo con este sector:	Capacitarlos y concientizarlos sobre ataques informáticos para que transmitan los mensajes de ciberseguridad y se logre corregir vulnerabilidades humanas de manera eficiente.
Canales y métodos de comunicación:	Reuniones, charlas, comunicación a través del correo electrónico y WhatsApp.
Mensaje:	“La comunicación tiene varios usos, pueden ser positivos o negativos, en este caso, funciona para corregir una vulnerabilidad relacionada con el error humano”.

Tabla 3: Mapeo de Comunicación y RRHH

Sectores operativos:

Sectores operativos:	
Perfiles:	Divididos en departamentos como adquisiciones, marketing, ventas, eventos, contraloría, etc.
Preocupación:	Realizar su trabajo de manera eficiente, evitar distracciones innecesarias y proteger su información personal y profesional.
Objetivo con este sector:	Sensibilizarlos sobre los riesgos de ataques de ingeniería social y phishing, y capacitarlos para reconocer y evitar estas amenazas en su día a día, esto les mostrará sus roles, responsabilidades y les empodera a promover prácticas ciberseguras.
Canales y métodos de comunicación:	Charlas, vídeos explicativos, comunicación a través del correo electrónico y WhatsApp, evaluaciones prácticas de ciberataques.
Mensaje:	"¡La seguridad de (nombre de la empresa) depende de ti, piensa dos veces antes de dar un clic! Tu superpoder es desconfiar, eres la primera línea de defensa, no te descuides".

Tabla 3: Mapeo de sectores operativos

Todo tipo de audiencias:

Público en general	
Perfiles:	Niños, jóvenes, adultos, adultos mayores.
Preocupación:	Proteger sus datos sensibles, privacidad, información personal y bancaría.
Objetivo con este sector:	Sensibilizarlos sobre los riesgos de ataques de ingeniería social y phishing, levantar conciencia en ellos para que emprendan prácticas ciberseguras responsables.
Canales y métodos de comunicación:	Medios de comunicación tradicionales, redes sociales y eventos.
Mensaje:	"Tú le abres las puertas a los ciberdelincuentes sin darte cuenta, pero también puede cerrarla si es que estás ciber-pilas".

Tabla 4: Mapeo del público en general

Alianzas estratégicas:

Las organizaciones donde se realizan las charlas también se catalogan como aliados estratégicos de Human Firewall. Esto porque están brindando el espacio, tiempo y los colaboradores para ejecutar la campaña. Además, en el caso, de la Universidad San Francisco de Quito, los expertos en ciberseguridad ofrecen una verificación y asesoría gratuita sobre el contenido de la capacitación. Este tipo de aliados estratégicos son la ya mencionada USFQ, Hotel GoQuito, Instituto Superior Tecnológico de Fútbol Quito y el Centro Cultural Metropolitano. Por otra parte, la campaña contó con otros aliados estratégicos que en la etapa de investigación facilitaron su conocimiento de ciberseguridad para idear, estructurar y

realizar las charlas, estos son Ecforensics y Greenetics. Asimismo, los medios de comunicación tradicionales también tienen un papel clave en los aliados estratégicos, a través de estos se difunde la campaña y las prácticas responsables de ciberseguridad a todo tipo de públicos. Además, este público genera contenido de valor para informar a sus audiencias y mantenerlas protegidas. Por ende, el apoyo de los aliados estratégicos es un elemento clave para diseñar la campaña y ejecutarla con éxito.

4.9 Planificación de la campaña:

Fase Expectativa:

Esta fase de la campaña será realizada principalmente en la red social de Instagram, plataforma escogida para publicar contenido relacionado a la campaña. Esto debido al alcance y número de usuarios cuyas necesidades cotidianas también están relacionadas a estar seguros dentro de estos espacios digitales. Durante esta fase, se lanza el primer vídeo en redes sociales con el objetivo de exponer los peligros de la piratería informática durante septiembre y diciembre del 2024 en Ecuador. La idea es mencionar y preguntar a los usuarios y colaboradores de las organizaciones si están preparados para defenderse e identificar un intento de ciberataque. Por ende, la fase expectativa, con una duración de una semana, consiste en anunciar el lanzamiento de Human Firewall para educar a las personas mientras que en esta fase se concretan las alianzas estratégicas con diferentes empresas y medios de comunicación que son claves para facilitar la campaña.

Fase informativa:

La fase informativa, igualmente, se desarrolla en redes sociales a través de publicaciones que indican cómo los ciberdelincuentes engañan a los usuarios. Pero al mismo tiempo, se informa cómo los usuarios tienen la oportunidad de defenderse frente a los

intentos de vulneración de los hackers. Se mostrarán artes y vídeos con el mensaje de la desconfianza hacia los correos y mensajes de desconocidos en las redes sociales. Además, se expone a los equipos de comunicación y recursos humanos de las organizaciones aliadas de la campaña sobre qué es la Ingeniería Social y el importante papel de la divulgación en función de prevenir estos ataques contra los funcionarios. Durante esta etapa con una duración de dos semanas, se explicará qué es la campaña, los riesgos de ciberseguridad y cuál es el propósito que se persigue vinculado a la creación de una cultura de seguridad cibernética.

Fase educativa:

Como fase clave de la campaña, la estrategia de edu-comunicación se convierte en el pilar esencial de Human Firewall. La iniciativa apunta a crear resultados reales, no solo dentro de las organizaciones, sino que todos los usuarios estén preparados para identificar y rechazar las ciberamenazas. Así, se utilizarán las charlas como herramienta principal para inculcar prácticas de protección digital en los colaboradores y se les extenderá la invitación a que compartan dichos consejos con sus familiares y amigos. La capacitación sobre ciberseguridad abordará temas como la explicación e identificación de la Ingeniería Social y el Phishing; qué son y cómo configurar contraseñas seguras; tutoría sobre cómo configurar la autenticación de factores múltiples en todas las cuentas de los usuarios y la enseñanza de prácticas de ciberseguridad cotidianas y muy efectivas. Cabe recalcar que para ejecutar estas charlas, se deberá recibir asesorías de expertos en el área de seguridad cibernética para que la información expuesta sea totalmente precisa y correcta. Después de cada capacitación, se busca realizar una serie de preguntas a los participantes donde se les pedía que identifiquen mensajes reales o falsos para determinar su comprensión a la Ingeniería Social. Al mismo tiempo, durante esta fase se llevarán a cabo entrevistas y publicaciones junto a medios de

comunicación tradicionales como FM Mundo, La Mega y Telesucesos. Esto es una estrategia de comunicación externa para compartir la campaña junto a su tema con todo tipo de audiencias, el contenido de ciberseguridad genera valor para los medios que buscan informar y proteger a su público. Así, se difunde sobre qué es Human Firewall, las acciones de capacitación de la campaña, qué es la Ingeniería Social y el Phishing y cómo defenderse frente a esto para alertar a todos los usuarios y trascender. Esta fase combina las charlas junto a la transmisión del mensaje en medios de comunicación para elevar el alcance del mensaje y prevenir a todos los usuarios en función de crear una cultura de ciberseguridad. También se ejecutará el evento ReConecta para generar interacción e informar a los asistentes.

