PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

Programa de seguridad de información ante ciber ataques de ingeniería social para empleados de una compañía de telecomunicaciones de Lima

Tesis para obtener el grado académico de Magíster en Integración e Innovación Educativa de las Tecnologías de la Información y la Comunicación que presenta:

Axel Igor Orihuela Quivaqui

Asesor:
Carol Rivero Panaqué

Lima, 2022

RESUMEN

Las amenazas informáticas son cada vez más sofisticadas y a la vez es normal que la formación en seguridad de información de los empleados de una empresa no sea suficiente para lograr y mantener un nivel de consciencia y de buenas prácticas que les ayude a evitar ser víctimas de ciber ataques involuntariamente.

Ante esta situación, se plantea esta propuesta de innovación educativa que se centra en el problema de la limitada consciencia en seguridad de información de los empleados de una empresa de telecomunicaciones de Lima, para enfrentar ciber ataques de ingeniería social, que les hace tomar acciones incorrectas y riesgosas en sus interacciones sobre internet.

Esta propuesta implica la incorporación de un programa en ciber seguridad centrado en las personas, que sea atractivo, efectivo y que logre que los empleados comprendan la importancia del rol que tienen en la protección de la información, ya sea personal o de la organización. Este programa considera un enfoque de formación que motive a los empleados mediante un aprendizaje inmersivo basado en gamificación, pero también busca sensibilizarlos sobre la importancia y criticidad de la ciber seguridad mediante la inclusión de experiencias y vivencias reales, así como impactos y daños personales y empresariales debido a ciber ataques. Por lo tanto, con este programa de formación y concientización se busca desarrollar una cultura saludable con pensamiento crítico y racional frente a la ciber seguridad, preparando de una mejor manera a los empleados para que reconozcan amenazas e intentos de ataques, y reaccionen correctamente.

Como resultados de la experiencia piloto se confirmó que los empleados se preocupan por las amenazas existentes en su interacción en internet y que tienen conocimientos generales de los riesgos, pero no necesariamente aplican buenas prácticas en seguridad de información, además que cada vez les es más difícil identificar las ciber amenazas, por lo que es importante implementar un proceso de enseñanza innovador en ciber seguridad.

Dedicatoria y Agradecimientos

A Dios por sus bendiciones.

A mi esposa Marcia y mis hijos André y Adam, por su amor e inspiración.

A mis padres y hermanos, por su impulso y apoyo incondicional.

A mi suegro Pepe por sus consejos y ánimos.

Además, un reconocimiento especial a mi asesora Carol por su guía y motivación.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El auge de la tecnología ha transformado al mundo radicalmente, lo cual se refleja en la influencia que tiene sobre la mentalidad, la conciencia y el desarrollo de la sociedad en la vida diaria (Pashentsev et al., 2019). En ese sentido, Isachenko (2018) explica que el uso activo de la tecnología es un medio que ejerce un efecto directo en la mente de las personas, generando una dependencia como la necesidad que tiene la gente de consultar constantemente los dispositivos digitales sin importar el tiempo o lugar.

La ciencia y la tecnología son elementos esenciales en la sociedad moderna, ya que simplifican la vida diaria y trascienden a la vida de todos (Sociology Guide, 2020). Sin embargo, por más que la tecnología facilita muchas cosas como el ser más productivo y acceder a una gran cantidad de información, también tiene inconvenientes que no se pueden ignorar. Por lo tanto, hay que considerar que el crecimiento de riesgos en ciber seguridad se ve favorecido por distintos aspectos como la interconexión de los sistemas informáticos, la integración y comunicación entre dispositivos y equipos electrónicos, la participación y atracción de las personas en las redes sociales, entre otros.

Así también, según la publicación *The 2020 Cyber Security Report*, las vulnerabilidades y los errores en seguridad de información son "más sofisticados, ilusorios y selectivos que nunca" (Check Point Research, 2020, pág. 5). Además, se precisa que los ciber ataques cada vez son más eficaces y atraen a usuarios desprevenidos convirtiéndolos en sus víctimas. En ese sentido Albladi y Weir (2018) muestran su preocupación por el incremento de ciber ataques de ingeniería social, en los cuales se pone en la mira a las personas como punto de acceso fácil de manipulación. Ambos autores plantean la importancia de comprender los factores que influyen en las competencias, conciencias y acciones de las personas ante un ciber ataque, y resaltan la necesidad de realizar investigaciones exhaustivas sobre ingeniería social, sus riesgos e impactos; además, proponen modelos y estrategias que permitan mejorar la conciencia y acción positiva en la detección de ciber amenazas.

Tomando en cuenta lo mencionado anteriormente, los ciber ataques y la ingeniería social desafían el nivel de consciencia sobre seguridad de información de los empleados, ya que los ciber delincuentes perfeccionan sus técnicas de manipulación aprovechando las vulnerabilidades del ser humano como la baja percepción del riesgo, el exceso de autoconfianza y la práctica de hábitos riesgosos. Por lo tanto, es necesario desarrollar y mantener un nivel de consciencia en seguridad de información que les permita adecuar su comportamiento ante las ciber amenazas.

La presente propuesta de innovación educativa nace con el fin de aportar un enfoque mejorado en la formación de la consciencia en ciber seguridad, centrado en los empleados de una empresa de telecomunicaciones de Lima, para que puedan enfrentar ciber ataques de ingeniería social, y evitar acciones incorrectas y riesgosas en sus interacciones sobre internet.

En ese sentido, se plantea un programa de capacitación en seguridad de la información eficaz, que permita incorporar una cultura de pertenencia y cumplimiento de seguridad de información en la organización, y que aporte un alto nivel de concientización y responsabilidad sobre la seguridad. Así también, se incluye un enfoque de formación basado en gamificación con un escenario de aprendizaje inmersivo de "sala de escape" (*escape room*), en la que los participantes deben resolver situaciones relacionadas con ciber seguridad para avanzar a la siguiente sala o nivel, lo cual aumenta la motivación y mejora el aprendizaje.

En el primer capítulo, del presente documento, se expone el diseño de la propuesta de innovación educativa, el cual incluye información general y datos de la intervención, su justificación y antecedentes, la fundamentación teórica, los objetivos y las metas. Asimismo, se expone la estrategia y actividades, los recursos y presupuesto necesarios, así como la sostenibilidad y cronograma.

En el segundo capítulo se presenta el informe de la experiencia piloto dirigida a la formación en ciber seguridad de un grupo de empleados. En este capítulo se profundiza sobre el desarrollo del piloto, el cual incluye información sobre su estrategia operativa, sus objetivos y metas, su cronograma y las cinco etapas del proceso de ejecución, detallando los resultados y conclusiones del piloto.

El documento finaliza con una exposición de conclusiones y recomendaciones a ser consideradas en la aplicación de esta propuesta de innovación.

CAPÍTULO I. DISEÑO DE LA PROPUESTA DE INNOVACIÓN

1. Información general de la Propuesta de Innovación

1.1 Título de la propuesta

Programa de Seguridad de Información ante ciber ataques de Ingeniería Social para empleados de una compañía de telecomunicaciones de Lima

1.2 Datos de la institución

La presente propuesta se realizará en una corporación privada de tecnología y telecomunicaciones, que tiene operaciones en Chile y Perú, y que actualmente cuenta con más de 18,2 millones de clientes de servicios de telecomunicaciones móviles (ENTEL, 2020). Brinda servicios de telefonía móvil y operaciones de redes fijas integradas de datos, voz, e internet para los segmentos de personas, empresas, corporaciones y mayoristas. Por lo tanto, debe asegurar la conectividad con internet y garantizar alta disponibilidad de las comunicaciones.

Nombre: Empresa de telecomunicaciones
Ubicación: Av. Paseo de la República 3490, Lima Perú
Público al que atiende: Personas naturales y jurídicas que contratan servicios de telecomunicaciones.
Tipo de gestión: Empresa privada que ofrece servicios de telefonía móvil, internet y de servicios fijos.

1.3 De la intervención

Esta propuesta se gesta ante la realidad hiperconectada en la cual vivimos, la cual es impulsada por tecnologías emergentes y avanzadas como las redes 5G, la inteligencia artificial, la integración y comunicación entre los objetos (internet de las cosas), entre otros. Ante esta situación, las personas y dispositivos están más expuestos a intentos de violación de seguridad de información, lo cual se agrava considerando que las debilidades más significativas suelen ser el desconocimiento, y las reacciones instintivas y apresuradas de las personas en su interacción con internet (Siadatia et al., 2017).

La empresa brinda servicios digitales y siempre debe estar conectado a internet para asegurar la comunicación y conectividad con alta disponibilidad, con lo cual el riesgo a ciber ataques aumenta.

Dado que la hiper conectividad implica una condición de riesgo, esta propuesta desea afrontar la situación actual de los empleados respecto a su consciencia digital, así como plantear acciones de prevención, cultura y políticas sobre seguridad de información, con el fin de preparar a los empleados para que reaccionen de forma responsable y segura ante situaciones de ataques a través de internet.

Ámbito de la intervención: Institucional, formación de empleados para concientizarlos en seguridad informática.

Duración de la propuesta: 6 meses.

Población objetivo: Doscientos cincuenta (250) empleados de la vicepresidencia de tecnología de información de la empresa de telecomunicaciones.

2. Justificación de la propuesta de innovación educativa

La tecnología digital está inmersa en la vida del ser humano. Está cambiando al mundo y a la forma en la que las sociedades y los individuos se comportan e interactúan. Un ejemplo de ello se dio cuando en octubre del 2012 se enviaron más de 20 millones de *tuits* solo en una semana, luego que el Huracán Sandy golpeó la costa este de Estados Unidos (Shih, 2012); y para el mismo evento, Instagram procesó más de 10 fotos por segundo (Ngak, 2012).

Podemos decir que la tecnología digital impacta en cómo las personas perciben el mundo y en la forma cómo interactúan con su entorno. En ese sentido, Pashentsev et al. (2019), indican que el uso generalizado de la tecnología digital, en todos los ámbitos de la sociedad, influye directamente en la mentalidad y en la conciencia de los individuos. Además, Isachenko (2018) nos dice que la tecnología fomenta el desarrollo de una sociedad moderna, ya que la transforma y adapta, aportando instrumentos para el desarrollo de la sociedad, y para la transferencia de información y de conocimiento. Sin embargo, la presencia, uso y dependencia de la tecnología implica riesgos de seguridad y privacidad para las personas y organizaciones (Andress y Leary, 2016), esto debido a que también facilita la creación de herramientas y técnicas, basadas en la interconectividad de internet, para saltar controles y romper barreras de seguridad informática de las organizaciones (Almeida, 2012) o para engañar y manipular a las personas con el fin de obtener información confidencial.

Por otro lado, internet se ha convertido en una herramienta clave para la comunicación, integración y colaboración entre personas y organizaciones, ya que ha transformado las prácticas y posibilidades de comunicación haciéndola más amplia, simple y casi instantánea (Rogers, 2019). Esto ha servido de impulso al crecimiento, popularidad y diversidad de las redes sociales, logrando una activa y masiva participación de las personas a través de publicaciones o siendo parte de juegos y retos sociales. Tayouri (2015) comenta que en el estudio "Why People Use Social Media Sites" se encontró al 31% de las personas usando las redes como herramienta de socialización, lo cual los lleva a compartir información, muchas veces sin necesidad ni con el cuidado respectivo.

En este escenario, la privacidad y la seguridad de información se vuelven críticas, más aún con el crecimiento de capacidades y acciones de delincuentes que aprovechan las redes sociales para obtener información que les sirva con la finalidad de realizar ataques a través de internet. Así también, existe una gran preocupación por el crecimiento y evolución de los llamados "exploits", que aprovechan las vulnerabilidades de usuarios y las brechas existentes en los sistemas, para comprometer la seguridad de las personas y organizaciones (Albladi y Weir, 2020). También realizan ataques llamados de "ingeniería social" sobre las personas, haciéndose pasar por gente o instituciones de confianza, con el fin de manipularlas y hacerlas caer en una trampa informática, para que revelen datos personales o financieros, o que compartan sus credenciales para infiltrarse en sus dispositivos, sistemas y organizaciones.

Ante esta situación aparece el concepto de ciber seguridad como mecanismo de defensa ante amenazas y ataques informáticos. Para Walker-Roberts et al. (2020), el objetivo principal en un incidente de ciber seguridad es la información, y tiene como característica frecuente a la violación de seguridad como resultado de la acción y del error humano. Estos comportamientos y acciones de los individuos, en su interacción con internet, influyen en mayor o menor grado para convertirse en víctimas de ataques informáticos y de suplantación de identidad (Abroshan et al., 2021).

De acuerdo con Aldawood y Skiner (2020), la ciber seguridad, junto a sus estrategias y técnicas, seguirá evolucionando debido a la necesidad de prevenir, enfrentar y contrarrestar los ataques informáticos. En el mismo sentido, Sonowal y Kuppusamy (2020) indican que los ciber ataques son un peligro para las organizaciones y un enorme desafío para la humanidad. Según el "The 2020 Official Annual Cybercrime Report" (Cybersecurity Ventures, 2020), el delito informático o ciber delito costará al mundo más de $ 6 billones anuales para este 2021 debido a los daños y a las acciones para enfrentarlo. Además, según estudios de *Threat Intelligence*

Insider Latin America (Fortinet, 2021), en el primer trimestre del 2021 Perú sufrió más de 1000 millones de intentos de ciber ataques.

Adicionalmente, Aldawood y Skiner (2020) comentan que atacar el conocimiento humano seguirá siendo una amenaza significativa, ya que los empleados son susceptibles de ser manipulados con el fin de que filtren información o permitan acceso no autorizado sin darse cuenta. Alzahrani (2020) considera que las personas están viviendo un estado de estrés y ansiedad social, lo cual las hace más vulnerables a ataques contra su seguridad de información. Para Albladi y Weir (2018) es muy importante plantear modelos y estrategias que ayuden a identificar y comprender mejor los factores que influyen en las personas, en sus competencias y en sus acciones ante eventos que atentan contra su seguridad de información, todo con el fin de ganar una mayor conciencia y tener una mejor reacción ante amenazas de ciber ataques.

Como vemos, la posibilidad de ser blanco de los delincuentes por internet pone a prueba la conciencia sobre seguridad de las personas en las organizaciones. Estos delincuentes perfeccionan y evolucionan sus técnicas de manipulación y suplantación, lo cual aumenta el nivel de amenaza y de riesgo. De acuerdo con las estadísticas de Frumento *et al*. (2016), el 97% de los ataques de software maligno se dirigieron a usuarios a través de intentos de piratería de ingeniería social, por lo que es crucial medir y fortalecer su nivel de conciencia en seguridad de información, así como moldear su comportamiento y su responsabilidad para que tomen las decisiones correctas ante amenazas de ataques por internet.

Los ciber delincuentes atacan a las organizaciones aprovechándose de la confianza de las personas, de su interés por ayudar y compartir información, de sus limitadas competencias digitales y de su poca conciencia sobre riesgos y daños generados tras un ciber ataque; pero también se aprovechan del estrés, ansiedad y angustia de las personas que los hace más vulnerables a amenazas de manipulación a través de ingeniería social (Alzahrani, 2020). Según Behar (2019), los ciber delincuentes también se aprovechan de las reacciones instintivas y apresuradas de las personas para hacerlas víctimas de sus ataques.

Los empleados de grandes compañías son un blanco atractivo para sufrir ciber ataques. Según el informe "Analysis of cyber attack and incident data from IBM's worldwide security operations" (IBM, 2014, p. 3), los ciber delincuentes aprovechan cuando los empleados acceden a internet y a las redes sociales para lanzar campañas dirigidas de ataques a través de sus cuentas corporativas; además atribuye al factor humano un desalentador 95% de los incidentes generados por estos ataques.

Por su lado, el Informe del Centro de Ciber Inteligencia de la empresa de telecomunicaciones (ENTEL Corp, 2020) comenta que las posibilidades de sufrir ciber ataques

se incrementan por la falta de consciencia digital en seguridad de información. Añade que, el impulso digital, provocado por la pandemia, ha acelerado la aparición de brechas y vulnerabilidades en ciber seguridad. Por lo tanto, esta corporación, donde se realizará la propuesta, es consciente de la existencia de vulnerabilidades y riesgos de sus empleados ante posibles ataques informáticos, lo cual se puede generar por falta de conocimientos y habilidades digitales, poca consciencia sobre seguridad de información, falta de responsabilidad en la interacción con la tecnología e incluso, por curiosidad e ignorancia. Es decir que, los empleados pueden realizar acciones no intencionales o no actuar adecuadamente, permitiendo un incidente de seguridad que ponga en riesgo a la información privada del mismo empleado, de la compañía o de los clientes.

Según lo expuesto, se define el problema a ser tratado en esta propuesta de innovación**, como la limitada consciencia y capacidad en seguridad de información por parte de los empleados de una empresa de telecomunicaciones de Lima para enfrentar ataques de ingeniería social**. Por ello, se desarrollará una estrategia que amplíe su nivel de consciencia sobre los riesgos en internet e impulse una mayor responsabilidad en sus interacciones en las redes sociales y en internet en general.

Teniendo en cuenta que el conocimiento y las tecnologías evolucionan, es necesario que las personas se mantengan motivadas y actualizadas, ya que a los ataques de ingeniería social se deben enfrentar reforzando la consciencia, con una correcta actitud y con un rol claro de los empleados en el marco de la seguridad de información (Alzahrani, 2020). Para ello, se necesita profundizar en educación, capacitación y tecnología (Tayouri, 2015), considerando que el ser humano es aliado a la seguridad de información cuando está fortalecido y consciente de su rol y de sus acciones.

