# LA FORMACIÓN A USUARIOS FINALES COMO MÉTODO DE FORTALECIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Pablo Cesar Gutiérrez Trujillo.
Pablocgutierrez1@gmail.com.com.com.com.
Universidad Piloto de Colombia

***Abstract*—This document proposes a series of strategies and methodologies that will allow the area in charge of the design, implementation and continuous improvement of the Information Security Management System (ISMS) for any company, to carry out a series of trainings and knowledge transfer framed in the training to end users, with the aim of publicizing and strengthening the ISMS in the organization.**

***Resumen*—**Este documento plantea una serie de estrategias y metodologías, que permitirán, al área encargada del diseño, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) para cualquier empresa, realizar una serie de entrenamientos y transferencia de conocimiento enmarcadas en la formación a los usuarios finales, con el objetivo de dar a conocer y fortalecer el SGSI en la organización.

***Palabras Clave* — Estrategia de aprendizaje, metodologías, ataques, usuario final, ingeniería social, estadísticas.**

## I. INTRODUCCIÓN

El documento inicia mostrando una serie de estadísticas que permiten al lector enmarcarse en la actualidad de los ataques cibernéticos en el país y la región, buscando crear un contexto sobre la importancia que tienen los sistemas de gestión de seguridad de la información. A continuación, se abordan las definiciones exactas de los diferentes tipos de ataque evidenciados al inicio del documento, con el fin de reforzar el conocimiento del lector, posteriormente se realiza la descripción de una estrategia de aprendizaje, incluyendo definiciones y buenas prácticas, que una empresa puede implementar para lograr el objetivo de formación.

Finalmente, se plantea una metodología para implementar una estrategia de aprendizaje enfocada en crear conciencia sobre la importancia del SGSI y las buenas prácticas de seguridad a los usuarios finales de la organización.

## II. ESTADÍSTICAS DE ATAQUES CIBERNÉTICOS EN COLOMBIA Y LATINOAMÉRICA

Según un informe dado a conocer por la firma de ciberseguridad Digiware, se presentaron 198 millones de ataques cibernéticos en Colombia de agosto del 2016 al mismo mes del 2017, de acuerdo con la compañía, en promedio se registran 542.465 incidentes, y el impacto que los delitos informáticos han generado en Colombia asciende a los 6179 millones de dólares en pérdidas [1].

Según Digiware, el sector del país más afectado por los delitos informáticos es el financiero con 214.600 ataques por día, seguido el sector de las telecomunicaciones con 138.329 ataques, mientras que el gobierno con 83.756 y la industria 51.263 los siguen. “Pero los usuarios son, sin duda, el blanco preferido de los cibercriminales. Ellos buscan suplantar la identidad para cometer robos, hurtar sus datos bancarios, instalar software malicioso en sus dispositivos o secuestrar sus archivos para luego pedir el pago de un rescate, modalidad conocida como ransomware” [1].

“Lo más común es intentar atacar al usuario. En las empresas hay diferentes tipos de controles, pero si logras ‘hackear’ al usuario (a través de engaños en correos, por ejemplo), todos esos millones de inversión en seguridad informática se pierden”, dice Andrés Galindo, experto en ciberseguridad de Digiware [1].

En un contexto regional, el informe divulgado por Digiware indica que el país más afectado por este tipo de ataques es Brasil con un 25,13% de impacto, seguido por México con 15,53% de impacto, Venezuela con 11,91% y Argentina con 9,63% [2].

El coronel Fredy Bautista, jefe del grupo de delitos informáticos de la policía nacional, aseguró que a diario se reciben denuncias de fraudes digitales por montos cercanos a los 120 millones de pesos. Según Bautista, los fraudes BEC, *Business Email Compromise* de su sigla en inglés, o Correos corporativos comprometidos en español, son los fraudes que más afectan a las empresas en el país, además los ciudadanos se ven diariamente afectados por ataques como fraudes financieros, suplantación de identidad y secuestro de información. Teniendo en cuenta lo anterior, se detalla que en

Colombia la clonación de tarjetas de crédito sucede en un 30% en cajeros electrónicos y 70% en plataformas de comercio que no cuentan con los suficientes procesos de verificación [2].