Fase de refuerzo:

Para reforzar los mensajes transmitidos en la campaña, se recurrirá a la red social de Instagram y a los medios de comunicación una vez más. La plataforma de internet funcionará para continuar con la transmisión eficaz de mensajes que sostengan la alerta y desconfianza en los usuarios. Además de que se compartirán testimonios sobre víctimas de hackeos y cómo cayeron en estas trampas para mantener a los espectadores atentos a las ciberamenazas. Asimismo, se realizará una publicación en Notimercio para dar a conocer los resultados de Human Firewall y continuar levantando conciencia en todo tipo de audiencia.

4.10 Objetivos:

Objetivo general:

Diseñar y ejecutar una campaña de Comunicación Interna para crear conciencia sobre la importancia de la Seguridad Informática y sus prácticas cotidianas en un periodo de 2 meses.

Objetivos específicos:

Charlas y Comunicación Interna:

1. Conseguir la apertura de al menos 3 organizaciones para ofrecer charlas de prevención de ataques de Ingeniería Social en un lapso de un mes.
2. Capacitar a por lo menos 2 departamentos por cada empresa en cómo prevenir ataques de Ingeniería Social en un tiempo de dos meses.
3. Reducir el número de víctimas de ataques de Ingeniería Social en los departamentos capacitados gracias a la campaña en las empresas en un tiempo de 2 meses.
4. Obtener una calificación de más de 70% de respuestas correctas en los cuestionarios de ciberseguridad de la campaña realizados al finalizar cada charla.
5. Capacitar a por lo menos 50 colaboradores en total en la identificación y prevención de Ingeniería Social y Phishing en un lapso de dos meses.
6. Lograr asesoría directa con al menos un experto en ciberseguridad para realizar la charla en un lapso de dos meses.

Medios de comunicación tradicionales

1. Generar noticia a través de la transmisión de contenido de valor para los medios de comunicación en un lapso de dos meses.
2. Aparecer o ser replicado por al menos 3 medios de comunicación sobre la campaña de comunicación interna en un lapso de dos meses.
3. Compartir el mensaje de prevención y conciencia sobre ciberseguridad para impactar una mayor cantidad de audiencias en un lapso de dos meses.

Estrategia Digital

1. Conseguir al menos 200 seguidores en la página de Instagram de la campaña en un lapso de dos meses.

2. Transmitir el mensaje de prevención digitalmente a través de la creación de publicaciones con contenido de valor sobre ciberataques en las redes sociales.
3. Generar al menos 3 conversaciones en redes sociales sobre experiencias de hacking que han tenido los usuarios y seguidores de la página de Instagram.

Evento

1. Lograr una asistencia de al menos 60 participantes en el evento Re-Conecta.
2. Transmitir prácticas de ciberseguridad a los asistentes del evento y realizar juegos interactivos para difundir el mensaje de prevención y desconfianza.
3. Generar conversaciones e interacciones con al menos 10 personas sobre ciberseguridad durante el evento.

4.11 Estrategias y tácticas:

Estrategia 1:

Estrategia: Enseñar y educar sobre la prevención de la Ingeniería Social en empresas y la ciudadanía.	
Táctica 1:	Ejecutar capacitaciones a los colaboradores de distintos departamentos susceptibles de las organizaciones aliadas.
Táctica 2:	Explicar qué es el Phishing y la Ingeniería Social, cómo identificarlos, qué son las prácticas ciberseguras y cómo llevarlas a cabo día a día.
Táctica 3:	Refuerzo de las charlas y generación de conciencia a través de contenido en redes sociales.
Táctica 4:	Acceso, por parte del equipo de Comunicación, a las charlas para futuras campañas.

Tabla 5: Estrategia 1

Estrategia 2:

Estrategia: Realización de cuestionario de preguntas sobre la charla a los colaboradores a través de Kahoot.	
Táctica 1:	Ejecutar Kahoot después de la charla.
Táctica 2:	Preguntar sobre algunos temas de la charla.
Táctica 3:	Poner casos prácticos: simulaciones de Phishing e Ingeniería Social donde los colaboradores deben identificar si los mensajes son ciertos o falsos.
Táctica 4:	Se refuerza lo enseñado en la charla.

Tabla 6: Estrategia 2

Estrategia 3:

Estrategia: Conseguir el apoyo de organizaciones para dictar las charlas y estructurar los contenidos técnicos de las mismas.	
Táctica 1:	Exponer la iniciativa de la campaña y por qué es pertinente realizarla.
Táctica 2:	Realizar alianzas estratégicas a través del ganar - ganar (la empresa refuerza su ciberseguridad, yo ejecuto mi trabajo de titulación).
Táctica 3:	Demostrar que se persiguen fines académicos y sociales cuya característica principal es prevenir delitos.
Táctica 4:	Analizar y verificar los contenidos de ciberseguridad de la charla con la ayuda de expertos en el tema facilitados por las organizaciones aliadas.

Tabla 7: Estrategia 3

Estrategia 4:

Estrategia: Comunicación externa a través de redes sociales.	
Táctica 1:	Compartir el conocimiento obtenido de ciberseguridad para todo público a través de las redes sociales.
Táctica 2:	Realizar contenido de valor para Instagram sobre consejos de ciberseguridad vinculados con los temas principales expuestos en las charlas.
Táctica 3:	Producir vídeos que apelen a los sentimientos de la audiencia para generar conciencia sobre la importancia de prácticas informáticas seguras y responsables e informar brevemente de qué se tratan.
Táctica 4:	Generar conversaciones con usuarios preguntando si han sido hackeados anteriormente, publicar esto en historias.

Tabla 8: Estrategia 4

Estrategia 5:

Estrategia: Comunicación externa a través de medios tradicionales.	
Táctica 1:	Empleo de los medios de comunicación para generar coyuntura y que el mensaje cobre aún más poder.
Táctica 2:	Aparecer en dos entrevistas de radio/televisión donde informe a la ciudadanía sobre prácticas de ciberseguridad y cómo operan los hackers.
Táctica 3:	Compartir un artículo redactado en un medio de comunicación donde se informe sobre las distintas prácticas de ciberseguridad.
Táctica 4:	Utilizar un vídeo informativo corto que pueda ser replicado por un medio en un corto periodo de tiempo.
Táctica 5:	Utilizar un vídeo informativo corto que pueda ser replicado por un medio en un corto periodo de tiempo.