Por ello, el planteamiento del estudio considera el diseño de una propuesta de innovación educativa enmarcada en la línea de investigación de cultura digital y redes de aprendizaje, y en la sublínea de desarrollo de competencias digitales, para implementar un programa de concientización y sensibilización de los empleados respecto a su rol en el ámbito de seguridad de información de la compañía. Este programa propone un modelo de formación en ciber seguridad que motive a los empleados a permanecer vigilantes y alertas a las ciber amenazas, y promueve que adecúen su comportamiento para que actúen de manera consciente en seguridad de información.

3. Fundamentación Teórica

La presente propuesta de innovación se fundamenta en un marco que relaciona los conceptos de tecnología, seguridad de información y comportamiento humano, y que facilita un mejor entendimiento de la importancia e impacto que supone la pérdida de confidencialidad, integridad y disponibilidad de la información. Esta fundamentación aporta una mayor claridad sobre la situación y riesgo que viven los empleados en este mundo tecnológico; además que incorpora aspectos relevantes en el aprendizaje de adultos como son su experiencia previa, motivación y dedicación. Todo esto ayuda al planteamiento, diseño e implementación de un programa de formación en consciencia, mejores prácticas y gestión de riesgos en seguridad de la información.

3.1 ¿Qué es la Ciber Seguridad?

De acuerdo con Matulewska y Ciszek (2019), el prefijo “ciber” es utilizado como denotativo de "digital”, es decir relacionado con la informática, con internet y en general con tecnología digital. Así aparecen términos como ciber espacio, ciber seguridad, ciber ataque, ciber crimen, entre otros.

La ciber seguridad se refiere al acto de defender a las personas y organizaciones de ataques informáticos, mediante un conjunto de técnicas, acciones, procesos, buenas prácticas y tecnologías diseñadas para identificar y protegerse de amenazas y de ataques o de accesos no autorizados. En una estrategia de ciber seguridad no solo se debe considerar las herramientas tecnológicas, sino que hay que involucrar al ser humano en la prevención y detección de amenazas de ciber ataques.

Según Herrmann y Pridöhl (2020), la ciber seguridad está sujeta a importantes asimetrías, ya que, por un lado, los ciber delincuentes tienen gran variedad de alternativas de ataques, mientras que los defensores deben prestar atención a cada detalle y estar preparados para cualquier cosa, en cualquier momento. Además, sin importar los controles, políticas o capacitaciones que se establezcan en torno a la seguridad de información, las personas seguirán siendo blanco de ataques informáticos. Por eso es fundamental definir e implementar una estrategia de ciber seguridad que integre la participación de las personas, los procesos y la tecnología.

Uno de los mayores desafíos de la ciber seguridad es la acción, reacción o inacción del factor humano durante eventos de ciber ataques. Esto refleja la importancia de la consciencia humana en seguridad, pero implica no solo conocimiento, sino actitudes y comportamientos

que ayuden y permitan enfrentar adecuadamente situaciones que afecten a la seguridad de la información. Por ello, es fundamental que los empleados estén al tanto de las amenazas y vulnerabilidades existentes en el mundo digital, así como la forma de detectarlos y mitigarlos.

En ese sentido, es importante tener una buena comprensión de aquellos conceptos base en gestión de seguridad de información para ser conscientes de la existencia de amenazas en internet, de la necesidad de protección ante las vulnerabilidades y de la prioridad que se debe dar a la gestión de riesgos en ciber seguridad.

3.1.1 Las amenazas, vulnerabilidades y riesgos

Dentro de la ciber seguridad se maneja un marco conceptual basado en los elementos fundamentales: amenaza, vulnerabilidad y riesgo; los cuales tienden a ser mezclados, confundidos e incluso muchas veces se usan de manera intercambiable. Sin embargo, su comprensión es importante porque puede hacerse suposiciones incorrectas sobre seguridad de información y no ser conscientes del peligro, dejando abiertas brechas de seguridad.

De acuerdo con Herrmann y Pridöhl (2020), la seguridad informática busca proteger los activos valiosos como hardware (por ejemplo, ordenadores y smartphones), software y datos, que están sujetos constantemente a amenazas que pueden provocar pérdidas o daños.

Las ciber amenazas son eventos o actos maliciosos que tienen el potencial de causar daño, robar datos o afectar la vida digital en general. Las ciber amenazas pueden ser intencionales o no intencionales y sus causas podrían originarse en incidentes, acciones o falta de acción. Entre las amenazas más comunes están los ataques de ingeniería social, el *phishing*, virus informáticos, filtraciones de datos, ataques de denegación de servicio (DoS) entre otros (Secureworks, 2017).

Por su lado, la vulnerabilidad en ciber seguridad, se trata de una debilidad, falla o error, que existe en las personas, organizaciones y sistemas; y que son atractivas para los delincuentes informáticos, ya que, con el esfuerzo adecuado, pueden realizar acciones no autorizadas para obtener información confidencial, infiltrarse y comprometer los activos de las compañías. A diferencia de las ciber amenazas que se producen como resultado de un evento externo, las ciber vulnerabilidades ya existen en el entorno (Hewitt, 2021). Por ello, es importante identificar aquellos factores que incentivan y magnifican las vulnerabilidades, con el fin de orientar esfuerzos y acciones en ciber seguridad.

Por otro lado, el riesgo en ciber seguridad es la pérdida o daño potencial de activos e información sensible, afectación financiera o de reputación, ante eventos maliciosos, los cuales

implican ciber amenazas que explotan a las vulnerabilidades, como en el caso de un ataque informático que aprovecha debilidades de los sistemas o de las personas. Estos eventos pueden ser el resultado de actos deliberadamente maliciosos, pero también pueden ser involuntarios, como un error de un empleado que genera algún daño en un sistema al descargar un programa con virus informático (RSA, 2016).

Las personas y organizaciones viven una situación de riesgo constante en internet, que se ve incrementado por las fuerzas continuas de amenazas de ciber delincuentes. Por ejemplo, por más que se cuenten con niveles de seguridad avanzados, si los empleados confían en la persona equivocada, se convierten en una vulnerabilidad que será aprovechada por los ciber delincuentes. En ese sentido, la división de seguridad de RSA (2016) comenta que el riesgo debe equilibrarse con actividades para gestionarlo dentro de una tolerancia que sea aceptable para la organización, para lo cual se debe tener una comprensión clara de la exposición al riesgo y considerarla dentro de su estrategia de crecimiento.

3.2 El Ciber ataque y sus características

Para las organizaciones, el impacto y costos asociados con delitos informáticos cada vez son mayores e incluyen daño y destrucción de datos, robo financiero y de propiedad intelectual, pérdida de productividad, robo de identidad y más; incluso con afectación posterior al ataque (Cybersecurity Ventures, 2020).

Los ciber ataques son intentos maliciosos, acciones ofensivas y deliberadas con el objetivo de acceder a un sistema informático sin autorización para dañar, robar información o activos financieros de un individuo o de una organización. El atacante se aprovecha de vulnerabilidades existentes para instalar algún programa informático malicioso que le permita cometer delitos informáticos, como el robo de información y de identidad.

Las organizaciones pueden sufrir distintos tipos de ataques de desarrolladores maliciosos, que buscan superar su seguridad. En tal sentido, Albladi y Weir (2018) comentan que, además, la autoconfianza en las habilidades informáticas puede conducir a conductas de riesgo, que la conciencia de seguridad y de privacidad son críticas en las prácticas de autoprotección; y que las dimensiones de motivación, así como de confianza influyen en la susceptibilidad a los ciber ataques.

A medida que las organizaciones y personas dependen de sistemas y aplicaciones interconectados a través de internet, la privacidad y seguridad están expuestos a mayor riesgo, ya que los ciber ataques se han vuelto cada vez más sofisticados, peligrosos y dañinos.

Los delincuentes informáticos utilizan distintas formas para perpetrar ciber ataques, como la ingeniería social, *malware*, *phishing*, *ransomware*, denegación de servicio, entre otros métodos. A continuación, se analizarán una serie de conceptos que permitirán tener una mirada completa sobre los ciber ataques.

3.2.1 Ciber delincuente

En un sentido más amplio, un ciber delincuente, también llamado hacker o pirata informático, es una persona que utiliza sus habilidades técnicas en tecnología y programación, apoyándose de hardware, software y redes interconectadas para resolver algún problema, limitación técnica o encontrar sus debilidades y explotarlas. Estas personas pueden estar motivadas por distintas razones; es decir con fines ilegales o poco éticos, como usar sus habilidades para obtener acceso no autorizado a sistemas o redes con el fin de cometer delitos, robar información, dinero, dañar sistemas o incluso secuestrar información y solicitar rescate.

El ciber delincuente se centra en realizar actividades ilegales mediante el uso de tecnología digital. Estas actividades ilegales o delitos informáticos pueden incluir robo de identidad, estafas y fraudes en línea, creación y diseminación de virus o ataques a sistemas y sitios informáticos (Sammons y Cross, 2017).

3.2.2 Software malicioso o malware

El Malware es un término utilizado para hacer referencia a una serie de variantes de software malicioso, incluyendo virus, *ransomware* y *spyware* y gusanos informáticos. Consiste en programas informáticos diseñados para ser invasivos y causar daños a los sistemas de información o para obtener acceso no autorizado a los dispositivos digitales. El malware entra en una red de computadoras a través de alguna vulnerabilidad, generalmente en complicidad de alguna persona, normalmente inconsciente de su participación, pero que activó el virus al tratar de abrir un archivo o un enlace infectado. Normalmente se transmite a través de correo electrónico, con enlaces o archivos adjuntos, con mensajería instantánea, suplantación de identidad, entre otros.

El *malware* puede destruir datos en las computadoras infectadas, aumentar considerablemente el tráfico de red informática, puede bloquear el acceso de usuarios, esparcir software dañino, robar información o dejar inoperativos dispositivos.

3.2.3 Suplantación de identidad o *phishing*

Se trata de un conjunto de técnicas que busca engañar a una persona para que realice o ejecute "algo incorrecto", como hacer clic en un enlace que parece provenir de una fuente confiable, pero que se trata de comunicaciones fraudulentas que terminan instalando un software malicioso o redirige al usuario a sitios web poco fiables. Este tipo de ciber ataque implica una mezcla de ingeniería social y técnicas usadas para suplantar la identidad de una persona o una institución, con el fin de persuadir al usuario de que revele datos confidenciales y personales (Alotaibi y Alsuwat, 2020).

Según Abroshan et al. (2021), los ciber delincuentes o estafadores diseñan un enfoque paso a paso para el *phishing* con el fin de ganarse la confianza de la víctima y convencerla de que realice las acciones que desea. Esta técnica de ciber ataque trata de ganar la confianza de su víctima con el fin de que ignoren las buenas prácticas en seguridad y proporcionen información o acceso restringido a terceros.

Estos estafadores utilizan vulnerabilidades técnicas, sociales y psicológicas de sus víctimas para adquirir información confidencial y utilizarla para robar o lanzar otros ataques (Abroshan et al., 2021). Por lo general se realiza a través de correos electrónicos, mensajes de texto, redes sociales o incluso por teléfono, con mensajes fraudulentos que parecen provenir de entidades fidedignas.

En ese sentido, es importante entender y conocer las razones por las que las personas siguen las indicaciones de los atacantes de *phishing* para considerarlas en un plan y programa eficaz que permita reaccionar correctamente ante los ataques de *phishing*.

3.2.4 Secuestro de datos o ransomware

El *ransomware* es actualmente una de las mayores amenazas en los ciber ataques de malware. La falta de conciencia y medidas de seguridad adecuadas impulsó su rápida propagación y el aumento de la gravedad de sus variantes (Ferreira, 2018). El *ransomware* o secuestro de datos, es un tipo de ataque que usa un software malicioso cuyo fin es acceder y robar información confidencial de los sistemas informáticos para luego cifrar y bloquear los datos, dejando inutilizables los archivos y los sistemas que dependen de ellos, con el fin de que los dueños no puedan acceder, con lo cual piden un rescate financiero.

Este tipo de ataque se propaga a partir de correos electrónicos de *phishing* que contienen archivos adjuntos maliciosos o mediante acceso a sitios web infectados, en ambos casos con participación de usuarios que sin saber descargan el virus.

Los ciber delincuentes de *ransomware* amenazan con vender, filtrar datos extraídos o eliminarlos si no se paga el rescate, lo cual puede ser devastador para un individuo o una organización. Los impactos personales, económicos y de reputación de los incidentes de *ransomware* suelen ir más allá que el monto de rescate, ya que no se garantiza que se recuperen intactos los sistemas e información, además que no es seguro que se elimine la infección, por lo que la recuperación ante este ataque puede ser costosa y duradera.

3.3 La ingeniería social

La ingeniería social es uno de los mayores desafíos que enfrenta la seguridad en internet, porque explota la tendencia natural humana de la confianza (Salahdine y Kaabouch, 2019); se basa en técnicas de manipulación altamente eficaces, ya que más del 80% de los ciber ataques se centran en el factor humano, en lugar de hacerlo en los fallos de seguridad de sistemas informáticos (Erbschloe, 2019). Según Breda et al. (2017), la ingeniería social es el "arte" de explotar los defectos humanos, ya que se enfocan en ganar la confianza de la víctima a través de mostrar una identidad suplantada o robada.

De acuerdo con Mouton et al. (2014), el factor humano sigue siendo un eslabón débil debido a que las personas son susceptibles de ser manipuladas y un ataque de ingeniería social aprovecha esa debilidad mediante el uso de la interacción social, como un medio para persuadir a un individuo a que realice una solicitud específica del atacante. Además, según Alazri (2015), la mayoría de las organizaciones sufren de una falta de consciencia y conocimiento de los riesgos de los ataques de ingeniería social.

En la ingeniería social, el atacante realiza una especie de intrusión no técnica, ya que se basa en la interacción humana y en patrones de comportamiento de las personas. Para esto, el ciber delincuente recopila información de su víctima que le pueda servir y busca establecer una relación de confianza con ella. Para desarrollar simpatía y confianza con su víctima usa la información, tergiversando una identidad, citando a personas o instituciones conocidas por la víctima, mostrando la necesidad de asistencia u ocupando un papel de autoridad. Cuando la persona parece confiar, el atacante explota esa confianza para manipular a su víctima.

Una de las razones por las que estos ataques son efectivos es la falta de habilidades digitales y la dificultad que tienen las personas de verificar y confirmar si las comunicaciones que se reciben son reales o no. Esta técnica de manipular a los individuos, para que divulguen información sensible, existe desde antes de la creación de internet, ya que los delincuentes

utilizaban el teléfono, el servicio postal o la publicidad para hacerse pasar por un agente de confianza con el fin de robar información.

De acuerdo con Albladi y Weir (2018) existe un conjunto de atributos que determinan la vulnerabilidad de las personas a un ataque de ingeniería social. Entre dichos atributos están el comportamiento y los hábitos de las personas en internet, su nivel de percepción y de respuesta ante una amenaza, sus rasgos de personalidad y autoconfianza que influyen en su comportamiento y en la toma de decisiones ante un riesgo, así como su nivel de que influye en su juicio y acción ante ataques en línea. confianza

En relación con lo anterior, Aldawood y Skinner (2018) realizaron un estudio en el que concluyen que la ingeniería social es una gran amenaza a la ciber seguridad e indican que una de las principales razones de su gran impacto es la falta de conciencia de los usuarios finales. Además, plantean que las organizaciones deben ser conscientes de esta amenaza, y que deben garantizar un nivel suficiente de consciencia en seguridad de información de sus empleados. Su investigación concluye que la participación de las personas es crucial durante ataques de ingeniería social y que la conciencia de seguridad de información es clave para mitigar impactos.

3.4 Consciencia en ciber seguridad

Zwilling et. al (2020) realizaron un estudio para evaluar las relaciones y diferencias entre la conciencia sobre los ciber peligros, el conocimiento y el comportamiento de seguridad ante los peligros de ciber ataques. El estudio lo realizaron en Eslovenia, Israel, Turquía y Polonia, ya que la economía de los dos primeros era más desarrollada que la de los otros dos, y consideraron como válido, que la ciber seguridad y la consciencia sobre riesgos de ciber ataques están directamente ligadas al desarrollo económico. Entre los resultados mencionan que los individuos saben que el uso de internet los expone a amenazas de ciber seguridad, pero su comportamiento no necesariamente refleja una acción congruente ante el riesgo. Además, afirman que un mayor conocimiento digital debería contribuir a un mejor nivel de consciencia sobre ciber seguridad y que los programas de formación en ciber seguridad deben desarrollarse con una orientación tecnológica internacional, no basados en expresiones locales y culturales, considerando el comportamiento y reacción individual de las personas.

A medida que la era digital avanza, las amenazas y los riesgos de seguridad van en aumento, las personas están más expuestas que nunca. La explotación y vulnerabilidad de los seres humanos, considerados como el eslabón más débil en la seguridad informática, vuelve

imprescindible la concientización de las personas en temas de ciber ataques. Para ello, es crucial contar con programas innovadores y eficaces de formación y educación en seguridad de información que permitan reducir los incidentes de ciber seguridad.

De esta manera, Aldawood y Skinner (2018) mencionan que para tratar de reducir la acción de la ingeniería social las instituciones deberían establecer protocolos exhaustivos y políticas de seguridad claras, que consideren programas integrales de seguridad de la información, basados en el desarrollo de una mayor consciencia y de capacidades digitales. De este modo, las personas sabrán cómo reaccionar para salvaguardar y proteger los activos de información.

Por lo expuesto anteriormente, podemos decir que es necesario contar con un programa de capacitación que sea eficaz, que permita incorporar una cultura de pertenencia y sentido al propósito de la organización, y que aporte un alto nivel de concientización y responsabilidad sobre la seguridad de información. Además, esta formación debe ser motivadora, influyente, participativa e informativa para que la organización completa asuma la importancia y beneficios de participar activamente en la protección de la información de las personas y de la organización.