Por otra parte, la Organización de Estados Americanos (OEA), el Ministerio de Tecnologías de la Información y Comunicaciones (Min TIC) y el Banco Interamericano de Desarrollo (BID), revelaron un estudio titulado "Impacto de los incidentes de seguridad digital en Colombia 2017", en el que indican que el 51% de las medianas empresas y el 63% de las grandes empresas en Colombia sufrieron incidentes digitales durante el 2016. El reporte tuvo la participación de 1.098 organizaciones de las cuales 515 eran empresas del sector real y 583 fueron entidades del sector público, en el mismo se advierte de la poca asignación presupuestal en temas de seguridad digital, ya que se invierte menos del 1% de las ventas e inversiones. Además, señala que solo el 37% de las empresas que participaron en la medición se sienten preparadas para afrontar un episodio de seguridad informática. También indica que, al analizar distintos sectores económicos, el 52% de las empresas pertenecientes a la industria y el 59% de las entidades de orden nacional han identificado incidentes digitales, mientras que el 70% de las microempresas aseguran no haber identificado eventualidades de este tipo [3].

Entre las amenazas cibernéticas más comunes presentadas en las empresas en 2016, se encuentran el malware y el phishing. Dentro del sector de servicios, el 50% notó un aumento en los ataques de malware, 47% de phishing, 39% de ataques basados en web y 18% de ataques de denegación de servicio. En el sector comercio, se reportó un incremento en el malware de un 53%, un 41% de aumento en el phishing y un 21% notó un incremento tanto en ataques basados en web, como en ataques de denegación de servicio. En el sector industria, el 67% señaló que hubo un crecimiento en la gravedad de los ataques basados en web y el malware; y el 59% dijo que se presentó un aumento en los ataques de phishing. La carencia de personal con dedicación exclusiva al área, el poco presupuesto y la falta de conciencia de los empleados, son los principales factores que, según las organizaciones entrevistadas, afectan la capacidad de abordar la seguridad digital, de igual manera, en cuanto a la asignación de recursos para afrontar esta problemática, se observó que la mediana del presupuesto fue aproximadamente 0,3% de las ventas en 2016, mientras que en las entidades públicas el valor es de 0.05%. Cabe resaltar que la mayor parte del presupuesto fue asignado para plataformas y medios tecnológicos, y hay una menor inversión en temas como capacitación y concientización de los empleados y funcionarios. Igualmente, muchas de las organizaciones no estiman el costo de los incidentes digitales, pues el 79% de las empresas afirmaron que no contaban con ningún costo estimado, mientras que el 85% de las entidades públicas dijeron que tampoco hacen este tipo de estimación [3].

Con el informe revelado por la compañía de ciberseguridad ESET denominado "ESET Security Report Latinoamérica 2017", se puede identificar que con un 56% la infección por código malicioso es la preocupación más grande en las empresas de la región, especialmente con el grado de sofisticación que tiene el malware y el retorno económico que genera, y teniendo en cuenta el protagonismo que están tomando los ransomware. De este informe se toma la figura 1, donde se evidencias las diferentes preocupaciones en ciberseguridad que tienen las empresas de acuerdo con su tamaño [4].

| Empresa | Año | Malware | Fraude | Vulnerabilidad de software y sistemas | Ataque de denegacion de servicios | Phishing | Acceso indebido a la información |
|---|---|---|---|---|---|---|---|
| Grandes | 2015 | 52% | 38% | 60% | 37% | 34% | 46% |
| | 2016 | 55% | 29% | 53% | 28% | 28% | 36% |
| Medianas | 2015 | 60% | 35% | 60% | 32% | 34% | 50% |
| | 2016 | 56% | 25% | 49% | 21% | 27% | 38% |
| Pequeñas | 2015 | 55% | 39% | 58% | 26% | 28% | 45% |
| | 2016 | 57% | 32% | 51% | 15% | 22% | 30% |

Fig. 1 – Preocupaciones en ciberseguridad, según el tamaño de las empresas para Latinoamérica.