Tabla 9: Estrategia 5

Estrategia 6:

Estrategia: Evento para generar conversaciones con todo tipo de personas e informarles directamente sobre las prácticas de ciberseguridad y los peligros del Phishing e Ingeniería Social.	
Táctica 1:	Alianza estratégica con otras campañas de comunicación para realizar el evento: A Un Clic de Conectar, Código 3, Lidera, Disruptivx.
Táctica 2:	Realización de alianza estratégica en el Centro Cultural Metropolitano para conseguir un espacio dónde realizar el evento.
Táctica 3:	Conformar stands con actividades interactivas para compartir con las audiencias sobre ciberseguridad.
Táctica 4:	Conseguir patrocinios de múltiples marcas para regalar premios y beneficios a los asistentes.
Táctica 5:	Generar interacciones, juegos y conversaciones en el stand de Human Firewall, donde se explique todo acerca de la comunicación destinada a la prevención de ciberataques.

Tabla 10: Estrategia 6

4.12 Planificación digital:

Dado que el objetivo digital de la campaña es transmitir los mensajes de prevención a través de contenido de valor sobre defensa de ciberataques, las publicaciones relacionadas a la campaña se enfocan en educar e informar los conocimientos transmitidos en las charlas a través de redes sociales. Además, otro de los propósitos de la presencia en los medios digitales es reforzar el material compartido en las capacitaciones. Así, se escogió a Instagram como la red social oficial de la campaña por los formatos existentes en esta plataforma para compartir el contenido. El tipo de publicación conocido como carrusel responde con precisión a la necesidad de compartir una serie de ilustraciones llamativas con información didáctica acerca de las prácticas de ciberseguridad y la prevención. Por ende, el contenido difundido en mayor cantidad se relaciona con consejos y explicaciones de prácticas simples, cotidianas y eficientes sobre seguridad informática. Estas publicaciones generan valor para los seguidores porque, a través de este conocimiento, se protegen y evitan ser vulnerados informáticamente. Por otro lado, la generación de material audiovisual que apele a las emociones y alerte a los usuarios también es sumamente importante. Entonces, se crearon vídeos en formato de reels donde se informa sobre cómo actúan los hackers, los errores que aprovechan y se ofreció una breve descripción sobre prácticas de prevención. Es muy importante presentar la información de esta manera para que los usuarios sean sepan sobre las amenazas informáticas a las que nos enfrentamos todos los días. También fue relevante presentar datos impactantes sobre cómo Ecuador es uno de los países más vulnerados de América Latina, esto en función de que los usuarios sepan el territorio de acción de la campaña. Usar Instagram como la red social de la campaña significó una estrategia para otorgar más material a los colaboradores capacitados de manera visual y didáctica; sin embargo, también es un medio por el cual se llegó a muchos más usuarios que encontraron el contenido interesante y útil para saber protegerse digitalmente.