3.5 El aprendizaje adulto

Es importante conocer y comprender aquellos aspectos que influyen en el aprendizaje de adultos con el fin de diseñar y desarrollar un programa de formación efectivo. Según Malcolm Knowles (1988, como se citó en Mukhalalati y Taylor, 2019), los adultos tienen experiencia, motivación, orientación y necesidad de aprender diferentes a los de los niños, a lo cual Mukhalalati y Taylor (2019) añaden que dichas ideas son importantes en la educación profesional, ya que sirven de marco conceptual para gestionar la adquisición de conocimientos, habilidades y lograr cambios en el comportamiento y desempeño del adulto.

Se entiende que los adultos y los profesionales son responsables y conscientes de sus necesidades de aprendizaje; además, tienen experiencias valiosas, conocimientos previos, capacidad de análisis y de reflexión que les favorecen en el proceso de aprendizaje y en el crecimiento profesional y personal. En ese sentido la madurez del adulto y su interés por seguir desarrollándose lo motiva a adquirir y aplicar nuevos conocimientos, lo cual le brinda satisfacción personal al reconocer el valor del aprendizaje para el mismo.

Por otro lado, hay que tener en cuenta situaciones que pueden afectar el proceso de aprendizaje de los adultos como la distracción, el tiempo limitado, la carga de trabajo y otras

responsabilidades que reducen la dedicación y concentración en los estudios. Además, otro aspecto a considerar es el temor y duda sobre lo nuevo, al cambio y la posibilidad de fracasar. En ese sentido, es fundamental que el programa de innovación educativa considere las necesidades de formación, las formas de aprendizaje y los objetivos del proceso de aprendizaje de un adulto.

Por lo tanto, considerar las características del aprendizaje de adultos facilitará la planificación y organización de actividades, creación de contenidos y recursos, diseño de estrategias didácticas, definición de tiempos y espacios para una capacitación exitosa.

4. Objetivos de la Propuesta

Objetivo general

- Desarrollar en los empleados de una compañía de telecomunicaciones de Lima, capacidades en seguridad de la información que les facilite detectar y reaccionar positivamente ante intentos de ciber ataques de ingeniería social, mediante un programa de formación para generar consciencia en ciber seguridad.

Objetivos Específicos

- Diseñar una propuesta de formación que permita mejorar la consciencia sobre ciber seguridad de los empleados de una compañía de telecomunicaciones de Lima.
- Sensibilizar a los empleados respecto al conocimiento y consciencia sobre ciber seguridad que conduzcan a una disminución y mitigación de ataques de ingeniería social.
- Incorporar herramientas de evaluación en el programa para medir el nivel de riesgo y consciencia de los empleados en ciber seguridad.

5. Metas de la Propuesta

Esta propuesta de innovación educativa de seguridad de información es el resultado de estrategias trazadas para cumplir con los objetivos y proteger a los empleados y a la organización de posibles ciber ataques.

La meta de atención del programa completo es de 250 empleados de las áreas de sistemas de la vicepresidencia de tecnología de información, quienes al tener buen nivel de conocimiento digital pueden ser influenciados por los atributos de autoconfianza y autoeficacia que facilita ser víctimas de ciber ataques de ingeniería social.

Las metas de capacitación incluyen a las áreas: de seguridad de información con 6 integrantes para la gestión del aspecto técnico, de capital humano con 1 integrante para la gestión de comunicaciones, del equipo de capacitación con 1 persona para gestionar el proceso de entrenamiento bajo las políticas de su área y a todos los empleados de las áreas de sistemas de la vicepresidencia de tecnología de información.

En cuanto a la meta de implementación se considera realizar sesiones síncronas y asíncronas: dos sesiones síncronas (inicio y fin del programa), tres sesiones asíncronas con material digital y con contenido sobre ciber seguridad para fortalecer conocimientos y realizar ejercicios prácticos, dos encuestas de medición del nivel de consciencia sobre ciber seguridad (inicio y fin del programa), dos simulacros de ciber ataques y 2 series de entrevistas a líderes y empleados participantes del programa.

6. Estrategias y actividades para el diseño de la propuesta

Las estrategias y actividades se basan en los pilares de comunicación, motivación, concientización, actualización y mejora continua. La propuesta completa tendrá una duración de 6 meses con el fin de que se cuente con el tiempo necesario para desarrollar, implementar y poner en marcha el programa, y para que los empleados tengan una participación activa y eficiente. Las fases de la propuesta son cinco:

- Fase 1: Sensibilización y coordinación por 4 semanas, con el fin de lograr la comprensión, apoyo y participación de los líderes de la compañía. En esta fase se sustentan los beneficios, tiempos y la inversión necesaria, logrando la aprobación de recursos humanos, técnicos y financieros. Las actividades y entregables de esta fase tienen como objetivo lograr el consenso y aprobación respecto a la importancia de impactar en la consciencia, comportamiento y buenas prácticas en seguridad de información por parte de los empleados. Sus principales entregables son:
    - Alcance y objetivos del Programa.
    - Beneficios de la implementación del programa.
    - Riesgos e impactos de no aplicar el programa.
    - Identificación y definición de recursos, software y hardware existente para apoyar a la propuesta educativa en la compañía.
    - Estimación de costos y tiempos.
    - Caso de Negocio que sustente la validez de implementar el programa.

- Identificación de los principales interesados y participantes para el programa.

- Fase 2: Diseño de la propuesta durante 4 semanas, para definir y estructurar el programa de formación acorde a las necesidades de la empresa, combinando cursos breves e interactivos, incluyendo refuerzo a través de simulaciones de *phishing* automatizadas y continuas. En esta fase se armará a detalle, el plan de implementación y de comunicación efectiva e integral para toda la compañía. Además, se determinarán las actividades, dependencias y sus responsables. Los entregables de esta fase son:
  - Planificación completa de la implementación (recursos, tareas, entregables, etc.).
  - Estrategia de comunicación.
  - Cronograma detallado (nivel 3) de actividades e hitos del programa.
  - Definición de las temáticas de sesiones educativas y evaluaciones.
  - Diseño de contenido de sesiones, incluyendo actividades lúdicas y gamificación.
  - Contratos y convenios para la elaboración y personalización de cursos en ciber seguridad.

- Fase 3: Construcción e implementación durante 4 semanas, en las que se desarrolla el programa de concientización en ciber seguridad. También se definen y elaboran los mecanismos de capacitación y comunicación con los empleados para la ejecución del programa de capacitación. Además, se construyen las actividades de formación, su calendario y se preparan los materiales, el marco de tiempo y las métricas de capacitación. En esta etapa se adecúa el contenido y metodología en relación a los diferentes roles, competencias y necesidades de los empleados. Los entregables son:
  - Calendario de sesiones de formación síncronas / asíncronas.
  - Material para sesiones, incluyendo flujos, retos y reglas de gamificación.
  - Mecanismos de comunicación y seguimiento a los empleados.
  - Publicación de las sesiones de formación en la plataforma de aprendizaje.

- Fase 4: Ejecución o desarrollo durante 12 semanas, en las que se pone en práctica la propuesta educativa, desarrollando las sesiones de aprendizaje y se realizan autoevaluaciones y ejercicios prácticos. En esta fase es crítico transmitir y comunicar claramente la importancia y obligatoriedad de las capacitaciones para que los

empleados sean conscientes que son parte de las políticas de la compañía. Los procesos principales de esta etapa son:

- Gestión de participación y avance del programa.
- Gestión de incidentes y problemas que se presenten.
- Gestión de cambio o ajuste si fuese necesario.

- Fase 5: Seguimiento y Monitoreo que se realiza en paralelo y a lo largo de todo el programa, para realizar una revisión y análisis de los resultados de la capacitación e identificar cambios en el comportamiento y consciencia sobre ciber seguridad de los empleados que llevaron el curso. En esta fase se identificarán oportunidades de mejora del programa.

Los riesgos con los cuales nace esta propuesta están relacionados con dos temas fundamentales. Primero, la poca aceptación y apoyo de los líderes de la compañía para invertir tiempo y el presupuesto necesario que soporte a esta iniciativa, lo cual se espera mitigar sustentando adecuadamente el beneficio de la propuesta y el riesgo de no hacerla. Como segundo riesgo está la posibilidad del bajo nivel de participación y compromiso de los empleados durante la ejecución del programa, lo cual se espera manejar con el apoyo de las autoridades y líderes de la empresa.

7. Recursos humanos

Para esta propuesta de innovación educativa en consciencia y sensibilidad de ciber seguridad se seleccionará un equipo que planifique, ejecute y asegure cumplir sus objetivos. Este equipo estará compuesto por:

- ***Sponsor* o patrocinador**; quien guía, facilita y toma las decisiones importantes y es portavoz del equipo del programa frente a la dirección de la compañía. Para este programa sería el vicepresidente de tecnología de información porque pertenece a la dirección de la compañía y dentro de su alcance está la seguridad de información.
- **Promotor o dueño**; quien toma como suyo al programa, y asume la responsabilidad de llevarlo adelante. Dado que se trata de una propuesta sobre ciber seguridad, quien debe asumir este rol es el manager del área de seguridad de información, el cual presentará y entregará al programa como parte de las políticas de seguridad de información.

- **Líder de la implementación**; quien se encarga de la gestión del programa, preocupándose por cada actividad de inicio a fin. Para este programa será un supervisor del equipo de seguridad de información o el gestor que plantea este programa de innovación.
- **Analista de ciber seguridad**; quien será responsable de participar junto al proveedor en el proceso de diseño y construcción del material digital para las sesiones de aprendizaje síncronas y asíncronas.
- **Responsable del área de comunicaciones**; de capital humano, para definir y validar las comunicaciones sobre el programa a los empleados y líderes de la compañía.
- **Responsable del área de entrenamiento**; quien gestiona la plataforma de entrenamiento de la compañía.
- **Equipo de diseño del curso**; que estará formado por un analista de seguridad, uno del área de capacitación y uno del área de innovación.
- **Proveedores**; de cursos, evaluaciones y simulaciones virtuales.

8. Monitoreo y Evaluación

Esta propuesta de innovación educativa tiene una mirada completa sobre el proceso en y sus resultados, por lo que incluye metodología y mecanismos para medir su progreso y su impacto al final del mismo. En ese sentido, considera la relevancia e importancia de medir y evaluar frecuentemente el cumplimiento de los objetivos trazados, identificando si el aprendizaje ha sido efectivo a partir del programa de formación planteado.

El monitoreo y evaluación constante permitirán identificar las fortalezas y puntos de mejora del programa. Además, fomentará la flexibilidad y mejora continua dentro de la propuesta educativa, y ayudará a validar la pertinencia del contenido y la metodología del proceso de enseñanza.

El monitoreo y control del programa es responsabilidad del líder de implementación, quien deberá considerar los siguientes puntos:

- Revisión periódica del estado del progreso del programa.
- Definición y medición de criterios de aceptación de fin de cada fase, como cumplimiento de alcance en tiempo según lo planificado, revisión y validación de calidad de los entregables y revisión de avance del cronograma y presupuesto.
- Desarrollo de evaluaciones, autoevaluaciones y retroalimentación previo y posterior a las sesiones de aprendizaje.

- Implementación de simulacros de ciber ataques, para medir el nivel de los empleados.
- Seguimiento a los indicadores:
    - Porcentaje de avance del programa.
    - Cumplimiento de criterios de aceptación de cierre de cada fase.
    - Porcentaje de empleados que culminan el programa completo.
    - Porcentaje de mejora en comportamiento / mejora en consciencia de ciber seguridad como resultado del entrenamiento y evidenciado con simulacros.
    - Tasa de resultados positivos de cuestionarios y participación en entrevistas.

Todos los indicadores serán definidos de forma que cumplan con las características de ser específicos, medibles, alcanzables, relevantes y de un tiempo duración específico.

9. Sostenibilidad de la propuesta

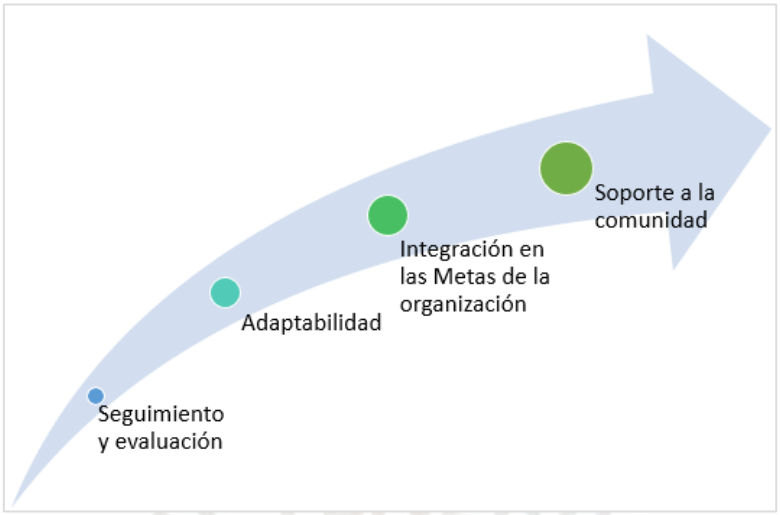
Respecto a la viabilidad y sostenibilidad de esta propuesta, la compañía ha desarrollado una estrategia de ciber seguridad, con alianzas, acuerdos y soporte de socios estratégicos en seguridad de información y especializados a nivel mundial. Esto le permite tener un ecosistema, soportado por socios como FORTINET, PALOALTO y CISCO, con soluciones tecnológicas que se centran el monitoreo y protección de plataformas e infraestructura ante ciber amenazas.

Además, tiene una política clara respecto al tratamiento de la información y a la importancia de protección de datos, lo cual sirve de catalizador y apoyo a este tipo de iniciativas. Todo esto es considerado y valorado en el comité de inversiones, al momento de revisar y aprobar presupuestos para las distintas iniciativas. También, se cuenta con recursos tecnológicos y humanos especializados en ciber seguridad para implementar un programa de este tipo de iniciativas de formación de los empleados.

De acuerdo con Morfaw (2014) el desarrollo sostenible está relacionado con la continuidad del proyecto en distintos aspectos como financieros, institucionales y de responsabilidades individual y organizacional. En ese sentido la planificación de los programas y proyectos deben incorporar actividades que desarrollen su sostenibilidad durante todo el ciclo de vida, con el fin de asegurar la mejora y continuidad de sus productos y beneficios a lo largo del tiempo. Para Wieners (2019) existen una serie de factores que influencian la gestión de sostenibilidad de un programa con el fin de obtener resultados eficientes y duraderos, de los cuales, el presente trabajo ha considerado cuatro (Figura 1) como los más importantes para asegurar la sostenibilidad de la propuesta.

Figura 1.

Factores que influencian la sostenibilidad de un programa



Nota: Adaptado de *Developing a Sustainability Plan in a Project Proposal* (Wieners, 2019)

- **Seguimiento y evaluación** periódica del programa y sus resultados. El área de seguridad de información realiza un proceso de revisión semestral del nivel de riesgo de los empleados, el cual se calcula basado en las pruebas de simulación de phishing, participación y evaluación de cursos de ciberseguridad y resultado de encuestas.
- **Adaptabilidad** o capacidad del programa de establecerse en el entorno acelerado y complejo de la empresa, en la cual los empleados están muy comprometidos con su trabajo y tienen prioridades que pueden afectar su participación en el programa. Para lo cual se medirá el porcentaje de avance del programa.
- **Integración en las metas de la organización**, de los objetivos y resultados del programa. En ese sentido la empresa aún está trabajando en establecer una línea base con indicadores de ciber seguridad, los cuales se incorporarán como objetivos en el plan estratégico anual. Esta situación permite la integración de la presente propuesta como una parte importante en el planeamiento del área de seguridad de información.
- **Soporte a la comunidad**, durante y después del programa propuesto. Para este factor se considera el desarrollo de las metas de capacitación del programa, que permitirá la preparación y adopción de la propuesta por parte de las áreas de seguridad de información, capital humano y de capacitación, con el fin de que aseguren el conocimiento y soporte del curso propuesto.

10. Presupuesto de la propuesta

En la siguiente tabla se presentan los conceptos y sus montos en soles peruanos (PEN) necesarios para la implementación de este programa de innovación. Hay varios conceptos que ya están cubiertos por presupuesto ya existente en la compañía, como licencias, recursos y personas internas de la empresa, pero otros conceptos deben ser cubiertos por presupuesto nuevo, como la construcción de los cursos por un proveedor.