Sebastián Brenner, estratega de ciberseguridad de Symantec Latinoamérica, inicia un informe sobre las amenazas que serán más relevantes en el 2018, de la siguiente manera: "Prepárese para un año ajetreado. Incidentes como el ataque WannaCry, que afectó más de 200 mil computadores en todo el mundo en mayo del 2017, son solo el calentamiento de un nuevo año de malware más virulento y ataques DDoS. Los delincuentes están preparados para intensificar sus ataques contra los millones de dispositivos que ahora están conectados a Internet de las Cosas, tanto en oficinas como en hogares". A continuación, daremos un vistazo a 10 de las amenazas mencionadas en el informe de Symantec Corporation, una de las principales empresas de seguridad informática del mundo.

**1)** ***Las criptomonedas estarán en la mira:***

Los delincuentes no se enfocarán en atacar la tecnología blockchain, la plataforma sobre la cual se apoyan monedas como el bitcoin, sino que se concentrarán en comprometer los intercambios de monedas y las carteras de monedas de los usuarios, ya que estos son los objetivos más fáciles y los que ofrecen los más altos rendimientos.

**2)** ***Los delincuentes usarán inteligencia artificial y aprendizaje automático:***

Hasta ahora, la inteligencia artificial (AI) y el aprendizaje automático (Machine Learning) se habían usado como mecanismos de protección y detección. Pero esto cambiará en el 2018, ya que los ciberdelincuentes usarán AI y ML para realizar ataques. "Ellos utilizarán la inteligencia artificial para atacar y explorar las redes de las víctimas", dice Symantec.

**3)** ***Se masificarán los ataques a la cadena de suministro:***

Las grandes empresas suelen tener redes muy seguras, pero sus proveedores, contratistas y clientes no necesariamente, y esto lo aprovecharán los delincuentes. "Con información públicamente disponible sobre tecnología, proveedores, contratistas, asociaciones y personal clave, los ciberdelincuentes pueden encontrar y atacar los enlaces débiles en la cadena de suministro. Tras una serie de ataques de alto perfil y exitosos en los dos años anteriores, los ciberdelincuentes se centrarán en este método en el 2018", dice Symantec.

La compañía agrega que estos ataques son altamente efectivos y explica que "utilizan la inteligencia humana para comprometer los eslabones más débiles de la cadena, así como

implantes de malware en la etapa de fabricación o distribución a través del compromiso o la coacción".

**4)** ***Se disparará el malware sin archivos y con archivos ligeros:***

El malware sin archivos y con poca carga de archivos representará una amenaza significativa, que crecerá de forma importante en el 2018. Según Symantec, los delincuentes atacan organizaciones que carecen de preparación contra estas amenazas, que tienen menos indicadores de compromiso y comportamientos complejos e inconexos, lo cual hace que sean más difíciles de detener y defender.

**5)** ***Seguridad en software en la nube seguirá siendo un reto:***

La adopción de SaaS (Software como Servicio) continúa creciendo rápidamente, a medida que las organizaciones se embarcan en proyectos de transformación digital para impulsar la agilidad empresarial. Pero esto presenta muchos desafíos de seguridad, según Symantec, ya que el control de acceso, el control de los datos, el comportamiento del usuario y el cifrado de los datos varían significativamente entre las aplicaciones de SaaS. Las organizaciones continuarán luchando con esto en el 2018.

**6)** ***Riesgos en infraestructura como servicio:***

La Infraestructura como Servicio (IaaS) ha cambiado la forma en que las organizaciones ejecutan sus operaciones, al ofrecer enormes beneficios en agilidad, escalabilidad, innovación y seguridad. Pero también presenta riesgos, con errores simples que pueden exponer una gran cantidad de datos y acabar con sistemas completos, según Symantec.