4.13 Gráfica digital:

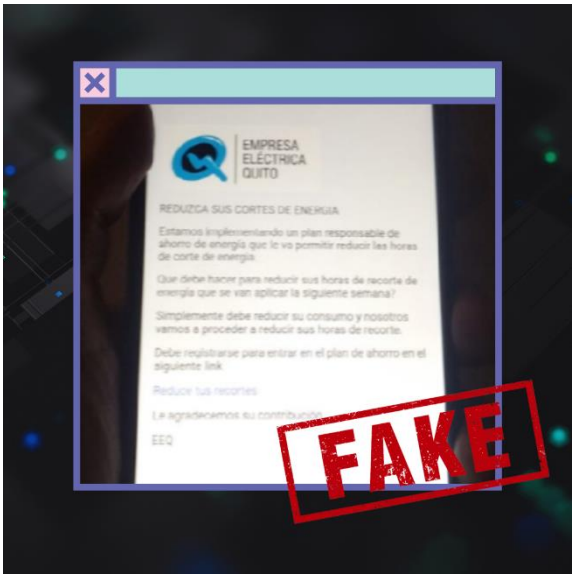

Figura 2: Post informativo

Figura 3: Post informativo

Figura 4: Post informativo

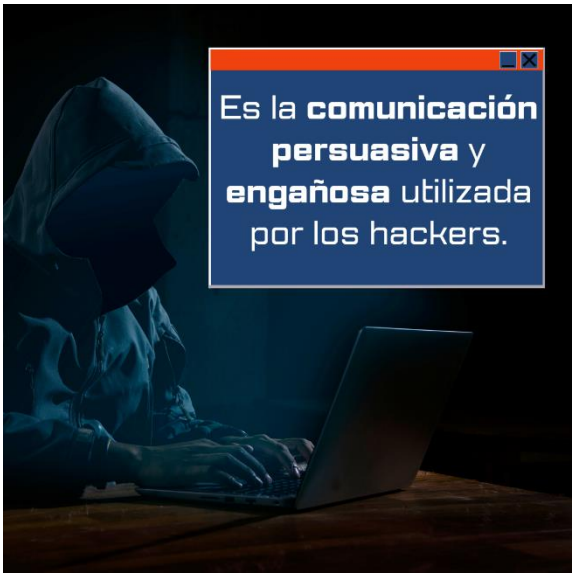

Figura 5: Post informativo

Figura 6: Post informativo

Figura 7: Post informativo

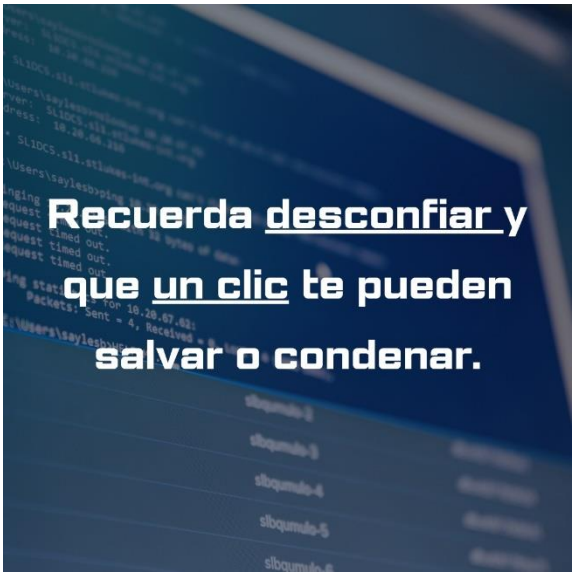

Figura 8: Post informativo

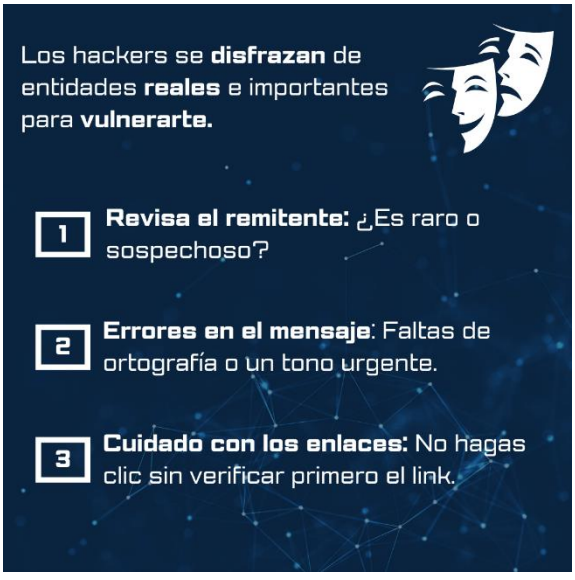

Figura 9: Post informativo

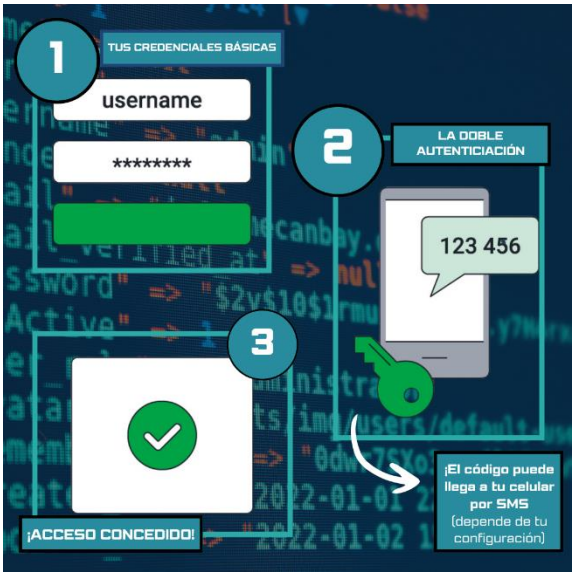

Figura 10: Post informativo

*Figura 11: Página de Instagram, @human.firewallec_*

Figura 12: Ejemplo de interacción con la comunidad en las historias

4.14 Ejecución de la campaña:

La campaña fue ejecutada en los meses de octubre hasta diciembre, debido a la trascendencia y la necesidad de compartir mensajes de ciberseguridad para todos los usuarios en épocas navideñas donde el movimiento económico es sumamente alto. La campaña fue difundida a través de más canales y medios para alcanzar a más personas. Se dividió en dos ejes, el de comunicación externa y el de interna. El primero se centraba en transmitir mensajes de prevención, cuidado y desconfianza para todo tipo de audiencia, además de inculcar prácticas de seguridad informática simples, cotidianas y poderosas para evitar vulneraciones. El segundo eje tiene que ver con la estrategia interna de realizar capacitaciones y entrenamientos de ciberseguridad a los colaboradores de múltiples departamentos en distintas organizaciones. Se ejecutó la estrategia de comunicación interna

de los talleres empresariales a funcionarios en la Universidad San Francisco de Quito, al Instituto Superior Tecnológico de Futbol Quito y Hotel GoQuito. Para la comunicación externa, se determinó a Radio La Mega, FM Mundo, Notimercio y Telesucesos como los medios por los cuales se difundiría la campaña y sus mensajes de prevención. Además de esto, se realizó un evento junto a más campañas llamado ReConecta, como se mencionó previamente, se montaron con éxito los stands de diferentes iniciativas de comunicación y una de estas fue Human Firewall. El propósito de esto fue interactuar con las personas, preguntarles sobre sus experiencias previas con vulneraciones informáticas y darles múltiples consejos de seguridad digital.

Ejecución y resultados de las charlas de Comunicación Interna:

En primer lugar, se realizaron reuniones virtuales y presenciales con los departamentos de comunicación, recursos humanos, tecnologías de la información y ciberseguridad de cada una de las organizaciones donde se realizarían las capacitaciones. El motivo de dichos encuentros fue para comentar y aprobar la iniciativa de Human Firewall en estas empresas, además, el equipo de Ciberseguridad y Tecnologías de la Información revisaron los contenidos de las capacitaciones y la aprobaron previamente. El siguiente paso fue la convocatoria, en cada una de las organizaciones con las que se trabajó y a través de los canales de comunicación interna, se llamaron a colaboradores de los departamentos de administración, adquisiciones, sistemas, contraloría, marketing, comunicación, recursos humanos, ventas, eventos, finanzas, etc. Las charlas fueron un éxito en cada empresa, abarcaron los temas de identificación y prevención de ataques de Ingeniería Social y Phishing, estructuración de contraseñas seguras, activación de autenticación de factores múltiples y prácticas simples de ciberseguridad para el día a día. El mensaje más poderoso que se buscó comunicar fue desconfiar en los entornos digitales y pensar dos veces antes de

hacer un clic. Después de cada capacitación, para verificar la comprensión, se realizó un juego interactivo a modo de cuestionario en la plataforma Kahoot. En esta serie de preguntas mostraban ejemplos de ciberataques de Ingeniería Social y mensajes reales por parte de entidades verificadas, se les pedía a los funcionarios asistentes que diferencien entre los casos reales y falsos. Los resultados fueron extremadamente positivos, se capacitaron a más de 2 departamentos de 3 organizaciones, además, las charlas se dirigieron a más de 50 colaboradores en total. Asimismo, se obtuvo una calificación de 80% de respuestas correctas por parte de los funcionarios en los cuestionarios de ciberseguridad, por lo cual, se entendió el mensaje principal de las charlas y esto conlleva a una reducción de víctimas de ciberataques de Ingeniería Social en las organizaciones con las que se trabajó.

Fotografía 1: Realización de una charla en la USFQ

Estrategia Digital:

La estrategia digital consistió en reforzar los conocimientos transmitidos en las capacitaciones a través de la publicación de contenido de valor educativo en Instagram. Así, los beneficiarios de las charlas pueden acceder a la red social y volver a revisar la información ya expuesta en la capacitación. Sin embargo, el tema trascendió y por lo tanto el

alcance de las audiencias. Dado que el contenido compartido es útil para todo tipo de usuarios, la página de Instagram consiguió más de 200 seguidores y se alcanzó a múltiples cuentas, incluso de otros países. Además, se generaron más de 3 conversaciones con usuarios donde revelaron sus experiencias con vulneraciones informáticas debido a la Ingeniería Social. Por otra parte, el contenido audiovisual compartido provoca sensaciones de alerta y prevención, entonces, los usuarios están más alertas debido a lo publicado en la campaña.