Tabla 1.
Resumen del presupuesto estimado para la propuesta

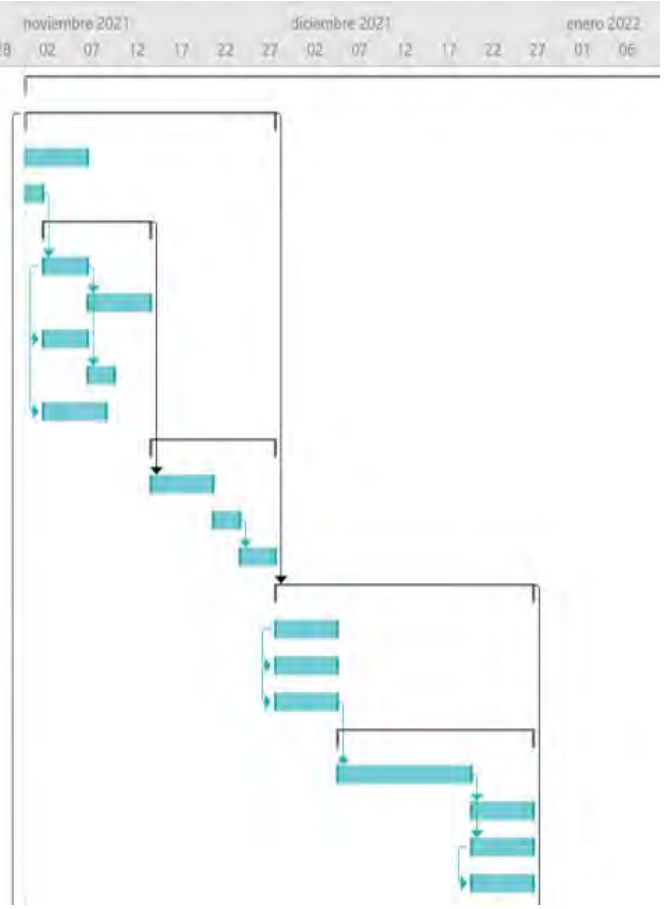
	Concepto	Tipo	Moneda	Cantidad	Monto	Periodo	Descripción
Plataformas	LMS - campus de Entrenamiento	Licencias	PEN	250	-	Anual	Plataforma de Capacitación, ya implementada en la compañía (SAP-Successfactors), las licencias están apalancadas en gasto operativo (OPEX) vigente.
	Simulación de ciber ataques	Licencias	PEN	250	-	Anual	Plataforma de simulación de *phishing* (Gophish), ya implementada en la compañía, de licenciamiento libre.
	Video conferencias	Licencias	PEN	250	-	Anual	Plataforma para sesiones síncronas, ya implementada en la compañía (MS Teams), las licencias están apalancadas en gasto operativo (OPEX) vigente.
Servicios	Servicio de consultoría y desarrollo de programa de capacitación en ciber seguridad.	Servicio	PEN	1	50,000	-	Proceso de diagnóstico, entrevista de profundidad, exploración grupal, desarrollo de encuestas, informes ejecutivos, sesiones síncronas, material en video y curso digital, certificado. Cotizado para 250 empleados.
	Diseño y lanzamiento de campañas y publicidad del programa	Servicio	PEN	-	-	-	Se utilizarán los recursos propios del equipo de Capacitación y de Comunicación de la compañía.
	Servicio de impresión, preparación envío de material físico, gestión de recursos y plataformas	Servicio	PEN	-	-	-	El programa será totalmente digital.

	Concepto	Tipo	Moneda	Cantidad	Monto	Periodo	Descripción
Recursos humanos	Patrocinador del programa	H/H	PEN	-	-	8 meses	Participación puntual por algunas horas durante el programa
	Promotor del programa	H/H	PEN	-	-	8 meses	Participación puntual por algunas horas durante el programa
	Líder de la implementación	H/H	PEN	20% día	12,800	8 meses	Costo de la participación por tiempo efectivo del líder. Se incluye costo ya que ese tiempo deja de atender las labores propias de su cargo.
	Analistas de ciber seguridad	H/H	PEN	20% día	8,000	8 meses	Costo de la participación por tiempo efectivo del analista. Se incluye costo ya que ese tiempo deja de atender las labores propias de su cargo.
	Responsable de comunicación	H/H	PEN	-	-	8 meses	Participación durante el programa. No se considera costo ya que parte de sus funciones actuales es la comunicación a nivel compañía.
	Responsable de entrenamiento	H/H	PEN	-	-	8 meses	Participación durante el programa. No se considera costo ya que parte de sus funciones actuales es el entrenamiento a nivel compañía.
	Empleados a capacitar	H/H	PEN	-	-	-	De las áreas de sistemas de la vicepresidencia de tecnologías de información. No se considera costo ya que las capacitaciones serán en horarios laboral.
				Total: S/.	**70,800.00**		

11. Cronograma de la propuesta

A continuación, se muestra el cronograma de actividades, detallado al tercer nivel de profundidad, agrupado por fases e indicando tiempo de duración por actividad e interdependencias. Las fechas son referenciales ya que se actualizarán una vez que el plan de implementación del programa sea aprobado e integrado al plan estratégico de la compañía:

	Nombre de tarea	Duración	Comienzo	Fin	Predeces.
1	**Propuesta de innovación educativa en ciber seguridad**	**120 días**	**mar 02/11/21**	**mar 19/04/22**	
2	**Fase Nro 1: Sensibilización y coordinación**	**20 días**	**mar 02/11/21**	**lun 29/11/21**	
3	Planificación del programa	5 días	mar 02/11/21	lun 08/11/21	
4	Formación de equipo de implementación del programa	2 días	mar 02/11/21	mié 03/11/21	
5	**Definición y estructura del programa**	**8 días**	**jue 04/11/21**	**lun 15/11/21**	
6	Análisis, diagnóstico, entrevistas y exploración grupal	3 días	jue 04/11/21	lun 08/11/21	4
7	Alcance de a capacitación: Temas y público	5 días	mar 09/11/21	lun 15/11/21	6
8	Definir métricas del programa	3 días	jue 04/11/21	lun 08/11/21	6CC
9	Identificación de riesgos y temas relevantes para inicio del programa.	3 días	mar 09/11/21	jue 11/11/21	6
10	Identificación de recursos, software y sus responsables.	5 días	jue 04/11/21	mié 10/11/21	6CC
11	**Análisis Financiero de la propuesta**	**10 días**	**mar 16/11/21**	**lun 29/11/21**	
12	Estimación de costos.	5 días	mar 16/11/21	lun 22/11/21	5
13	Preparación de Caso de Negocio y Sustentación	3 días	mar 23/11/21	jue 25/11/21	
14	Aprobación por Comité de Inversión	2 días	vie 26/11/21	lun 29/11/21	13
15	**Fase Nro 2: Diseño de la propuesta**	**20 días**	**lun 29/11/21**	**mar 28/12/21**	**2**
16	Plan detallado de implementación del programa.	5 días	lun 29/11/21	lun 06/12/21	
17	Estrategia de comunicación.	5 días	mar 30/11/21	lun 06/12/21	16CC
18	Definición y estructura del programa de formación acorde a las necesidades.	5 días	mar 30/11/21	lun 06/12/21	17CC
19	**Gestión de contrato para servicio de desarrollo de sesiones y material digital**	**15 días**	**mar 07/12/21**	**mar 28/12/21**	
20	Proceso de diagnóstico, entrevista de profundidad, exploración grupal.	10 días	mar 07/12/21	mar 21/12/21	18
21	Diseño de material digital audiovisual para las sesiones síncronas y asíncronas.	5 días	mié 22/12/21	mar 28/12/21	20
22	Diseño de simulacros de phishing.	5 días	mié 22/12/21	mar 28/12/21	20
23	Diseño de Encuestas, evaluaciones y autoevaluaciones.	5 días	mié 22/12/21	mar 28/12/21	22CC



	Nombre de tarea	Duración	Comienzo	Fin	Predecesc
24	**Fase Nro 3: Construcción e Implementación**	**20 días**	**mié 29/12/21**	**mar 25/01/22**	
25	Implementación del programa de concientización en ciber seguridad.	20 días	mié 29/12/21	mar 25/01/22	15
26	Elaboración de mecanismos de capacitación y comunicación con los empleados .	5 días	mié 29/12/21	mar 04/01/22	15
27	**Preparación de material digital para sesiones síncronas y asíncronas**	**20 días**	**mié 29/12/21**	**mar 25/01/22**	
28	Elaboración de material digital audiovisual para las sesiones síncronas y asíncronas.	5 días	mié 29/12/21	mar 04/01/22	15
29	Elaboración de simulacros de phishing.	10 días	mié 29/12/21	mar 11/01/22	15
30	Elaboración de Encuestas.	10 días	mié 05/01/22	mar 18/01/22	28
31	Revisión y pruebas del matearial elaborado.	3 días	mié 19/01/22	vie 21/01/22	29,30
32	Despliegue de sesiones y estructura de capacitación en plataforma LMS.	2 días	lun 24/01/22	mar 25/01/22	31
33	Elaboración de cronograma de sesiones y programación en plataforma de video conferencias.	5 días	mié 19/01/22	mar 25/01/22	25FF
34	**Fase Nro 4: Ejecución y evaluación del programa de concientización en ciber seguridad.**	**60 días**	**mié 26/01/22**	**mar 19/04/22**	
35	Lanzamiento del programa de capacitación.	1 día	mié 26/01/22	mié 26/01/22	33
36	Reservación de agenda para sesiones de aprendizaje.	3 días	jue 27/01/22	lun 31/01/22	35
37	Reservación de agenda para Encuestas y Evaluaciones.	3 días	jue 27/01/22	lun 31/01/22	35
38	Gestión de participación y avance del programa.	56 días	mar 01/02/22	mar 19/04/22	37
39	Gestión de incidentes y problemas que se presenten.	56 días	mar 01/02/22	mar 19/04/22	37
40	Gestión de cambio o ajuste si fuese necesario.	56 días	mar 01/02/22	mar 19/04/22	37
41	**Fase Nro 5: Seguimiento y Monitoreo**	**120 días**	**mar 02/11/21**	**mar 19/04/22**	
42	Revisión y análisis de indicadores durante el proceso	120 días	mar 02/11/21	mar 19/04/22	2CC
43	Revisión y análisis de resultados del programa	55 días	mié 02/02/22	mar 19/04/22	34CC

CAPÍTULO II. INFORME DE LA EXPERIENCIA PILOTO

1. Estrategia operativa de la experiencia piloto

La estrategia de la experiencia piloto se enmarca en un conjunto de acciones que permiten identificar el beneficio y oportunidades de la propuesta de innovación educativa, para el desarrollo y crecimiento del nivel de consciencia en seguridad de información de los empleados de la compañía.

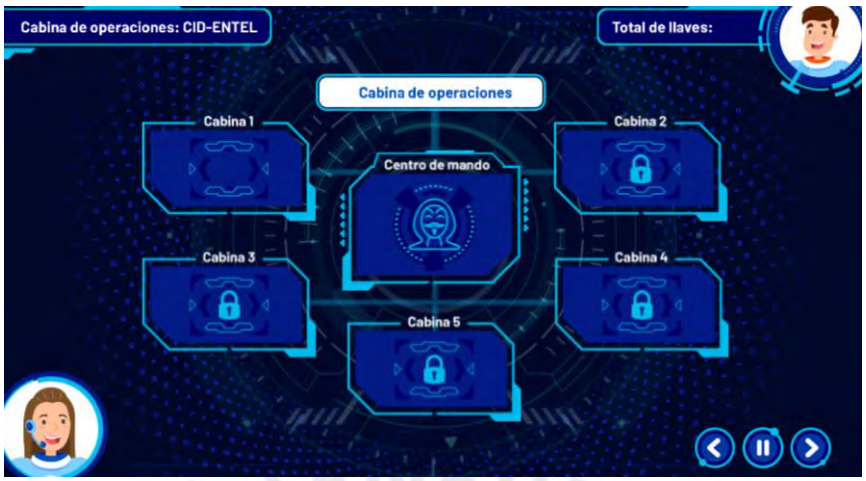
La experiencia piloto plantea introducir una nueva dimensión y método de aprendizaje que incorpore elementos realistas, prácticos y situaciones concretas que generen un pensamiento crítico y un accionar responsable de los empleados en su interacción con internet; y, por lo tanto, promueva el desarrollo y crecimiento de la consciencia en seguridad de información. Para esto, la propuesta planteó un enfoque de formación que motive a los empleados, pero que a la vez les presente experiencias y vivencias reales de vulnerabilidades, amenazas y riesgos de ciber seguridad, y que incluya casos de impactos personales y empresariales de ciber ataques dentro y fuera de la compañía.

La metodología propuesta para esta experiencia piloto considera un proceso de aprendizaje basado en retos y juegos que permita a los empleados no ser solo receptores de información, sino que logre un equilibrio entre sus habilidades digitales y el desafío que plantea el juego con miras a una mayor participación, comprensión, así como altos índices de satisfacción y autoconfianza en los empleados.

La modalidad de gamificación usada fue el escenario de aprendizaje inmersivo “sala de escape” (*escape room*) (Figura 2), que básicamente usa actividades lúdicas en las que los participantes ingresan a una habitación para salir de ella y pasar a una siguiente sala, luego de resolver algunos acertijos o problemas, lo cual aumenta su motivación y mejora su aprendizaje (Borrego et al., 2017). Este enfoque fomenta la continuidad del proceso e incentiva al empleado a avanzar a la siguiente sala o cabina mediante la obtención de la llave requerida. Esta modalidad facilita un entorno de aprendizaje activo, pero también maximiza la motivación y satisfacción, a la vez que favorece el aprendizaje (Gill-Simmen, 2021).

Figura 2.

Enfoque del Curso – Escape Room



Nota: Adaptado del Curso Seguridad de la información – Entel Nov-2021

Según Van Teijlingen y Hundley (2002), el estudio piloto es un elemento crucial en una investigación, ya que permite detectar anticipadamente los puntos en los que podría fracasar el proyecto principal; aunque su realización no garantiza el éxito, sí aumenta sus probabilidades. En ese sentido la prueba piloto se trabajó para identificar puntos de mejora, allanar problemas y resolver impedimentos relacionados con el programa.

La propuesta contempló realizar el piloto durante 7 semanas, considerando un público objetivo de 170 empleados de la vicepresidencia de Tecnología de Información y Operaciones, en sus gerencias de *Operations & Support*, Desarrollo de Sistemas, Seguridad de Información y Gestión de Demanda, cuyo personal cuenta con un nivel similar de competencias digitales, conocimientos y experiencias con seguridad de la información.

Para la experiencia piloto se gestionó la participación de empleados de las áreas de Seguridad de Información y de Capital Humano para facilitar y asegurar su ejecución. Durante la planificación e implementación de la experiencia piloto participaron:

- **Gestor del piloto**: como responsable de articular e integrar todos los componentes, actividades y recursos del piloto; así como de hacer seguimiento y monitoreo durante todo su ciclo de vida.
- **Manager del área de Seguridad de Información**: como patrocinador y promotor de la iniciativa. Ha sido clave para la incorporación de la propuesta en el curso de seguridad de información, en el lanzamiento de la encuesta y en el proceso de simulación de *phishing* o ciber ataque.

- **Manager de Operaciones y Soporte**: como responsable de la participación de los empleados de sus áreas en el curso, en la encuesta y entrevistas del piloto.
- **Coordinador de Seguridad de Información**: como apoyo fundamental en el diseño del curso, validación de las encuestas y ejecución de las simulaciones de *phishing*.
- **Coordinador de Capital Humano**: rol autorizado para gestionar las comunicaciones hacia los empleados. Además, revisó las encuestas solicitando ajustes en el lenguaje y mensaje a enviarse para cumplir con las políticas y cultura de la organización.

2. Objetivos y metas de la experiencia piloto

2.1. Objetivos del piloto

- Validar la efectividad de la metodología, con enfoque de formación basado en gamificación, de la propuesta de innovación para mejorar la consciencia sobre ciber seguridad de los empleados de una compañía de telecomunicaciones de Lima.
- Conocer en profundidad el nivel de conocimiento y capacidades de reacción de los empleados en cuanto a situaciones específicas de ciber seguridad.

2.2. Metas del piloto

La experiencia piloto definió metas para medir y evaluar los resultados de la propuesta de formación en ciber seguridad. Estas metas sirven como puntos de control que ayudan a revisar los criterios de aceptación y cumplimientos de las actividades en las diversas fases.

En cuanto a la meta de atención del piloto, se consideró a 170 empleados de las distintas vicepresidencias de la compañía, quienes en general tienen un nivel similar de formación con las tecnologías digitales, y viven situaciones comunes en su interacción con internet y en las posibilidades de ser víctimas de las ciber amenazas.

Para la meta de implementación, considerando la agenda, políticas y procedimientos del área de Capital Humano de la compañía, se tomó en cuenta una sesión asíncrona, compuesta por un curso con seis temas relacionados con:

- Conceptos de Seguridad de Información.
- Clasificación y Normas.
- Amenazas y Peligros de Ciber Seguridad.
- Conductas de Riesgo en Seguridad de Información.
- Conductas y Acciones positivas en la interacción con Internet.

- Gestión de Incidentes de Seguridad de Información

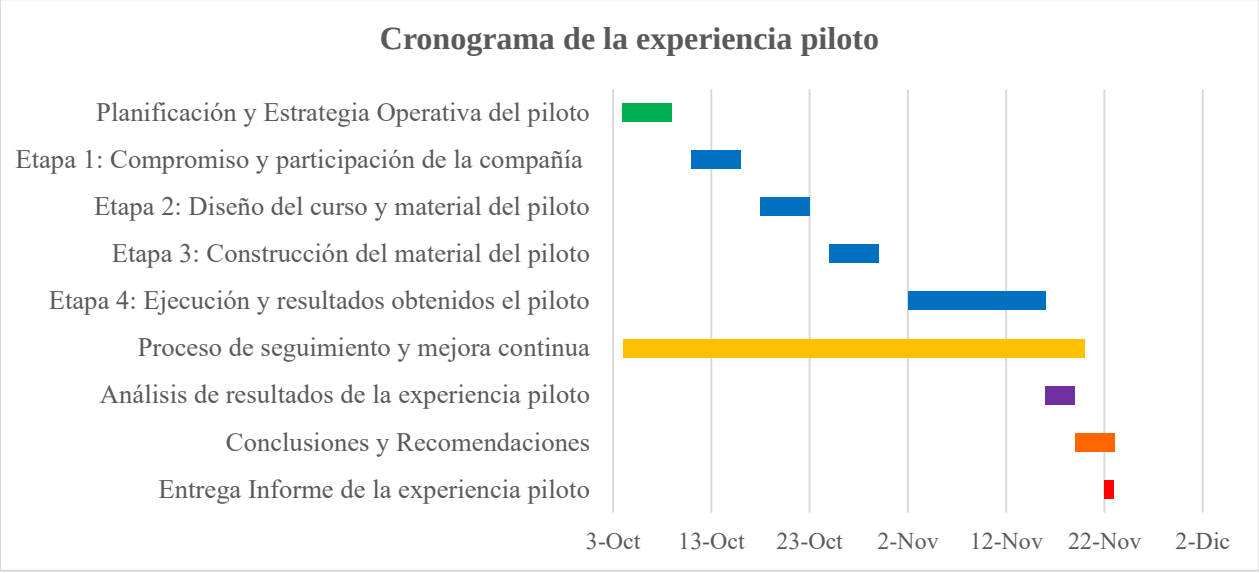
En estos temas, los empleados adquirieron conocimientos de forma autónoma, pero guiados a través de la formulación de casos reales y pruebas cuya resolución les permitía avanzar en el curso. Además, se consideró la implementación de una encuesta para medir el nivel de consciencia en ciber seguridad de los empleados, se desarrolló una entrevista estructurada para una muestra de empleados, con el fin de obtener directamente su forma de pensar sobre el curso y la ciber seguridad, y finalmente una prueba de simulación de un ciber ataque de phishing con ingeniería social.

Por el lado de las metas de producción, se trabajó en el plan de implementación, su cronograma de actividades (Tabla 2), diseño y desarrollo de la encuesta (Anexo 7) y de la entrevista (Anexos 1 y 2), y recomendaciones para el curso de seguridad de información.

3. Cronograma de la experiencia piloto

El trabajo de la experiencia piloto se desarrolló durante siete semanas para su implementación total, la cual incluyó el ciclo de vida completo considerando: la planificación, diseño, desarrollo, ejecución y monitoreo. El cronograma (Tabla 2) de la experiencia piloto a su segundo nivel de actividades es el siguiente:

Tabla 2.
Cronograma de la experiencia piloto



Nota: Plan de actividades para la experiencia piloto

La organización y planificación de la experiencia piloto en una lista y secuencia de actividades permitió ordenar su ejecución identificando interdependencias y prioridades de las diferentes tareas. Así mismo en el cronograma de actividades se identificaron los roles de los participantes que debían participar en cada tarea.

Este cronograma ayudó a tener una visión completa del piloto, permitiendo monitorear su avance, identificar riesgos en su ejecución y supervisar la obtención de sus objetivos.

4. Proceso de ejecución de la experiencia piloto

Esta experiencia piloto se ejecutó como un proyecto de corta duración, con la finalidad de medir la factibilidad e impacto de la propuesta de innovación educativa, la cual plantea incorporar en los cursos de seguridad de información, mejoras y elementos que fomenten que los empleados cuestionen y evalúen las situaciones de amenazas y riesgos en ciber seguridad en su día a día, y que dejen de ser solo receptores de información y pasen a ser parte de la solución o defensa ante vulnerabilidades y ataques de ciber seguridad.

Este proyecto se estructuró en etapas y actividades que permitieron conducirlo y controlarlo de la mejor forma, ya que al dividirlo en componentes más pequeños se pudo hacer un mejor seguimiento y gestionar los riesgos y factores que afectaban al normal progreso, según lo planificado.

En ese sentido, a continuación, se describen las actividades y entregables de cada etapa de la experiencia piloto:

Etapa 1: Compromiso y participación de la compañía en el piloto.

Durante la segunda semana de octubre se realizaron dos reuniones con el manager y un coordinador del área de seguridad de información. En dichas reuniones se presentó el sustento, beneficio y resultados esperados del piloto, para conseguir su compromiso e involucramiento.

El *manager* de seguridad estuvo de acuerdo en unir esfuerzos y ganar sinergias al integrar el planteamiento del piloto a las actividades que su área tenía planificadas para capacitar a los empleados en ciber seguridad. Se definió utilizar un curso sobre seguridad de la información que estaban trabajando, al cual se incorporarían las sugerencias del piloto.

En ese sentido, se trabajó en conjunto para diseñar la solución del piloto, el cual se basó en los siguientes pilares:

- **Visión vinculada a la estrategia del área de seguridad de información**, a partir de la cual se favorece, impulsa y apoya a la capacidad de innovación y nuevas formas de aumentar la consciencia en ciber seguridad, favoreciendo la adaptación flexible y la réplica del curso piloto para extender su metodología y resultados a nivel compañía.
- **Visión en la capacidad de la organización,** para asumir el reto y responsabilidad frente al factor humano como un punto crítico en el resguardo de la seguridad de información; y por lo tanto ser capaz de actuar de forma preventiva reforzando su mentalidad, comportamiento y acciones ante ciber amenazas.
- **Visión en la cultura de aprendizaje en la organización**, para lo cual, la empresa debió dedicar esfuerzo en revisar y replantear la forma cómo las personas estaban aprendiendo y analizar las capacidades actuales que favorecen o limitan la consciencia en ciber seguridad, para fomentar una cultura de aprendizaje que facilite la efectividad del curso.

En resumen, lo más importante de esta etapa fue lograr el compromiso y patrocinio del área de seguridad de información, así como su involucramiento en la ejecución del piloto. Con ello, se definió el equipo base del piloto en el cual estuvieron: el manager de seguridad de información, el manager de operaciones y soporte y un coordinador de seguridad de información. Además, se involucró a un coordinador de Capital Humano para asegurar el cumplimiento de las políticas y procedimientos en comunicaciones y cursos de la compañía.

Etapa 2: Diseño del piloto.

En la tercera semana de octubre se trabajó con el coordinador del área de seguridad de información, revisando los temas del curso, las recomendaciones del piloto y su diseño basado en un entorno de gamificación para aprovechar el potencial de los juegos en el aprendizaje y lograr mejores resultados de los participantes.

El diseño ha considerado aquellas características y fortalezas de la compañía que favorecen la apertura necesaria para aceptar y adoptar esta propuesta de innovación para la capacitación sobre ciber seguridad. El diseño ha contemplado los siguientes tres aspectos:

- **Lo que se espera de los empleados;** para lo cual se tiene en cuenta un enfoque centrado en el factor humano y en sus necesidades, respecto a la cultura y consciencia en seguridad de información. Además, el contenido del curso debía considerar las

necesidades en seguridad de información de los empleados según sus diferentes roles y competencias digitales.

- **La viabilidad para el negocio**; en el sentido que el curso esté alineado a lo que necesita la compañía, en su rol protagónico y decisivo sobre las comunicaciones y tecnología digital, las cuales son transversales a toda la sociedad. Por lo tanto, requiere de un entendimiento profundo sobre la importancia de la ciber seguridad.
- **La factibilidad de su implementación**; considerando la capacidad de la organización, sus líderes y empleados para adoptar un enfoque mejorado de aprendizaje y buenas prácticas en seguridad de información.

En ese sentido, el diseño del curso del piloto incorporó características que lo diferencian de aquellos cursos tradicionales basados solo en teoría y evaluación. Se buscó que no solo genere conflicto cognitivo al empleado, sino que lo motive y lo rete a reflexionar y a lograr un objetivo significativo, más allá de solo completarlo y aprobarlo. Según los procesos y agenda de las capacitaciones de la compañía se determinó que el curso sea asíncrono y que se lanzaría en la plataforma de capacitación de la organización.

En esta etapa también se diseñó la estructura de la encuesta de "percepción y opinión sobre la ciber seguridad" para ser enviada al público objetivo del piloto. Para construir, lanzar y recopilar resultados de la encuesta se definió el uso de la plataforma de *MS Office 365* licenciada para la compañía. Esta encuesta se dividió en cuatro aspectos:

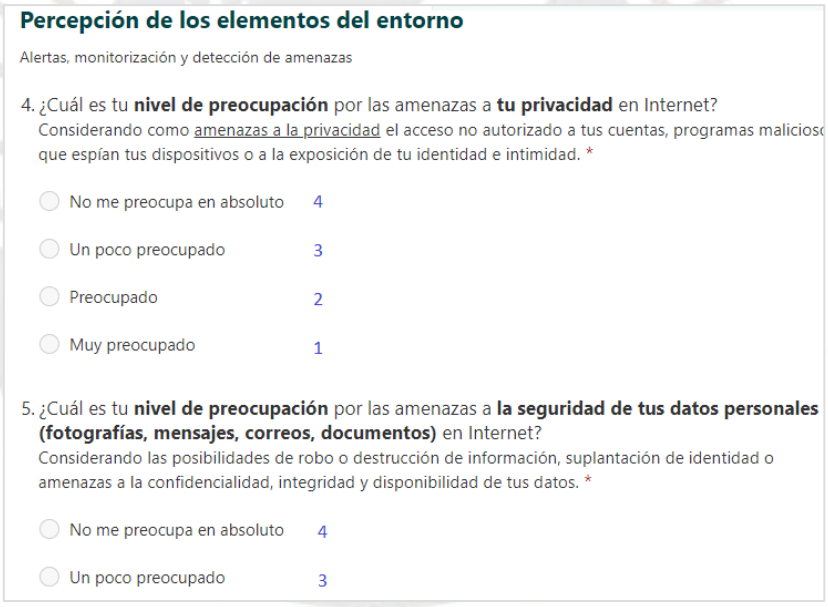
- **Percepción de los elementos del entorno**; preguntas relacionadas con el nivel de percepción de las amenazas de ciber seguridad que sienten los empleados en relación a su privacidad, protección de datos y cibera acoso.
- **Conciencia sobre prácticas de seguridad de información**; preguntas relacionadas con el conocimiento sobre buenas prácticas en seguridad de información, considerando algunas acciones preventivas y otras disuasivas o que el empleado prefiere no tomar acción para evitar riesgos.
- **Conciencia sobre amenazas frecuentes**; preguntas relacionadas con el nivel de conocimiento y consciencia sobre situaciones de ciber amenazas en el día a día de cada empleado.
- **Medidas de protección**; preguntas relacionadas con el conocimiento y uso de herramientas que favorecen la protección ante un intento de ciber ataque.

Por lo tanto, la encuesta no solo fue diseñada para capturar información que ayude a entender el nivel de percepción de ciber seguridad, sino que las preguntas fueron pensadas para que refuercen el análisis, cuestionamiento y formación de los empleados hacia la seguridad de información. Además, las preguntas se prepararon para identificar la existencia de una fuerte consciencia y buenas prácticas de seguridad de información o en su defecto determinar una débil concienciación y un comportamiento negligente ante la interacción en internet.

Se asignó una puntuación de "intensidad de riesgo" a las respuestas de cada pregunta (Figura 3), excepto las preguntas generales. Se consideró al valor uno (1) con un riesgo bajo, y al valor 5 como un riesgo muy alto, de tal forma que permita medir las respuestas en base a un valor numérico y a su equivalente de riesgo. En la figura 2 se puede ver un ejemplo de valores asignados a las opciones de respuesta por pregunta.

Figura 3.

Puntuación por pregunta



Nota: Asignación de puntaje por opción de respuesta de cada pregunta (desde 1 = riesgo hasta 5 = riesgo alto)

A partir de esos valores se calculó el acumulado total de los puntajes por cada pregunta de todas las encuestas respondidas, y ese puntaje se dividió entre el número de encuestados para calcular un índice que representó el nivel de riesgo de la organización o la probabilidad de que los empleados se conviertan en víctimas de un ciber ataque. A continuación, se muestra una tabla con los índices de riesgo compañía definido para este piloto:

Tabla 3.
Índice de riesgo

Índice	Descripción
Bajo (22 - 30)	Los empleados tienen un buen nivel de consciencia sobre las amenazas, aplican buenas prácticas y comportamientos de seguridad de información, y cumplen todas las normas y políticas de seguridad.
Medio (31 - 40)	Los empleados son conscientes de las amenazas, pero pueden no seguir las recomendaciones y buenas prácticas de seguridad del todo.
Moderado (41 - 50)	Los empleados son conscientes de las amenazas y saben que deben seguir las políticas y buenas prácticas, pero necesitan refuerzo y formación sobre una mayor consciencia y políticas de seguridad.
Significativo (51- a más)	Los empleados no conocen o no aplican buenas prácticas de seguridad, no son conscientes de las amenazas existentes ni cumplen las políticas de seguridad de información.

Nota: Índice de riesgo cuyo valor mínimo promedio de la encuesta es 22 puntos y el máximo es sobre los 51 puntos.

Más adelante se comentarán los resultados de esta encuesta realizada a los empleados de la compañía y se explicará el valor calculado del índice de riesgo promedio encontrado.

Por otro lado, se diseñó la estructura de la entrevista a realizarse al manager de seguridad de información y a un grupo de empleados participantes del curso del piloto. Estas entrevistas, con preguntas abiertas, permitieron obtener respuestas amplias sobre la consciencia en seguridad de información, para lo cual se utilizó los siguientes criterios:

- **La gestión de riesgos de seguridad de la información**, en el cual se consideran los esfuerzos necesarios para la protección, detección, respuesta y recuperación en el ámbito de la ciber seguridad. Las preguntas se prepararon para entrevistar al *manager* de seguridad de información sobre la estrategia, acciones y planes que se tienen para reforzar la cultura de seguridad en la empresa.

- **Las responsabilidades de los empleados en el ámbito de seguridad de información**, con preguntas que permiten triangular la información entre los entrevistados para conocer su opinión sobre ciber seguridad, teniendo en cuenta que se trata de personas

que pasaron por el curso del piloto y por lo tanto tienen conocimiento reciente y fresco en materia de ciber seguridad.

Para estas entrevistas se determinó usar *MS Teams y MS Office 365*, también bajo licenciamiento de la organización.

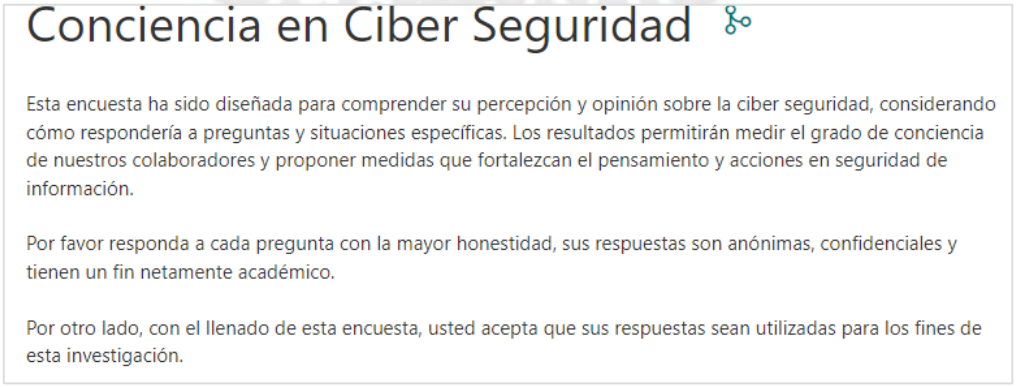
Etapa 3: Construcción de material del piloto.

La construcción del curso lo gestionó el coordinador de seguridad de información y trabajó con un proveedor especialista en herramientas de educación a distancia. Este trabajo implicó desarrollar, programar e implementar los materiales e interfases para las sesiones de aprendizaje. El costo de este proveedor fue asumido por el área de seguridad, ya contaba con presupuesto para realizar un curso de ciber seguridad en el tercer trimestre del año.

Para esta construcción de la encuesta se revisaron varios artículos relacionados a la ciber seguridad y se desarrolló el instrumento buscando que proporcione una comprensión integral sobre la conciencia de los empleados en ciber seguridad. Por otro lado, debido a la política de la compañía y a la estrategia propia del estudio, se decidió no almacenar dato personal alguno para fomentar la libre participación y sinceridad en las respuestas. Esta encuesta fue validada y ajustada con las áreas de seguridad de información y de capital humano. Ambas áreas solicitaron orientar el mensaje, redacción y contenido según las políticas y recomendaciones de la compañía. En la figura 4 se muestra la introducción de la encuesta validada con el equipo de capital humano.

Figura 4.

Introducción de la encuesta



Respecto al desarrollo de las preguntas para las entrevistas, como se indicó en el diseño, se trabajó en dos grupos de preguntas: uno enfocado en el rol de dirección que tiene el manager del área de seguridad de información con consultas relacionadas a la visión, estrategia y

esfuerzo necesario para enfrentar a las amenazas de ciber ataques. Y otro grupo orientado a algunos empleados con preguntas específicas para comprender el nivel de entendimiento y efectividad del curso del piloto. La muestra del público objetivo se basó en los siguientes criterios:

- Tomar 3% de la población que participó del curso, lo que equivale a cinco personas, considerando al menos una de la mitad de las vicepresidencias que son nueve.
- Considerar, dentro de esas 5 personas, a un empleado con cargo de jefatura.
- Seleccionar a 4 empleados (al azar) entre aquellos que participaron del curso. De ellos, considerar a dos varones y dos mujeres. Lamentablemente por temas de política interna (reserva de información) no fue posible identificar a aquellos empleados que dieron clic en la simulación del ciber ataque con phishing.

Los dos grupos de preguntas (Anexos 1 y 2) que se usaron en las entrevistas tuvieron el fin de profundizar y obtener más información y una mayor comprensión sobre la mentalidad de los empleados y sobre las estrategias de capacitación en concientización sobre ciber seguridad y su efectividad en la compañía.

Etapa 4: Ejecución de la experiencia del piloto y resultados obtenidos.

Esta etapa trata específicamente de las actividades relacionadas con la ejecución del curso, el cual inició con la comunicación para a través del correo corporativo de la empresa y con su publicación en la plataforma de entrenamiento (Figura 5 y 6).

Figura 5.

Comunicación y lanzamiento del curso.