Medios de comunicación:

La gestión de medios de comunicación tenía como iniciativa compartir más contenido de valor sobre la campaña para todas las audiencias, no solo el sector corporativo. En primer lugar, los temas de ciberseguridad ya son ampliamente cubiertos por los medios y mucho más en épocas de Navidad y Fin de Año caracterizadas por el aumento del movimiento económico. Así, se buscó generar noticia a través de la información a los usuarios sobre prácticas de ciberseguridad cotidianas para que se eviten pirateos y estafas. Estos son temas que generan noticias de valor para los medios de comunicación porque se está informando y protegiendo de delitos a las audiencias. Como resultados, se consiguió un espacio de dos minutos en la emisión estelar de las 7:00 pm en Notimundo (noticiero estelar) del medio FM Mundo donde se compartían consejos de ciberseguridad. De igual forma, Human Firewall apareció en La Mega a las 9:00 am en una conversación con Pato Borja durante 60 minutos en la cual se habló sobre la ejecución de la campaña y cómo un clic responsable puede salvar o condenar al usuario. En Telesucesos, se logró un espacio de 6 minutos en el programa En Familia donde se realizó una entrevista sobre consejos de seguridad informática. En el periódico, Notimercio, Human Firewall apareció en una publicación en la sección de empresas donde se informó cómo la campaña busca proteger a los usuarios de ciberataques. Por ende, se consiguió transmitir el mensaje de la campaña a todo tipo de públicos y sembrar

las primeras raíces de una cultura de seguridad informática impulsada por la comunicación estratégica.

Imagen 2: Aparición en Telesucesos, programa "En Familia"

Evento:

La campaña se coordinó con otras iniciativas para llevar a cabo un evento llamado ReConecta. En este proyecto, se buscaba generar interacciones con todo tipo de públicos e informarles sobre las acciones de comunicación de cada una de las campañas a través de stands informativos dinámicos. Human Firewall estuvo presente con juegos de identificación de Phishing e Ingeniería Social y premios para todos quienes se acerquen al stand de la campaña. Se consiguió un total de 9 patrocinadores que apoyaron al evento con agua, energizantes, flores, etc. El propósito fue generar conversaciones con cada asistente e informarles sobre pautas de ciberseguridad que evitarán que sean vulnerados a corto y largo plazo. La acogida del evento fue muy satisfactoria, asistieron más de 60 personas y se logró interactuar con todos los participantes, con esto, el mensaje de la campaña se transmitió ampliamente a niños, adultos mayores y a todo tipo de audiencia.

Imagen 3: Interacción con participantes durante el evento

CONCLUSIONES:

Luego de conocer los aspectos técnicos generales de la seguridad informática, su importancia, prácticas, conceptos, tipos de amenazas y funcionalidades; para concluir, la comunicación es una herramienta fundamental que puede ser empleada para potenciar cualquier área del conocimiento. En este caso, es utilizada con el propósito de poner un parche a un desperfecto que es difícil de corregir técnicamente. Así como la ingeniería social recurre a la comunicación persuasiva para producir errores en los usuarios y abrir puertas para los ciberdelincuentes, la comunicación estratégica para todo tipo de entornos, especialmente internos, puede contrarrestar esta metodología. En el Ecuador, los ataques informáticos son cada vez más recurrentes, y al mismo tiempo, la necesidad de que los colaboradores se encuentren más informados respecto a las buenas prácticas de ciberseguridad crece. Por lo tanto, la comunicación construye una capa de protección muy importante en las organizaciones que no necesariamente se compone de software o hardware, sino de la capacidad de los usuarios para identificar y evadir las amenazas que atentan contra la integridad de la empresa.

El fortalecimiento de las prácticas de seguridad informática dentro de la cultura corporativa supone proliferar los esfuerzos en fortalecer los sentidos compartidos de los miembros de la entidad organizacional, esto es un enfoque enriquecedor que consiste en múltiples prácticas facilitadas por una correcta gestión de comunicación coordinada con otros departamentos. Entonces, se plantea la realización de una campaña de comunicación cuyos mensajes se esfuerzan para solidificar las rutinas y acciones aceptables a favor de la integridad digital de una entidad. Se destacan aquellas iniciativas de la campaña en las que se capacita al personal en cuanto a levantar su conciencia respecto a responsables y conocimientos para diferenciar un malware o intento de ataque de otro. Se deben compartir comunicados constantemente y de diferentes tipos para reforzar los aprendizajes inculcados. También es

ampliamente necesario pensar medidas de protección digital que regulen el comportamiento de los empleados, estas son políticas que detallan claramente los límites y responsabilidades de los funcionarios. Al mismo tiempo, es inminente facilitar canales de interacción que acompañen a las disposiciones de ciberseguridad y que permitan la reacción adecuada a los expertos con técnicos de este tema. Adicionalmente, la creación de un manual de protocolo para que el trabajador tenga una guía auténtica por escrito es de suma importancia, esto apoyará y moldeará la manera en la que el colaborador reacciona ante una vulneración a los sistemas; así, actuará correctamente tanto de manera interna junto a sus compañeros en el entorno de trabajo, como externa porque ofrece una respuesta pertinente a los clientes o stakeholders de afuera. Los medios a través de los cuales se puede difundir esta campaña de comunicación interna tienen la posibilidad de ser creativos, siempre y cuando sean pertinentes con la propia empresa. Uno de los mencionados en este trabajo alude a la gamificación, donde mediante juegos interactivos y dinámicos, se enseña y se refuerzan la propagación de las buenas costumbres y protocolos responsables de seguridad informática.

La comunicación en crisis es otra de las funcionalidades que actúa como defensa de la reputación de la empresa por si alguna amenaza informática atraviesa la barrera establecida anteriormente. Esta constituye una serie de procedimientos que gestionan una crisis, tanto en el ámbito interior de la organización, como en el exterior. El manual concebido en por la estrategia de comunicación interna también tiene que contar con secciones de administración de problemas para solventar las diferentes eventualidades que acompañan a un ataque informático. Cabe destacar que un plan de comunicación en crisis exitoso viene desde la ejecución de una excelente transmisión interna y de las buenas prácticas de los colaboradores. Esto permite que los empleados sean un soporte fuerte que facilita la resiliencia ante las eventualidades graves que puede experimentar una organización.