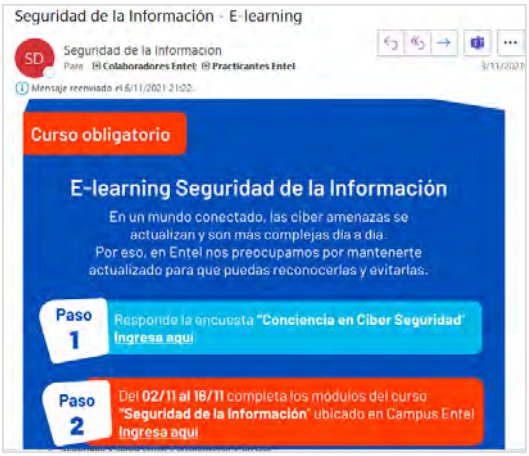
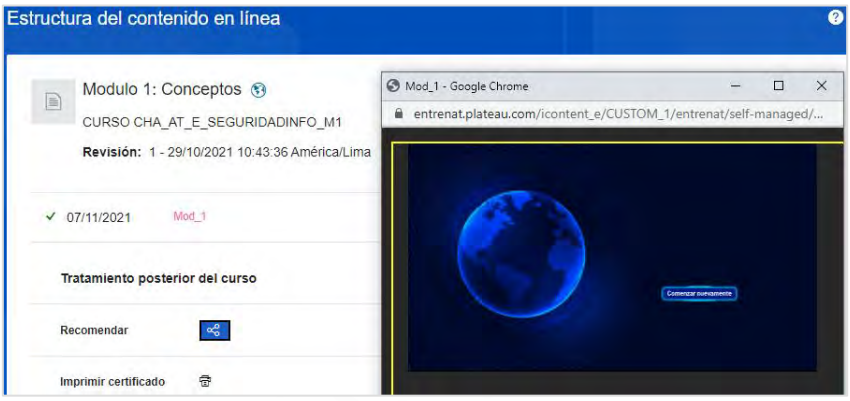


Figura 6.

Publicación en la plataforma de entrenamiento.



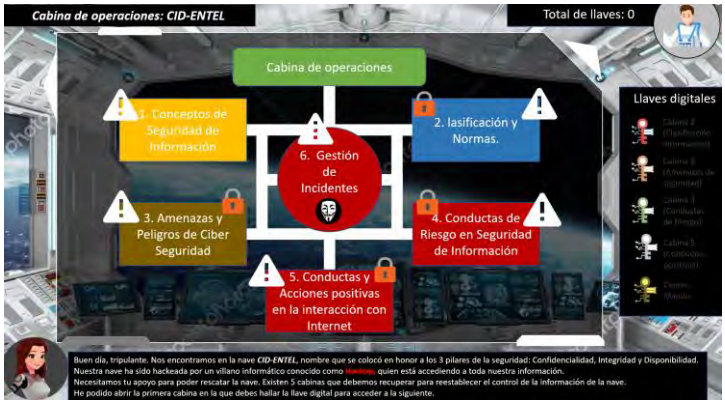
El curso incluyó 6 secciones con conceptos y contenidos relacionados con ciber seguridad, los cuales estaban organizados y ordenados bajo una temática de juego con retos (Figura 7), los que al ser superados permitían avanzar al siguiente nivel o capítulo (llamado "cabina" dentro del curso). Los temas de este curso para la experiencia piloto fueron:

- Conceptos de Seguridad de Información.
- Clasificación y Normas sobre la información.
- Amenazas y Peligros de Ciber Seguridad.
- Conductas de Riesgo en Seguridad de Información.
- Conductas y Acciones positivas en la interacción con Internet.
- Gestión de Incidentes de Seguridad de Información

Cada tema incorporó contenido propio y especializado, así como evaluaciones y retroalimentación que ayudaba al empleado en reforzar lo aprendido.

Figura 7.

Modelo de temas del curso.



Además, este aprendizaje basado en gamificación fomentó que los participantes construyan nuevos conocimientos a partir de conocimientos previos, generó una discusión positiva sobre el enfoque del curso y motivó la participación de los empleados.

Los empleados pudieron decidir el momento en el cual llevaran el curso, para lo cual ingresaron a la plataforma de capacitación y seleccionaron el curso, el cual tenía un diseño atractivo con un enfoque digital y con una usabilidad simple y práctica que guiaba al estudiante. El proceso iba acompañado con retroalimentación y reconocimientos al logro según el avance del estudiante, mostraba el éxito de haber cumplido las misiones y entregaba un certificado. En el anexo 8 se muestran algunas pantallas del curso desarrollado para la experiencia piloto.

Inicialmente se definió y comunicó un tiempo de dos semanas para que los empleados realicen y terminen el curso; pero posteriormente, debido a decisiones y políticas internas de la compañía, el área de capital humano decidió ampliar plazo a los empleados para que realice el curso hasta fin de año. Esta situación obligó al equipo del piloto ajustar el plan y hacer un corte para medir resultados con solo el grupo de empleados que habían terminado el curso.

Por otro lado, debido a que la empresa no definió su posición respecto a compartir información sensible de situaciones y alertas de ciber seguridad ocurridas en la organización, no fue posible incorporar este tipo de información como parte del curso en seguridad de información, lo cual habría sido muy valioso para que los participantes comparen lo aprendido con situaciones reales. En la empresa y en muchos lugares existe recelo de compartir información de problemas de seguridad porque se cree que podría generar un impacto en su imagen. La presente propuesta plantea que las situaciones de ciber seguridad sucedidas en el entorno de la misma empresa deben ser analizadas y asimiladas para su uso y aprovechamiento en beneficio de la consciencia de los empleados. Estos puntos se detallan en la sección de recomendaciones del presente documento.

Así también, junto al lanzamiento del curso se compartió una encuesta con el objetivo de comprender la percepción y opinión sobre la ciber seguridad de los empleados a partir de situaciones específicas relacionadas con este tema. Las respuestas de esta encuesta permitieron cuantificar una puntuación o indicador sobre el nivel de riesgo en la compañía. Además, estos resultados permitieron medir el grado de conciencia de los colaboradores y proponer medidas que fortalezcan el pensamiento y acciones en seguridad de información.

De esta manera, se hizo seguimiento al cumplimiento y participación de los empleados en el curso y en la encuesta. Se identificaron y tuvieron que gestionar riesgos como el cambio o ampliación de fechas dispuesto por el área de capital humano, y también la poca disponibilidad de tiempo de los empleados para las entrevistas. Teniendo en cuenta que se trató

de una iniciativa piloto de corta duración, se verificaba diariamente lo avanzado de forma similar a la ceremonia "*daily*" de la metodología ágil, la cual se centraba en el progreso del trabajo y permitía identificar acciones para asegurar el desarrollo del curso y la participación de los empleados.

Concluidas las dos semanas del curso se realizó un punto de control para identificar a los empleados que realizaron el curso y obtener resultados de la encuesta. A partir de este punto se procedió a realizar un análisis de lo ejecutado y se identificó a la muestra de empleados para invitarlos a participar de las entrevistas. Estas entrevistas se realizaron durante la tercera semana de noviembre con su respectiva autorización, se transcribieron y luego se utilizó una matriz para analizar las respuestas e ideas planteadas en dichas entrevistas.

Etapa 5: Evaluación del Piloto.

De acuerdo con Waithera y Wanyoike (2015), el monitoreo permite realizar una recopilación y análisis continuos para determinar si un proyecto está logrando el progreso hacia las metas establecidas. En el caso del piloto, la evaluación implicó dos momentos con enfoques distintos: uno a lo largo de todo el piloto evaluando y monitoreando puntos de mejora y otro, al terminar el piloto con el análisis de los resultados de la encuesta y entrevista, además se analizó la evolución de la curva de tendencia de simulación de phishing.

- **Puntos de mejoras durante la ejecución del piloto.** Se evidenciaron situaciones y decisiones externas al piloto que afectaron directamente a su planificación y que deben ser tomadas en cuenta y gestionadas de cara a la aplicación completa de la propuesta. Entre estos factores se pueden mencionar los siguientes:

    - Al inicio del piloto se acordó la participación y disponibilidad de los empleados, tanto para la gestión del piloto, como para ser parte del curso, encuestas y entrevistas. En la práctica hubo bastante interés y apoyo, pero la disponibilidad de las personas estuvo limitada. Para implementar la propuesta completa se deberá contar con el apoyo y compromiso de la alta dirección y la inclusión de este programa como parte del plan estratégico de la empresa.
    - Existen políticas y lineamientos de la compañía que deben ser considerados como el tipo de lenguaje y la forma de comunicarse con los empleados. Si bien se debe usar una correcta redacción, el lenguaje debe mostrar cercanía usando

la segunda persona. Además, las encuestas y entrevistas deben ser cortas y puntuales. Para la propuesta de innovación completa se debe considerar este punto.

- Hay cambios en decisiones y prioridades que provienen del área de Capital Humano como el mover la fecha de fin del curso. En el caso del piloto, al tener un tiempo muy corto, estos cambios le afectaron directamente. Para la propuesta completa deberían manejarse holguras de tiempo que permitan manejar y controlar los impactos por este tipo de cambios.

- **Retrospectiva de la ejecución y resultados del piloto.** Al finalizar el piloto se analizaron los resultados del curso, la encuesta y las entrevistas. A partir de estos resultados se puede apreciar que existe interés y preocupación de los empleados por temas relacionados con la ciber seguridad, pero que hay un déficit a nivel de buenas prácticas y de conocimientos de impactos cercanos y reales. En la siguiente sección se presentan los resultados obtenidos en el piloto.

5. Resultados

Se identificaron los factores contextuales que afectaron el desarrollo de la experiencia piloto, los cuales son parte de lecciones aprendidas que serán integradas en la planificación de la propuesta de innovación con el fin de que el programa sea sostenible y escalable. Estos factores externos son:

- Cambio de prioridades de la dirección y del área de capital humano de la empresa, quienes por necesidades y dependencias decidieron centrar los esfuerzos de los empleados en actividades distintas al programa propuesto.
- Distracción de los empleados por otras actividades, responsabilidades y personas que los alejan del objetivo del curso.
- Distinto nivel de conocimiento digital entre los empleados que facilita realizar el curso a unos más que a otros.

El área de seguridad de información está trabajando en integrar transversalmente los conceptos, necesidades y objetivos en ciber seguridad, para lo cual ha definido el rol llamado oficial de seguridad de información empresarial, BISO por sus siglas en inglés (*Business*

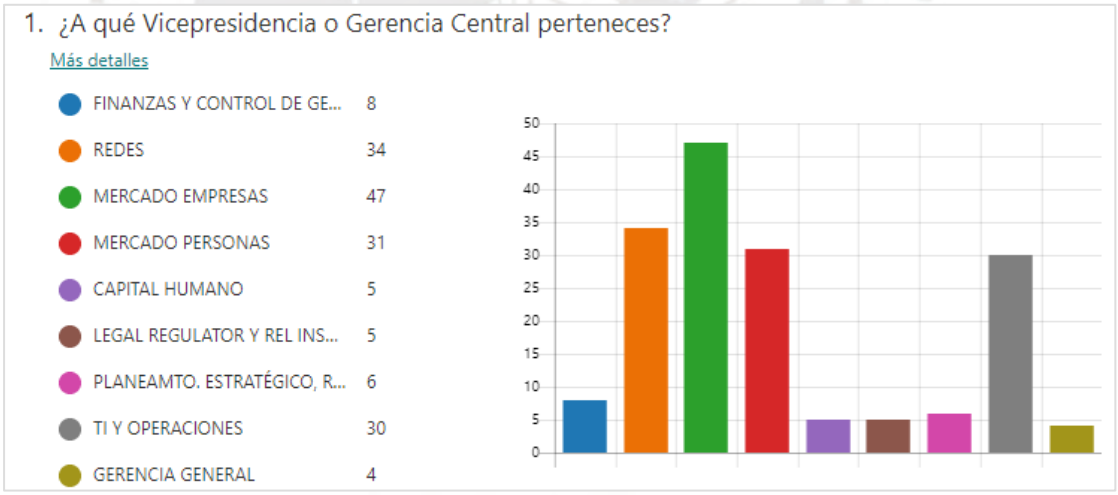
Information Security Officer), el cual es el responsable de liderar la seguridad en una unidad específica de la compañía, sirviendo de enlace entre los intereses de la empresa y de seguridad. Este trabajo no es parte de la presente propuesta, pero aportará significativamente a identificar y gestionar los factores externos que pueden afectar su efectividad.

Como se indicó en la etapa de diseño, se implementó una encuesta para medir el conocimiento y nivel de riesgo en seguridad de información de los empleados. Además, paralelamente a la ejecución del curso se realizaron las entrevistas preparadas para conocer el nivel de gestión de riesgos y de responsabilidad sobre ciber seguridad de los empleados.

La encuesta fue respondida por 170 empleados (figura 8), con lo cual se calculó la intensidad de riesgo de la compañía con una puntuación promedio de 42.76 (según tabla de índice de riesgo de la tabla 3). De acuerdo con ese puntaje se puede decir que la compañía tiene un nivel de riesgo "Moderado"; es decir que los empleados son conscientes de las amenazas y de las políticas, pero necesitan refuerzo y formación sobre una mayor consciencia y políticas de seguridad de información.

Figura 8.

Participación de los empleados en la encuesta.



Nota: Distribución de empleados por vicepresidencia o gerencia que respondieron la encuesta.

Respecto al riesgo en ciber seguridad en la compañía, en la entrevista con el *manager* del área de seguridad de información indicó que la digitalización vertiginosa a raíz de la pandemia y el tener a los empleados trabajando en forma remota han ampliado las brechas entre la seguridad y riesgos informáticos. Además, que la ignorancia de los empleados sobre las ciber amenazas es uno de los puntos de mayor preocupación, y que es importante considerar

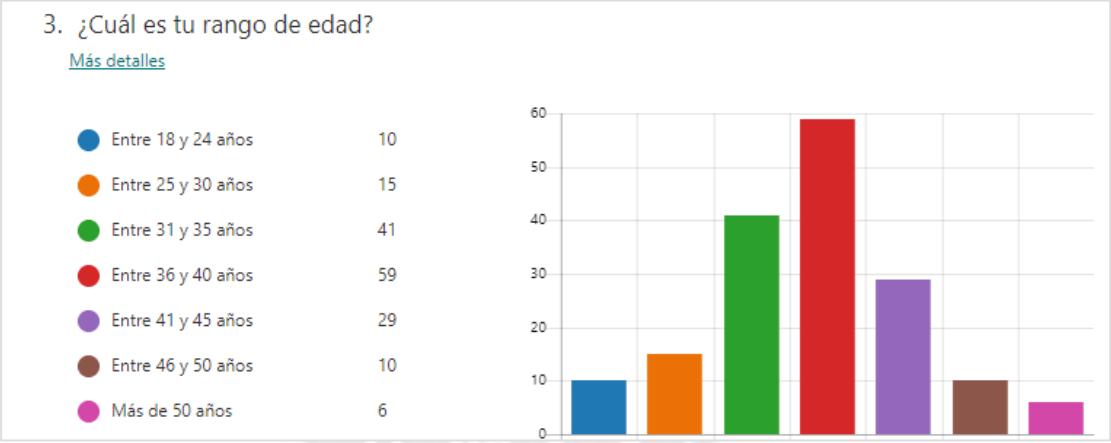
la cultura de las personas, ya que en general vivimos en una sociedad que evalúa poco el riesgo y recién reacciona cuando ocurre algún problema.

Sin embargo, los empleados entrevistados coinciden en su preocupación por las amenazas existentes en su interacción en internet, aunque algunos confunden lo que son vulnerabilidades, amenazas y riesgos en ciber seguridad. Por lo tanto, es importante reforzar este tema para que los empleados sean conscientes de los peligros.

En cuanto al tema de segmentación y distribución de resultados de la encuesta por rango de edades (Figura 9) se puede apreciar que la mayoría de los empleados están entre las generaciones "X" y "Y" (*millennials*), lo cual implica una combinación interesante, dado que ambas generaciones se ven inmersas en la tecnología y los riesgos que implica, pero la generación "X" ha tenido que desarrollarse y crecer en un entorno no tan avanzado como lo hizo la generación "Y"; sin embargo ambas generaciones enfrentan las mismas amenazas en ciber seguridad y deben adoptar las mismas buenas prácticas.

Figura 9.

Rango de edades de la población muestra.

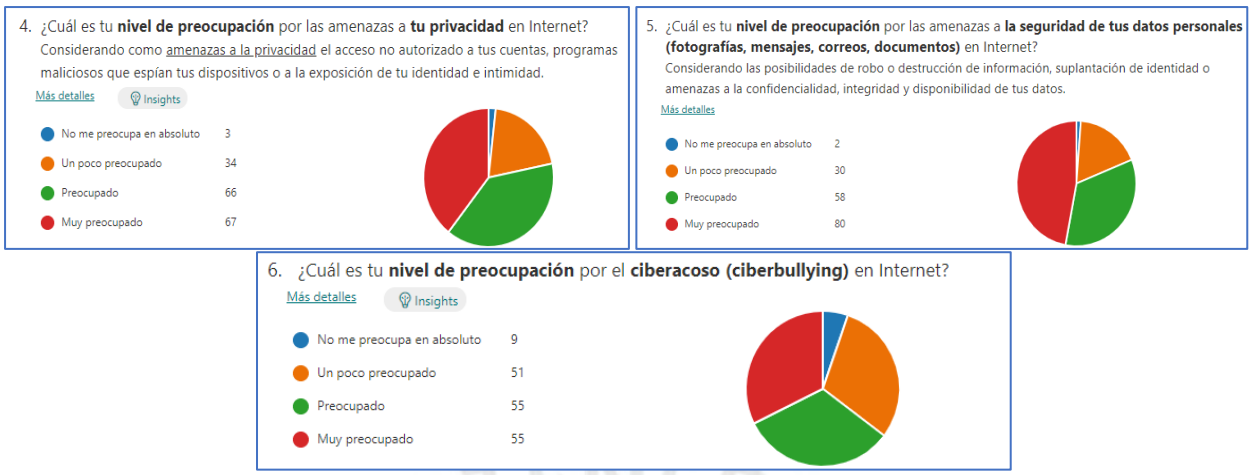


Nota: Distribución de empleados participantes de la encuesta, agrupados por rango de edades.

Un tema relevante e inquietante que resalta de la encuesta es que entre el 18% y 35% de empleados se preocupan poco o nada sobre las amenazas de ciber ataques (Figura 10), por más que en la entrevista si comentan que les interesa y tienen preocupación por la ciber seguridad, aunque eso no se observa en la encuesta. Esto refleja falta de trabajo en la formación de consciencia en ciber seguridad.

Figura 10.

Nivel de preocupación por ciber amenazas.



Nota: Resultados de preocupación de la privacidad, datos personales y ciber acoso.

Asimismo, el líder de seguridad comenta que se debe desmitificar lo que es seguridad de información, para que se le deje de ver como un tema netamente técnico o con un alcance inquisitorio, y se le considere como un agente aliado que tiene una preocupación genuina por los ciber riesgos. Además, agrega que es necesario identificar el nivel de madurez de las áreas de la compañía para entregarles el detalle de formación que necesitan, y que vaya según su madurez en ciber seguridad.

Por su lado, los empleados entrevistados tienen comentarios favorables sobre la eficacia de la formación en ciber seguridad, pero el nivel de influencia que sienten del curso del piloto es variado, ya que algunos comentan que ya conocen y hacen uso de las buenas prácticas y otros empleados dicen que les ha servido para reforzar su conocimiento. Esto demuestra que es recomendable segmentar las capacitaciones de acuerdo con el nivel de manejo de seguridad de información de cada empleado.

El conocimiento y experiencia de los empleados entrevistados se refleja en parte de la encuesta sobre buenas prácticas de ciber seguridad, pero no todos aplican buenas prácticas (Anexo 3 y 4). El 81% está familiarizado con formas avanzadas de autenticación e inicio de sesión, pero más del 40% no lo usa para asegurar sus cuentas personales. Más preocupante aún es que el 52% utiliza la misma contraseña para cuentas de aplicativos o dispositivos diferentes, y solo el 34% realiza cambio de sus contraseñas de manera frecuente, lo cual los vuelve más vulnerables a un ciber ataque. Con estos resultados vemos que es importante reforzar la consciencia y hábitos de los empleados en ciber seguridad.

Adicionalmente, en la misma línea de buenas prácticas, un alto porcentaje (81%) ha identificado situaciones en los que recibió correo *phishing* (Anexo 5) e indican que lo

eliminaron, reportaron o ignoraron; sin embargo, un 24% comenta que inconscientemente pudo haber dado clic a un enlace o botón de un correo electrónico sospechoso, lo cual se convierte en una amenaza latente ante un posible ciber ataque. Además, un 72% respondió que usa software antivirus actualizado en sus equipos personales, ya sean computadores personales o laptops; pero el 66% no usa software antivirus en sus equipos móviles como *smartphones* o *tablets* (Anexo 6). Esto indica que conocen la importancia de un antivirus, pero no lo ven como prioritario en sus equipos móviles, lo cual constituye otra amenaza.

Ese tipo de acciones imprudentes es explicado a partir de la entrevista a los empleados cuando mencionan que cada vez se hace más difícil identificar una amenaza y que es necesario contar capacitaciones frecuentes sobre ciber seguridad para estar más preparados y alertas. Por su lado el *manager* de seguridad añade que la ciber seguridad es necesaria porque los riesgos existen, pero su enfoque debe ser de cercanía a los empleados y generar valor a la compañía.

Finalmente, en la última sección de la encuesta, se dio libertad con una última pregunta para que los empleados puedan comentar sobre la importancia de la seguridad de información en la compañía. Se revisaron todas las respuestas de las que se desprende la preocupación de los empleados por la protección y riesgo de la información, ya sea personal, de la compañía o de sus clientes. Además, se hizo un análisis básico de texto y estadísticas de frecuencia de palabras (Figura 11), lo cual permitió identificar las palabras clave más usadas en las respuestas.

Figura 11.

Nube de palabras a partir de respuestas a pregunta abierta.

Nota: Imagen que representa a las palabras clave con mayor frecuencia en la respuesta abierta de la encuesta.

Podemos ver que, tanto el manager de seguridad de información, como los empleados muestran una preocupación auténtica por los riesgos en ciber seguridad, y coinciden en la

importancia de contar con programa de concientización y buenas prácticas. En ese sentido, el líder de seguridad aclara que es indispensable medir la eficacia de los programas de ciber seguridad, pero que los indicadores existentes aún son insuficientes para determinar el nivel de madurez de la cultura de la compañía. Sin embargo, esta propuesta de innovación será contemplada en los siguientes planes estratégicos.

Por el momento, una forma de medir el nivel de riesgo en ciber seguridad es realizar pruebas de ciber ataque o simulación de *phishing* lo cual estaba contemplado dentro del piloto una vez que todos los participantes terminaran el curso. Sin embargo, como la compañía decidió ampliar los plazos para que los empleados puedan terminar el curso, se tuvo que ejecutar la prueba phishing en paralelo al curso.

Figura 12.

Procesos de simulación de ciber ataque phishing

Nota: Adaptado de Seguridad de Información Entel 2021.

Por más que el curso y la simulación de phishing aún están en progreso, se puede apreciar (Figura 12) que hasta el momento hay 8% de empleados que han sido víctimas de la prueba de ciber ataque. Se puede esperar que al final del proceso esa cantidad se acerque al 10% u 11% similar a las pruebas de meses anteriores. Por lo tanto, la formación y desarrollo de consciencia sobre ciber seguridad es importante, pero debe realizarse buscando nuevas formas y alternativas.

Conclusiones

En base a la experiencia del piloto, al problema y objetivos de la propuesta y a los resultados obtenidos del curso, encuesta y entrevistas se plantean las siguientes conclusiones:

- **La participación como factor crítico de éxito para el programa de innovación.** Se confirma que el nivel de involucramiento y participación de la dirección y empleados de la compañía es fundamental para el desarrollo y cumplimiento de los objetivos del programa. Los directivos de la compañía deben apropiarse de esta iniciativa y priorizarla a fin de garantizar la participación de los empleados.

- **Desarrollar un programa de consciencia para una cultura de seguridad de información.** Los resultados del piloto demuestran que la compañía requiere un programa de formación de consciencia sobre ciber seguridad para los empleados. En general los empleados tienen buen nivel de conocimientos sobre riesgos, pero también hay actitudes que ponen en peligro a la seguridad de la información en la compañía.

- **Distinto nivel de conocimientos y capacidad de acción en ciber seguridad.** Los empleados tienen distinto nivel de capacidades digitales y de reacción ante ciber amenazas, por lo cual necesitan distinto nivel de capacitación en consciencia de seguridad de información.

- **Generar reflexión sobre riesgos e impactos de ser víctima de un ciber ataque.** Para lo cual se debe romper el paradigma del temor que tienen algunas personas de compartir información real de impactos a personas, organizaciones externas e incluso a la misma compañía, ya que lo consideran riesgoso o creen que puede incentivar más vulnerabilidades.

El piloto ha evidenciado que en la empresa hay una preocupación real por la seguridad de información, y que es crucial desarrollar, en los empleados, una consciencia sobre ciber seguridad para que piensen y actúen positivamente en su interacción en internet. En ese sentido la presente propuesta de innovación educativa plantea sensibilizar a los empleados para que adecúen su comportamiento hacia una cultura de ciber seguridad saludable y responsable.

Recomendaciones

En base a la ejecución del piloto y considerando el diseño de la propuesta de innovación educativa, se plantea una serie de recomendaciones de acuerdo con los siguientes aspectos:

Diseño de la propuesta

- **Incorporar en el plan estratégico de la compañía** la propuesta de innovación educativa sobre ciber seguridad, con lo cual se logra el patrocinio de los directivos, así como el compromiso de los líderes para participar y promover que los empleados participen y le den la importancia debida.

- **Transparencia y apertura total** en la comunicación de casos e impactos reales de ciber ataques. Para esto la compañía debe comprender que compartir información de situaciones reales, e incluirlas en la formación a sus empleados, es una ventaja ya que el conocimiento de ese tipo de situaciones les permitirá un mayor razonamiento y análisis.

- **Integrar en el programa de formación** elementos que permitan generar experiencias significativas para un mayor desarrollo de habilidades y consciencia en ciber seguridad:

    - **Escenarios y casuísticas** de ciber amenazas para que los empleados realicen análisis, discusión y propuestas de cómo enfrentar cada caso.
    - **Inclusión de casos emblemáticos a nivel mundial,** para evidenciar que las ciber amenazas y vulnerabilidades se dan en cualquier lugar o empresa.
    - **Casos reales ocurridos en la compañía;** para mostrar situaciones que se dieron dentro de la organización, y así ver que la empresa y sus empleados no están libres de los ciber ataques.
    - **Resultados de simulaciones de ciber ataques por phishing** realizados por la compañía, para evidenciar la necesidad de reforzar la consciencia en seguridad.

Ejecución de la propuesta

- **Desarrollar y actualizar los cursos que motiven a los empleados.** Debido a los buenos comentarios sobre el curso del piloto y a su estrategia de usar métodos de gamificación, es recomendable seguir trabajando en esa misma línea, pero incorporando información adecuada según el nivel en ciber seguridad de los empleados.

- **Identificar y segmentar las necesidades de formación de los empleados.** Se debe tomar como base realizar encuestas y entrevistas sobre consciencia en ciber seguridad que permitan tabular respuestas para realizar analítica y determinar el contenido y nivel de formación que requiere cada rol de empleado. También es importante las preguntas abiertas para que los empleados se sientan libres de comentar sobre situaciones específicas de ciber amenazas.

- **Realizar seguimiento y mejora continua durante la ejecución de la propuesta.** Esto incluye llevar un control frecuente del avance de la propuesta, hacer seguimiento a las actividades y progreso del curso, identificar y gestionar los riesgos que aparezcan, obtener retroalimentación y realizar ajustes necesarios al programa

Por lo tanto, la formación en seguridad de información debe realizarse con nuevos enfoques, nuevas ideas e innovando para lograr activar en los empleados una consciencia plena y responsabilidad para tomar decisiones adecuadas y minimizar la posibilidad de ser víctima de un ciber ataque.

Referencias

Abroshan, H., Devos, J., Poels, G. y Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access*, 44928-44949. https://ieeexplore.ieee.org/document/9380285

Alazri, A. (2015) The awareness of social engineering in information revolution: Techniques and challenges. *10th International Conference for Internet Technology and Secured Transactions (ICITST)*. 198-201, doi: 10.1109/ICITST.2015.7412088.

Albladi S. y Weir G. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*. https://hcis-journal.springeropen.com/articles/10.1186/s13673-018-0128-7

Albladi, S. y Weir, G. (2020). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity 3 (7) pp. 1-19. https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00047-5

Aldawood, H. y Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62-68, doi: 10.1109/TALE.2018.8615162.

Aldawood, H. y Skiner, G. (2020). Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access* 8, pp. 67321-67329. https://ieeexplore.ieee.org/abstract/document/9049417

Almeida, F. (2012). Web 2.0 Technologies and Social Networking Security Fears in Enterprises. *International Journal of Advanced Computer Science and Applications 3*(2), 152 - 156. https://arxiv.org/abs/1204.1824

Alotaibi, A.y Alsuwat, E. (2020). A study on social engineering attacks: phishing attack. *International Journal of Recent advances in Physics.,* 6374-6380. https://www.researchgate.net/publication/348606991_a_study_on_social_engineering_attacks_phishing_attack

Alzahrani, A. (2020). Coronavirus Social Engineering Attacks: Issues and Recommendations. *International Journal of Advanced Computer Science and Applications 11* (5), 154 - 161.

https://thesai.org/Publications/ViewPaper?Volume=11&Issue=5&Code=IJACSA&SerialNo=23

Andress, J. y Leary, M. (2016). *Building a Practical Information Security Program.* https://searchsecurity.techtarget.com/feature/Building-a-Practical-Information-Security-Program

Behar, J. (2019 de Jun de 2019). Protecting against Cybersecurity's Weakest Link: The Human Factor. Obtenido de Cyber defense magazine: https://www.cyberdefensemagazine.com/protecting-against-cybersecuritys-weakest-link-the-human-factor/

Borrego, C., Fernández, C., Blanes, I. y Robles, S. (2017). Room escape at class: Escape games activities to facilitate the motivation and learning in computer science. *Journal of Technology and Science Education*, 162-171. http://www.jotse.org/index.php/jotse/article/view/247

Brandtzaeg, P. y Heim, J. (2009). Why People Use Social Media Sites. *Computer Science* Volume 5621, 143-152. https://doi.org/10.1007/978-3-642-02774-1_16

Breda, F., Barbosa, H. y Morais, T. (2017). Social engineering and cyber security. *INTED2017 Proceeding: International Technology, Education and Development Conference*, 4204-4211.https://www.researchgate.net/publication/315351300_social_engineering_and_cyber_security

Check Point Research. (2020). Check Point Research. Obtenido de The 2020 Cyber Security Report: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

Cybersecurity Ventures (2020). *The 2020 Official Annual Cybercrime Report*. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report

ENTEL. (2020). *Información Corporativa Entel.* https://informacioncorporativa.entel.cl/nuestra-compania

ENTEL Corp. (2020). Entel Corp. Estado de la ciberseguridad Informe 2020: https://www.entel.cl/corporaciones/notas/pdf/Informe-Ciberseguridad-2020.pdf

Erbschloe, M. (2019). Social Engineering: Hacking Systems, Nations, and Societies. Florida: CRC Press. https://docer.com.ar/doc/nxs51sx

Ferreira, A. (2018). "Why Ransomware Needs A Human Touch". *2018 International Carnahan Conference on Security Technology (ICCST)*, 1-5, doi: 10.1109 / CCST.2018.8585650.

Fortinet. (2021). Threat Intelligence Insider Latin America. https://www.fortiguardthreatinsider.com/

Frumento, E., Puricelli, R., Freschi, F., Ariu, D., Weiss, N., Dambra, C., . . . Pachego, B. (2016). The role of Social Engineering in evolution of attacks. https://www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf

Gill-Simmen, L. (2021). Get me outta here! Motivating online learners with digital escape rooms. Journal of Learning Development in Higher Education, 1-9. https://doi.org/10.47408/jldhe.vi22.782

Herrmann, D. y Pridöhl., H. (2020). Basic Concepts and Models of Cybersecurity. En M. Christen, G. B., & L. M., The Ethics of Cybersecurity. *The International Library of Ethics, Law and Technology*, 11-41. Zürich, Switzerland: Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-29053-5_2

Hewitt, K. (2021). What is a Cybersecurity Vulnerability? Definition and Types. SecurityScorecard: https://securityscorecard.com/blog/what-is-a-cybersecurity-vulnerability

IBM. (2014). IBM Security Services 2014 - *Cyber Security Intelligence Index*. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

Isachenko, N. (2018). The role of information and informational and communication technologies in modern society. *Utopia y Praxis Latinoamericana* 23, 361-367. https://zenodo.org/record/1512122

Matulewska, A. E. y Ciszek, H. S. (2019). A case study of the productivity of the prefix cyber- in English and Greek legal languages. *Studies in Logic, Grammar and Rhetoric*, 58(71), 35–58. https://www.sciendo.com/pdf/10.2478/slgr-2019-0016

Morfaw, J. (2014). Fundamentals of project sustainability. Paper presented at PMI® Global Congress 2014-North America, Phoenix, AZ. Newtown Square, PA: Project Management Institute. https://www.pmi.org/learning/library/fundamentals-project-sustainability-9369

Mouton, F., Malan, M., Leenen, L. y Venter, H. (2014) Social engineering attack framework. *Information Security for South Africa*, 1-9, doi: 10.1109/ISSA.2014.6950510

Mukhalalati, B. A. y Taylor, A. (2019). Adult Learning Theories in Context: A Quick Guide for Healthcare Professional Educators. Journal of Medical Education and Curricular Development. https://doi.org/10.1177/2382120519840332

Ngak, C. (2012). CBS NEWS. https://www.cbsnews.com/news/social-media-a-news-source-and-tool-during-superstorm-sandy/

Pashentsev, D., Zaloilo, M., Ivanyuk, O. y Alimova, D. (2019). Digital technologies and society Directions of interaction. *Espacios* 40, 1-6. https://www.revistaespacios.com/a19v40n42/19404202.html

Rogers, S. (2019). *Forbes*. https://www.forbes.com/sites/solrogers/2019/10/15/the-role-of-technology-in-the-evolution-of-communication/

RSA (2016). *Organizations Need to Determine Their 'Cyber Risk Appetite'*. https://www.rsa.com/en-us/company/news/organizations-need-to-determine-their-cyber-risk-appetite

Salahdine, F. y Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, 2-17. https://www.mdpi.com/1999-5903/11/4/89

Sammons, J. y Cross, M. (2017). Cybercrime. *The Basics of Cyber Safety*. https://www.sciencedirect.com/science/article/pii/B978012416650900005X

Secureworks. (2017). Cyber Threat Basics, Types of Threats, Intelligence & Best Practices. Secureworks: https://www.secureworks.com/blog/cyber-threat-basics

Shih, G. (2012). https://www.reuters.com/article/internet-eeuu-sandy-twitter-idLTASIE8A104K20121102

Siadatia, H., Nguyena, T., Gupta, P., Jakobsson, M. y Memona, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security*, 14-28. https://www.sciencedirect.com/science/article/pii/S016740481630116X

Sociology Guide. (2020). Impact of Technology Change on Society. *Sociology Guide*. https://www.sociologyguide.com/social-change/impact-of-technology-change.php

Sonowal, G. y Kuppusamy, K. (2020). PhiDMA – A phishing detection model with multi-filter approach. *Journal of King Saud University - Computer and Information Sciences*, 99-112. http://dx.doi.org/10.1016/j.jksuci.2017.07.005

Tayouri, D. (2015). The human factor in the social media security –combining education and technology to reduce social engineering risks and damages. *Procedia Manufacturing* 3, 1096 – 1100. https://www.sciencedirect.com/science/article/pii/S2351978915001821

Van Teijlingen, E. y Hundley, V. (2002). The Importance of Pilot Studies. Nursing Standard, 33-36, https://www.researchgate.net/publication/11173521_The_Importance_of_Pilot_Studies

Waithera, S. y Wanyoike, D. (2015). Influence of project monitoring and evaluation on performance of youth funded agribusiness projects in Bahati sub-county, Nakuru, Kenya. *International Journal of Economics, Commerce and Management, United*

Kingdom. 375-394. https://1library.net/title/influence-project-monitoring-evaluation-performance-funded-agribusiness-projects

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *Journal of Supercomputing*, 2643-2664. https://link.springer.com/article/10.1007%2Fs11227-019-03028-9

Wieners, E. (2019). Proposals for NGOs. Obtenido de Developing a Sustainability Plan in a Project Proposal: https://proposalsforngos.com/sustainability-plan-project-proposal

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F. y Basım, N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*. DOI:10.1080/08874417.2020.1712269

Anexos

Anexo 1. Entrevista al manager del área de seguridad de información.