Por otra parte, después de ejecutar la campaña en múltiples organizaciones, se concluye que el aprendizaje de conceptos y acciones de seguridad informática sí se producen eficientemente a través de las estrategias de comunicación interna. Particularmente, las capacitaciones para los funcionarios son herramientas claves para transmitir mensajes poderosos y crear acciones de prevención que favorezcan una cultura de protección cibernética. Este último concepto debe trascender, no solo dentro de las empresas, también en las prácticas cotidianas de cada uno de los usuarios y a su vez, la protección informática tiene que ser comunicada a todo tipo de audiencias porque nadie está exento de sufrir una vulneración grave. También, es importante aprovechar y utilizar estratégicamente cada canal de comunicación para transmitir la información, por ejemplo, si se recurren a las redes sociales, los mensajes compartidos deben ser valiosos, útiles y concisos para atraer a la audiencia mientras que se comparte información de utilidad. Los temas de ciberseguridad pueden ser vistos como conocimientos muy complejos como para ser comprendidos; por ende, es importante presentar los comunicados educativos de maneras simples y asimilables para los usuarios. Se aprendió que la labor del comunicador, al efectuar este tipo de campañas, es de ayudar a las audiencias y demostrarles su papel en la ciberseguridad. Es muy importante indicar que el público no está alejado de este tópico como se piensa y que cada usuario tiene el poder de repeler un ciberataque siempre que esté prevenido y reflexione antes de hacer un clic o entregar su información confidencial de alguna manera. Adicionalmente, al efectuar un trabajo correcto y eficiente de comunicación interna, el tema trasciende externamente y por lo tanto los receptores aumentan. Así, los medios informativos tradicionales retransmitirán las acciones efectuadas en las organizaciones y las adaptarán a contenidos instructivos para los espectadores, lectores y oyentes. Human Firewall es uno de los primeros trabajos que plasman académicamente el uso de la comunicación y sus herramientas para generar culturas de ciberseguridad, por ende, todavía hay múltiples acciones creativas que se pueden utilizar e implementar para corregir

errores humanos a través de la conciencia. La naturaleza de este trabajo también corresponde a una invitación para seguir trabajando por la protección de los usuarios y prevención de ciberdelitos a través de un instrumento tan poderoso como lo es la comunicación.

REFERENCIAS BIBLIOGRÁFICAS

¿Qué es el cifrado de datos? Definición y explicación. (2023, 13 diciembre). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/encryption

Aldawood, H., & Skinner, G. (2018). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. School Of Electrical Engineering And Computing, 11(3). https://www.mdpi.com/1999-5903/11/3/73

Álvarez, J. (2023). INGENIERÍA SOCIAL: TÉCNICAS UTILIZADAS POR LOS CIBERDELINCUENTES Y CÓMO PROTEGERSE. UNIVERSIDAD TÉCNICA DE BABAHOYO. http://dspace.utb.edu.ec/bitstream/handle/49000/13062/E-UTB-FAFI-SIST-000396.pdf?sequence=1&isAllowed=y

Arango, O. (2023). EL ABC DE LA SEGURIDAD INFORMATICA, GUIA PRACTICA PARA ENTENDER LA SEG (1.a ed., Vol. 1). Edición del autor. https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5901/El%20ABC%20de%20la%20seguridad%20inform%c3%a1tica%20gu%c3%ada%20pr%c3%a1ctica%20para%20entender%20la%20seguridad%20digital.pdf?sequence=4&isAllowed=y

Arévalo, F., Ordoñez, I., Peñaherrera, M., & Suárez, V. (2019). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. Dominio de las Ciencias, 6(2), 835-846. https://dominiodelasciencias.com/ojs/index.php/es/article/view/1197/1898

Avilés, M. (2021, 4 agosto). La situación actual de la CNT es “crítica y seria” www.expreso.ec. https://www.expreso.ec/actualidad/situacion-actual-cnt-critica-seria-

109428.html#:~:text=El%20ataque%20afect%C3%B3%20varios%20servicios,realizar%20pagos%20o%20presentar%20reclamos.

Benavidez, E. (2019*). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura.* Ciencias Informáticas UTEQ.

Benavidez, E., Fuertes, W., & Sánchez, S. (2019). Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social [Artículo científico, Universidad de las Fuerzas Armadas ESPE]. https://www.redalyc.org/journal/5826/582661898003/

Bogantes, A. (2019). El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados [Universidad Estatal a Distancia San José]. https://www.iiisci.org/journal/PDV/risci/pdfs/CB294NT20.pdf

Brandolini, A., & Frígoli, M. (2009). Comunicación interna. Claves Para una Gestión Exitosa. https://sedici.unlp.edu.ar/handle/10915/69725

Campoverde, L. (2021). UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN [Proyecto de titulación, Universidad Estatal Península de Santa Elena]. https://repositorio.upse.edu.ec/bitstream/46000/7726/1/UPSE-TTI-2022-0009.pdf

Cañizares, E. (2023, 21 septiembre). Ecuador es uno de los tres países latinoamericanos con más ciberataques. Ecuador | Noticias | el Universo. https://www.eluniverso.com/noticias/ecuador/ecuador-es-uno-de-los-tres-paises-latinoamericanos-con-mas-ciberataques-nota/

Cañizares, E. (2023, 21 septiembre*). Ecuador es uno de los tres países latinoamericanos con más ciberataques*. Ecuador | Noticias | El Universo.

https://www.eluniverso.com/noticias/ecuador/ecuador-es-uno-de-los-tres-paises-latinoamericanos-con-mas-ciberataques-nota/

Capriotti, P. (1998). LA COMUNICACIÓN INTERNA. Capacitación y Desarrollo, 13, 5-7.

Castro, P. (2023). *Latinoamérica es blanco de ciberataques*. https://radiomegaestacion.com/latinoamerica-es-blanco-de-ciberataques/mundo/

Corallo, A., Lazoi, M., & Lezzi, M. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers In Industry, 137. https://www.sciencedirect.com/science/article/abs/pii/S0166361522000094?casa_token=7LJbhfENQyAAAAAA:A387gIeGSlfjq0KsbfwWMHjbl_BaqBXXux3grTbtko_V6rGeTawlZFGsZqK9A76LBlbIe182Lcs

Cuenca, J., & Verazzi, L. (2020). Guía Fundamental de la Comunicación Interna (3.a ed.). Editorial UOC. https://books.google.es/books?hl=es&lr=&id=mxSzDwAAQBAJ&oi=fnd&pg=PT4&dq=comunicacion+interna&ots=eQ2toGcZfd&sig=UzSoEg6qKBR28_YHrJdimMH5NvQ#v=onepage&q&f=false

Chavez, J. J. S. (2024, 23 enero). Seguridad de la red: ¿Qué es, cómo funciona y qué tipos existen? https://www.deltaprotect.com/blog/seguridad-de-la-red

Da Silva, D. (2021, 16 septiembre). Canales de comunicación interna: tipos y 3 tips para elegir. Zendesk. https://www.zendesk.com.mx/blog/canales-de-comunicacion-interna/

Dávalos. (2021, 30 julio). Los misterios del ataque que dejó a CNT sumida en la «emergencia». Primicias. https://www.primicias.ec/noticias/tecnologia/los-misterios-del-ataque-que-dejo-a-cnt-sumida-en-emergencia/#:~:text=Se%20sabe%20que%20se%20trat%C3%B3,contra%20los%20sistemas%20de%20CNT.

De La Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers And Security, 92, Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S0167404820300018?casa_token=9WxLZ2qMAcUAAAAA:M-qUwfc6CM77QGFMdQtRBvdGAfCTiJxsNizMCCNxyy2iWEDymYOqLOmy5iGsb7SUHKvcJwRGGc8#sec0004

Diaz, V. (2021). Banco Pichincha confirma «incidente de ciberseguridad» en sus sistemas. El Comercio. https://www.elcomercio.com/actualidad/negocios/banco-pichincha-ciberseguridad-ciberataque-hackeo.html

Ecuador en Vivo. (2025). *Ecuador entra en el top tres de países con más ataques cibernéticos*. https://www.ecuadorenvivo.com/index.php/economia/item/167236-ecuador-entra-en-el-top-tres-de-paises-con-mas-ataques-ciberneticos

Ecuavisa. (2024, 28 enero). Ecuador bajo ataque: Los ciberataques son la principal causa de interrupción de las actividades empresariales. www.ecuavisa.com. https://www.ecuavisa.com/noticias/seguridad/ciberataques-principal-causa-interrupcion-actividades-empresariales-XF6711536

Egas, E., & Yance, K. (2018). Estrategias de comunicación interna para fortalecer la identidad corporativa de una empresa de seguridad ubicada en la ciudad de Guayaquil - Ecuador. Revista Espacios, 39(24), 20. https://ww.revistaespacios.com/a18v39n24/a18v39n24p20.pdf

El Comercio. (2021). Banco Pichincha advierte de correos fraudulentos que buscan obtener información para realizar «transacciones ilegítimas». https://www.elcomercio.com/actualidad/negocios/banco-pichincha-correos-transacciones-ilegitimas.html

El Universo. (2024, 23 febrero). Movistar Empresas impulsa la ciberseguridad en Ecuador. Doctor Tecno | la Revista | el Universo. https://www.eluniverso.com/patrocinado/movistar-empresas-impulsa-la-ciberseguridad-en-ecuador/

Enriquez, M. (2019). Gestión y prevención de crisis. Un enfoque desde la estrategia global de la empresa. Colección de Comunicación Estratégica 2019, 23-28.

Fábregas, J., & Tejedor, S. (2021). La gamificación como recurso telemático en la comunicación empresarial en tiempos de pandemia. Comunicación, 44. https://openurl.ebsco.com/EPDB%3Agcd%3A7%3A2205367/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A150423073&crl=c

Fárfan, C. (2022, 5 julio). Caso de éxito | Concientización en Seguridad de la Información en el sector educativo. Nuvol Cybersecurity. https://www.cybernuvol.com/post/concientizaci%C3%B3n-en-seguridad-de-la-informaci%C3%B3n-en-el-sector-educativo

Fernández, A., Puentes, I., & Vázquez, M. (2016). Las empresas gallegas más contaminantes y su gestión de la comunicación de crisis. Casos de Estudio de Relaciones Públicas: Espacios de Diálogo E Impacto Mediático, 33-57.

Garzón, C., Navas, C., Illiacachi, A., Espinoza, R., & Estrella, G. (2024). Análisis de los Ataques de Ingeniería Social en Ecuador. Ciencia Latina Internacional, 8(1). https://ciencialatina.org/index.php/cienciala/article/view/9777/14420

González, A. (2023, 29 marzo). Ransomware representa 60% de ciberataques en América Latina | DPL News. DPL News. https://dplnews.com/ransomware-representa-60-de-ciberataques-en-america-latina/

González, G. (2013, 26 octubre). Buffer hackeada, Twitter y Facebook se inundan de spam. Hipertextual. https://hipertextual.com/2013/10/buffer-hackeada

Guaña, J., Sánchez, A., Chérrez, P., Chulde, L., Jaramillo, P., & Pillajo, C. (2019). Ataques informáticos más comunes en el mundo digitalizado. Risti. https://dspace.itsjapon.edu.ec/jspui/bitstream/123456789/3445/1/ATAQUES%20INFORMATICOS.pdf

Hadnagy, C. (2011). Ingeniería social: El Arte del Hacking Personal.

Hernández, S. (2019). CULTURA EN SEGURIDAD DE LA INFORMACIÓN [Especialización en Seguridad Informática, Universidad Piloto de Colombia]. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6436/Art%C3%ADculo_Cultura_Seguridad_de_la_Informaci%C3%B3n.pdf?sequence=1&isAllowed=y

Hueca, A., Manley, B., & Rogers, L. (2020). Building a Cybersecurity Awareness Program [Tesis, Universidad Carnegie Mellon]. https://apps.dtic.mil/sti/pdfs/AD1112780.pdf

Ibarra, M. (2018). DELITOS INFORMÁTICOS ASOCIADOS A LA INGENIERÍA SOCIAL EN COLOMBIA Y LATINOAMÉRICA. *UNIVERSIDAD NACIONAL ABIERTA y A DISTANCIA ESCUELA DE CIENCIAS BASICAS E INGENIERIA ESPECIALIZACION EN SEGURIDAD INFORMATICA*. https://repository.unad.edu.co/bitstream/handle/10596/27420/%20%09myibarrai.pdf?sequence=1&isAllowed=y

Islas, O., & Hernández, G. (2012). Investigando la comunicación en crisis. Razón y Palabra, 1, 3-6.

Jaimovich, D. (2023, 23 noviembre). Los 14 tipos de ciberataques más comunes (y cómo prevenirlos). Los 14 tipos de ciberataques más comunes (y cómo prevenirlos). https://blog.invgate.com/es/tipos-de-ciberataque

Jove, E., Calvo, J., Urda, D., Herrero, A., Zurutaza, U., & Casola, V. (2023). Avances recientes en la aplicación de la ciencia de datos a la ciberseguridad industrial. *Tecnología de Telecomunicaciones, 1*.

https://gicap.ubu.es/publications/2021/PDF/2021_c01_Recent%20advances%20in%20the%20application%20of%20data%20science%20to%20industrial%20cybersecurity.pdf

Kolesnikov, N. (2024). 50 Estadísticas Clave de Ciberseguridad para Marzo de 2024. Technopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Leite, P., Da Silva, S., & De Souza, E. (2025). KnowBe4 platform for information security in a financial institution: a case study. REVISTA OBSERVATORIO DE LA ECONOMIA LATINOAMERICANA, 21(12). https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/view/2199/1720