Nro.	Pregunta de la entrevista	Objetivo
1	¿Cuál es su opinión sobre la situación que viven los empleados en su interacción con internet? ¿Cuáles considera que son los mayores riesgos?	Conocer la mirada que el manager tiene sobre la situación de ciber seguridad actual.
2	Los empleados son la primera línea de defensa ante un ciber ataque. ¿Qué acciones están tomando para para que los empleados comprendan el papel que desempeñan como responsables y aliados de la seguridad de información en la compañía?	Identificar las acciones y planes para reforzar una cultura de seguridad de información en la empresa.
3	¿Cuáles son algunas pautas importantes para considerar al implementar un programa de capacitación y refuerzo de consciencia en ciber seguridad para empleados?	Conocer los criterios usados para implementar un programa de concienciación sobre ciber seguridad.
4	¿Cómo miden la eficacia de los programas de concientización sobre ciber seguridad?	Investigar sobre la estrategia utilizada para medir el impacto de los programas de concienciación sobre ciber seguridad.
5	¿Considera que la seguridad de información es algo ineludible u obligatorio en la compañía o puede servir como herramienta que ayude al crecimiento del negocio y su reputación?	Entender el nivel de importancia y de beneficios que se da a la seguridad de información a nivel empresa.

Anexo 2. Preguntas para entrevistas a empleados participantes del piloto.

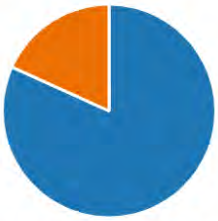
Nro.	Pregunta de la entrevista	Objetivo
1	¿Qué riesgos en línea conoce? En su día a día.	Descubrir la capacidad del empleado para identificar los diferentes riesgos online
2	¿Cree que el curso de capacitación de Seguridad, como programa de concientización en los empleados es eficaz? ¿En qué medida?	Conocer la opinión de los empleados sobre los beneficios del programa de concienciación sobre ciber seguridad.
3	¿Cómo influyó la capacitación (curso) en ciber seguridad en su comportamiento en línea?	Investigar cómo el programa de concienciación sobre ciber seguridad influyó en el comportamiento de los empleados en línea.
4	¿Cuáles son las limitaciones del programa de concienciación sobre ciberseguridad? ¿Qué le falta?	Investigar las limitaciones del programa de concienciación sobre ciber seguridad.
5	Las empresas enfrentan muchas amenazas de ciber ataques. ¿Qué tan difícil es identificar y responder correctamente a dichas amenazas?	Conocer la opinión de los empleados sobre la dificultad que sienten en reaccionar correctamente ante una amenaza de ciber ataque.

Anexo 3. Resultados sobre buenas prácticas en autenticación

7. ¿Estás familiarizado con el método de **autenticación de 2 o más factores**, el cual requiere que proporciones dos o más factores de verificación para obtener acceso a tus cuentas?

Más detalles

Sí	139
No	31



8. ¿Usas algún tipo de autenticación con dos o mas factores en **tus cuentas personales** (No laborales)?

Más detalles Insights

Sí	97
No	42

Anexo 4. Resultados sobre buenas prácticas en el uso de contraseñas

9. ¿Tienes una **contraseña común** que usas en más de una cuenta, dispositivo o sistema?

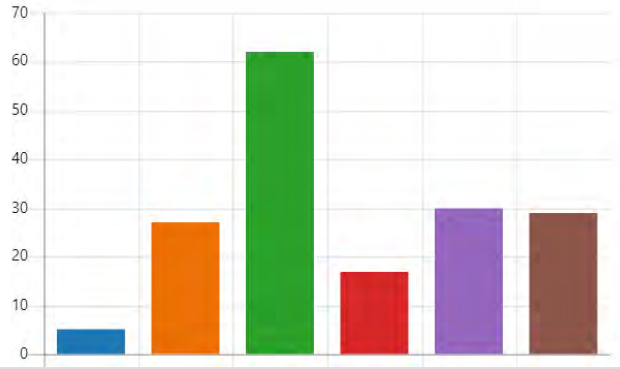
Más detalles Insights

Sí	89
No	81

10. ¿Con qué frecuencia realizas el **cambio de contraseña de tus cuentas personales** asociadas a dispositivos informáticos o redes sociales?

Más detalles

Nunca	5
Casi Nunca	27
Ocasionalmente	62
Cada año	17
Cada semestre	30
Cada trimestre	29



12. ¿En tus cuentas personales utilizas **contraseñas complejas?**
Es decir aquellas con una extensión considerable y que incluyan símbolos, mayúsculas, minúsculas y números.

Más detalles

Nunca	2
Casi Nunca	9
Ocasionalmente	28
Casi siempre	64
Siempre	67

Anexo 5. Consciencia sobre ciber amenazas frecuentes.

15. ¿Has detectado o **identificado correos phishing** (mensaje fraudulento que parece legítimo) en los últimos meses?

Más detalles Insights

Sí	138
No	32

16. Si la respuesta anterior fue afirmativa; ¿Qué hiciste con el correo phishing detectado?

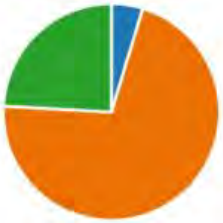
Más detalles

Lo abrí	0
Lo eliminé	64
Lo reporté	60
Lo dejé ahí, solo lo ignoré	14

17. ¿Alguna vez has dado **clic a un enlace o botón** de un correo electrónico sospechoso o que no esperabas recibir?

Más detalles Insights

Sí	8
No	121
Quizás, sin darme cuenta.	41

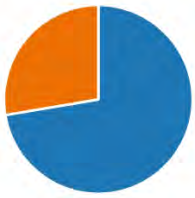


Anexo 6. Protección ante ciber amenazas: Antivirus y Control Parental

19. ¿Utilizas un **antivirus actualizado** en tu PC o laptop **personal**?

Más detalles Insights

Sí	123
No	47



20. ¿Utilizas un **antivirus actualizado** en tu smartphone o tablet **personal**?

Más detalles Insights

Sí	58
No	112

21. Si tienes hijos que usan dispositivos conectados a internet (smartphone, tablet, consolas de videojuegos) ¿utilizas **software de bloqueo de control parental**?

Más detalles

Sí	39
No	50
No tengo hijos que usen disp...	81

Anexo 7. Encuesta sobre percepción y opinión en ciber seguridad

Conciencia en Ciber Seguridad

Esta encuesta ha sido diseñada para comprender su percepción y opinión sobre la ciber seguridad, considerando cómo responderían a preguntas y situaciones específicas. Los resultados permitirán medir el grado de conciencia de nuestros colaboradores y proponer medidas que fortalezcan el pensamiento y acciones en seguridad de información.

Por favor responda a cada pregunta con la mayor honestidad, sus respuestas son anónimas, confidenciales y tienen un fin netamente académico.

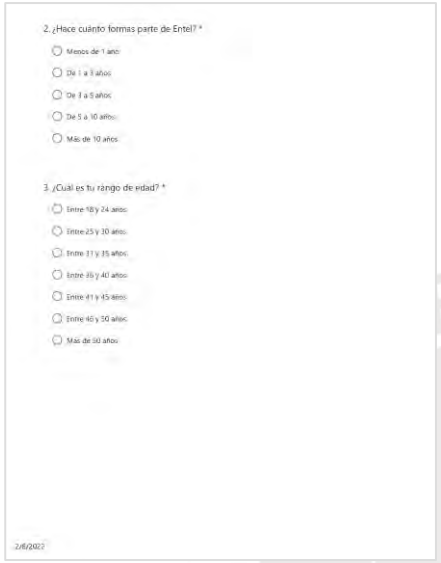
Por otro lado, con el llenado de esta encuesta, usted acepta que sus respuestas sean utilizadas para los fines de esta investigación.

* Obligatorio

Información general

1. ¿A qué Vicepresidencia o Gerencia Central perteneces? *
- FINANZAS Y CONTROL DE GESTION
- RHOET
- MERCADO EMPRESAS
- MERCADO PERSONAS
- CAPITAL HUMANO
- LEGAL REGULATORY INSTITUC
- PLANEAMTO. ESTRATÉGICO, RIESGOS Y MEG. MAYOR
- TI Y OPERACIONES
- GERENCIA GENERAL

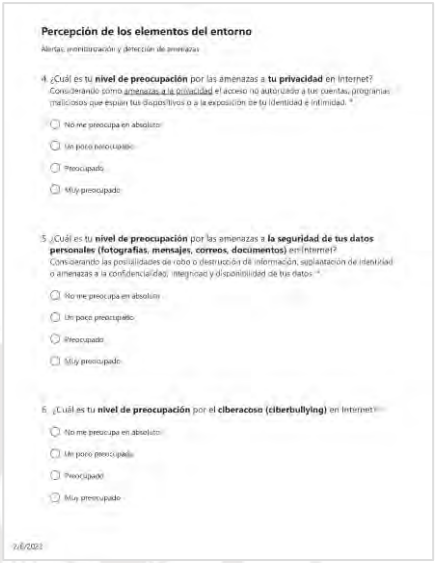
2/6/2023



2. ¿Hace cuánto formas parte de Entel? *
- Menos de 1 año
- De 1 a 3 años
- De 3 a 5 años
- De 5 a 10 años
- Más de 10 años

3. ¿Cuál es tu rango de edad? *
- Entre 18 y 24 años
- Entre 25 y 30 años
- Entre 31 y 35 años
- Entre 36 y 40 años
- Entre 41 y 45 años
- Entre 46 y 50 años
- Más de 50 años

2/6/2023



Percepción de los elementos del entorno

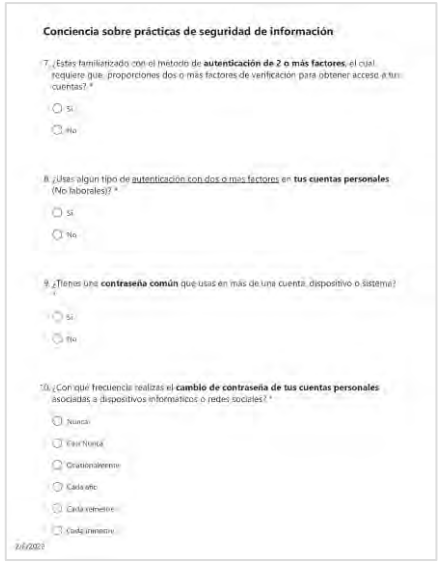
Alertas, sensibilización y detección de amenazas

4. ¿Cuál es tu **nivel de preocupación** por las amenazas a **tu privacidad** en Internet?
Considerando como amenazas a la privacidad el acceso no autorizado a tus cuentas, programas maliciosos que espían tus dispositivos o a la exposición de tu identidad e intimidad. *
- No me preocupa en absoluto
- Un poco preocupado
- Preocupado
- Muy preocupado

5. ¿Cuál es tu **nivel de preocupación** por las amenazas a **la seguridad de tus datos personales (fotografías, mensajes, correos, documentos)** en Internet?
Considerando las posibilidades de robo o destrucción de información, suplantación de identidad o amenazas a la confidencialidad, integridad y disponibilidad de tus datos. *
- No me preocupa en absoluto
- Un poco preocupado
- Preocupado
- Muy preocupado

6. ¿Cuál es tu **nivel de preocupación** por el **ciberacoso (ciberbullying)** en Internet? *
- No me preocupa en absoluto
- Un poco preocupado
- Preocupado
- Muy preocupado

2/6/2023



Conciencia sobre prácticas de seguridad de información

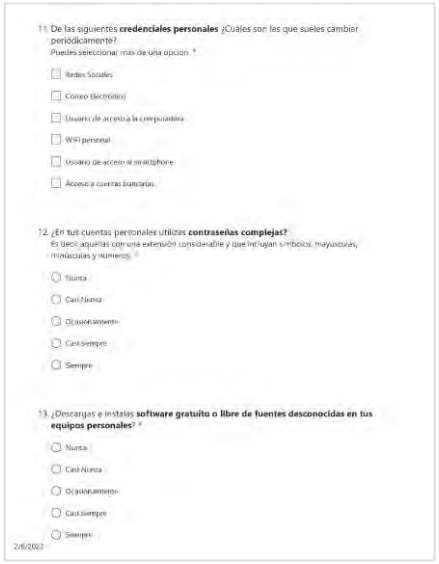
7. ¿Estás familiarizado con el método de **autenticación de 2 o más factores**, el cual requiere que proporciones dos o más factores de verificación para obtener acceso a tus cuentas? *
- Si
- No

8. ¿Usas algún tipo de autenticación con dos o más factores en **tus cuentas personales** (No laborales)? *
- Si
- No

9. ¿Tienes una **contraseña común** que usas en más de una cuenta, dispositivo o sistema? *
- Si
- No

10. ¿Con qué frecuencia realizas el **cambio de contraseña de tus cuentas personales** asociadas a dispositivos informáticos o redes sociales? *
- Nunca
- Casi Nunca
- Ocasionalmente
- Cada año
- Cada semestre
- Cada trimestre

2/6/2023

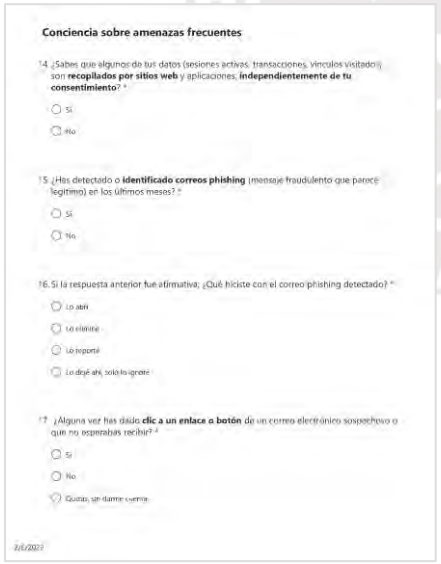


11. De las siguientes **credenciales personales** ¿Cuáles son las que sueles cambiar periódicamente?
Puedes seleccionar más de una opción. *
- Redes Sociales
- Correo Electrónico
- Usuario de acceso a la computadora
- WIFI personal
- Usuario de acceso al smartphone
- Acceso a cuentas bancarias

12. ¿En tus cuentas personales utilizas **contraseñas complejas**?
Es decir, aquellas con una extensión considerable y que incluyan símbolos, mayúsculas, minúsculas y números. *
- Nunca
- Casi Nunca
- Ocasionalmente
- Casi Siempre
- Siempre

13. ¿Descargas e instalas **software gratuito o libre de fuentes desconocidas en tus equipos personales**? *
- Nunca
- Casi Nunca
- Ocasionalmente
- Casi Siempre
- Siempre

2/6/2023



Conciencia sobre amenazas frecuentes

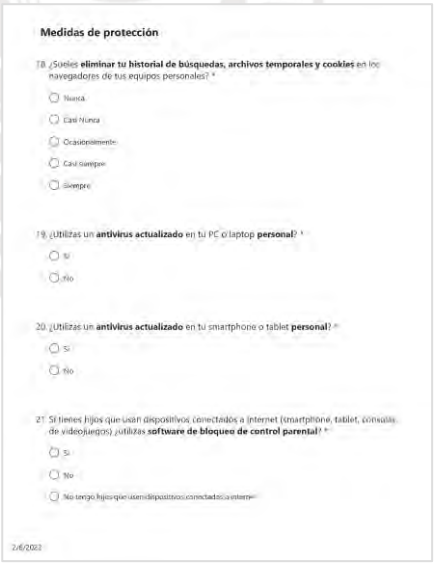
14. ¿Sabes que algunos de tus datos (sesiones activas, transacciones, vínculos visitados) son **recopilados por sitios web** y aplicaciones, **independientemente de tu consentimiento**? *
- Si
- No

15. ¿Has detectado o **identificado correos phishing** (mensaje fraudulento que parece legítimo) en los últimos meses? *
- Si
- No

16. Si la respuesta anterior fue afirmativa; ¿Qué hiciste con el correo phishing detectado? *
- Lo abrí
- Lo elimine
- Lo reporté
- Lo dejé ahí, solo lo ignoré

17. ¿Alguna vez has dado **clic a un enlace o botón** de un correo electrónico sospechoso o que no esperabas recibir? *
- Si
- No
- Quizás, sin darme cuenta

2/6/2023



Medidas de protección

18. ¿Sueles **eliminar tu historial de búsquedas, archivos temporales y cookies** en los navegadores de tus equipos personales? *
- Nunca
- Casi Nunca
- Ocasionalmente
- Casi Siempre
- Siempre

19. ¿Utilizas un **antivirus actualizado** en tu PC o laptop **personal**? *
- Si
- No

20. ¿Utilizas un **antivirus actualizado** en tu smartphone o tablet **personal**? *
- Si
- No

21. Si tienes hijos que usan dispositivos conectados a Internet (smartphone, tablet, consolas de videojuegos) ¿utilizas **software de bloqueo de control parental**? *
- Si
- No
- No tengo hijos que usen dispositivos conectados a internet

2/6/2023

Pregunta abierta

Por favor tome un par de minutos en responder la siguiente pregunta libre.

22. **¿Por qué crees que es importante preocuparte por la seguridad de la información en la compañía?**

2/6/2023

Anexo 8. Algunas pantallas del curso de la experiencia piloto