López, C., & Salvador, R. (2015). Ingeniería Social: El Ataque Silencioso. REVISTA TECNOLÓGICA, 8, 39. http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

Mackay, J. (2023). Desvelando el lado oscuro: cómo la IA permite sofisticados ataques de phishing. MetaBlog. https://www.metacompliance.com/es/blog/phishing-and-ransomware/how-ai-enables-sophisticated-phishing-attacks

Machado, J. (2022, 18 abril). El 15% de la información del Municipio de Quito fue hackeada. Primicias. https://www.primicias.ec/noticias/sociedad/municipio-quito-informacion-hackeada/

Marín, F. (2009). Comunicación en Crisis. Editorial Almuzara. https://books.google.com.ec/books/about/Comunicaci%C3%B3n_de_crisis.html?id=cdsDEAAAQBAJ&redir_esc=y

Marquez, M. (2023). Gamificación en la construcción de la marca interna - Playmotiv. Playmotiv - Gamificación Para Empresas. https://playmotiv.com/gamificacion-en-la-construccion-de-la-marca-interna/

Mieres, J. (2009). Ataques informáticos: Debilidades de seguridad comúnmente explotadas. EvilFinger, 1. https://www.evilfingers.org/publications/white_AR/01_Ataques_informaticos.pdf

Ministerio de Telecomunicaciones y Sociedad de la Transformación. (2022). *Estrategia Nacional de Ciberseguridad* (1.ª ed.). https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Molina, Y., & Orozco, L. (2019). Vulnerabilidades de los Sistemas de Información: una revisión Information System Vulnerabilities: A review. Dspace. https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1&isAllowed=y

Moya, J., Sánchez, A., Chérrez, P., Chulde, L., Jaramillo, P., & Pillajo, C. (2022, 16 agosto). Ataques informáticos más comunes en el mundo digitalizado - ProQuest. ProQuest. https://www.proquest.com/openview/02492b51bc001f7bf3254a198698d1d7/1?pq-origsite=gscholar&cbl=1006393

Organización Internacional de Normalización. (2022). Seguridad de la información, ciberseguridad y protección de la vidaprivada — Sistemas de gestión de la seguridad de la información —Exigencias. Comunicación (Norma Núm. 7.4), uie. https://es.scribd.com/document/616176936/ISO-27001-2022-espanol

Orihuela, A. (2022). Programa de Seguridad de Información Ante Ciber Ataques de Ingeniería Social para Empleados de una Compañía de Telecomunicaciones de Lima. Pontificia Universidad Catolica del Peru. https://www.proquest.com/openview/b6efaf03caeef16dc907cbff528e4df6/1?pq-origsite=gscholar&cbl=2026366&diss=y

Parra, R. (2021, 22 julio). Corporación de Telecomunicaciones de Ecuador sufrió un ataque cibernético | DPL News. DPL News. https://dplnews.com/corporacion-de-telecomunicaciones-de-ecuador-sufrio-un-ataque-cibernetico/

Pesantes, K. (2023, 18 octubre). Ciberataques: ¿cuánto le cuesta a las empresas el robo de datos? *Primicias*. https://www.primicias.ec/noticias/tecnologia/ciberataques-costo-robo-datos-empresas/

Piñeiro, J. L., & Wong, L. (2022). Web architecture for URL-based phishing detection based on Random Forest, Classification Trees, and Support Vector Machine. Inteligencia Artificial, 25(69), 107-121. https://doi.org/10.4114/intartif.vol25iss69pp107-121

Postigo, A. (2020). Seguridad informática (1.a ed.). Parainfo. https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=seguridad+informatica&ots=-IVWhkaRj3&sig=KCdmGEAeyLY0_jNpM7tKaHMWFS0#v=onepage&q=seguridad%20informatica&f=false

Ramírez, M. (2018). EL CONCEPTO DE CIBERSEGURIDAD EN EL ÁMBITO ORGANIZACIONAL. *43estudiante*. https://xxencuentro.aeca.es/wp-content/uploads/2022/09/43estudiante.pdf

Robbins, S., & Judge, T. (2017). Comportamiento Organizacional. Pearson.

Romero, D. (2019). *EL ARTE DE LA INGENIERÍA SOCIAL*. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6354/El%20arte%20de%20la%20ingenier%c3%ada%20social.pdf?sequence=1&isAllowed=y

Samson, E., & Bayas, K. (2023). Seguridad Digital: ¿Realmente sabes cómo protegerte? Enfoque, 97. https://www.usfq.edu.ec/sites/default/files/2023-08/enfoque-97-junio-2023.pdf

Sandoval, C. (2023). *Ciberdelincuentes lanzan ataques informáticos con falsas fotomultas de tránsito en Ecuador*. El Comercio. https://www.elcomercio.com/tendencias/ciberdelincuentes-ataques-falsas-fotomultas-ecuador.html

Serrano, D., & Diaz, V. (2021). Virus RansomEXX es el responsable del ciberataque a CNT. https://www.elcomercio.com/actualidad/negocios/virus-ransomeware-cnt-ministerio-telecomunicaciones.html

Silva, H. (2013, 27 octubre). Buffer hackeado. Revisen sus cuentas. - ilmaistro.com. ilmaistro.com. https://ilmaistro.com/buffer-hackeado-revisen-sus-cuentas/

Sulay, L., Cruzado, C., Mejía, C., & Alarcón, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana [Monografía, Universidad San Ignacio de Loyola]. http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

Swissinfo. (2022, 18 abril). El Municipio de Quito, víctima de ciberataque que afectó el 15 % de sus datos. SWI Swissinfo. https://www.swissinfo.ch/spa/el-municipio-de-quito-v%C3%ADctima-de-ciberataque-que-afect%C3%B3-el-15-de-sus-datos/47525602

Secureframe. (2023). Más de 60 estadísticas de ingeniería social para 2023. *Secureframe*. https://secureframe.com/es-es/blog/social-engineering-statistics

Team, K. (2023, 23 agosto). Nueva epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el. Kaspersky. https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/#:~:text=Entre%20los%20pa%C3%ADses%20m%C3%A1s%20afectados,(9%2C4%20millones).

Vaccaro, R. (2023). Introducción a la Ciberseguridad a Través de Amenazas Cibernéticas. *PRCR*. https://prcrepository.org/handle/20.500.12475/1941

Yaguache, J. (2019). La práctica de la reacción y no de la prevención. Colección de Comunicación Estratégica 2019, 16-22.

Yanulis, B. (2023, 6 abril). *Noticias de ciberseguridad América Latina 2023 - GlobalSign*. GlobalSign. https://www.globalsign.com/es/blog/es-blog-noticias-ciberseguridad-en-america-latina-abril