"Aunque los controles de seguridad sobre la capa IaaS son responsabilidad del cliente, los controles tradicionales no se adaptan bien a estos nuevos entornos basados en la nube, lo que genera confusión, errores y problemas de diseño al aplicar controles ineficaces o inapropiados, mientras que los controles nuevos se ignoran. Esto dará lugar a más infracciones durante el 2018, a medida que las organizaciones luchan por cambiar sus programas de seguridad para que sean efectivos en IaaS", dice el informe de Symantec.

**7)** ***Los troyanos financieros seguirán siendo muy rentables:***

Symantec explica que los troyanos financieros están entre las primeras piezas de malware monetizadas por los ciberdelincuentes. Desde sus inicios como simples herramientas de recolección de datos financieros, han evolucionado a esquemas de ataque avanzados que apuntan a múltiples bancos, envían transacciones ocultas y esconden sus pistas. Además, son altamente rentables para los delincuentes.

Según Symantec, el paso a la banca móvil basada en aplicaciones ha reducido parte de la efectividad, pero los ciberdelincuentes están moviendo sus ataques rápidamente a estas plataformas. Y se espera que las ganancias de los delincuentes con los troyanos financieros crezcan, lo que les brindará mayores utilidades incluso que el ransomware.

**8)** ***Ransomware, ahora contra dispositivos caseros:***

El ransomware es uno de los flagelos de internet hoy en día. Este es un tipo de ataque con malware en el que el computador o dispositivo de la víctima se bloquea o se encripta toda su información, hasta que esta pague un rescate. Symantec dice que una mentalidad de "fiebre del oro" ha empujado a más delincuentes a distribuir ransomware, y además ellos ahora están buscando expandir su alcance aprovechando el aumento masivo de costosos dispositivos domésticos conectados.

"Por lo general, los usuarios no son conscientes de las amenazas contra los smart TV, los juguetes inteligentes y otros dispositivos inteligentes, lo que los convierte en un objetivo atractivo para los ciberdelincuentes", dice Symantec.

**9)** ***Los dispositivos IoT serán secuestrados y utilizados en ataques DDoS.***

En el 2017 se vieron ataques DDoS masivos usando cientos de miles de dispositivos del Internet de las Cosas (IoT) comprometidos en los hogares y lugares de trabajo. Según Symantec, esto seguirá pasando en el 2018, pues los delincuentes explotarán las pobres configuraciones de seguridad y el manejo personal laxo de los dispositivos IoT hogareños. "Además, las entradas y los sensores de estos equipos también serán secuestrados, y los atacantes alimentarán audio, video u otras entradas falsas para hacer que estos aparatos hagan lo que ellos quieren", dice el informe.

**10)** ***Los dispositivos LoT darán acceso persistente a las redes domésticas:***

Los dispositivos de IoT en el hogar serán usados por los delincuentes para proporcionar acceso persistente a la red de la víctima, según Symantec. "Los usuarios domésticos no suelen consideran la seguridad de sus dispositivos de IoT en el hogar; por eso, dejan la configuración predeterminada y no la actualizan, como sí lo hacen con sus computadores. El acceso persistente significa que, no importa cuántas veces una víctima limpie su máquina o proteja su computador, el atacante siempre tendrá una puerta trasera en la red de la víctima y los sistemas a los que se conecta", explica Symantec. [5]

## III. DEFINICIÓN DE LOS DIFERENTES TIPOS DE ATAQUES

Realizando un análisis a los datos suministrados en el capítulo anterior, podemos determinar que la mayoría de las amenazas que afectan a Colombia y Latinoamérica, están concentradas en dos tipos: la ingeniería social y el Malware. Para poder entender este tipo de ataques a fondo, a continuación, se realiza una breve descripción de cada uno de ellos, y se enumerarán sus subclases más conocidas.

1) ***Ingeniería social****:*

Es un tipo de ataque que se basa en la manipulación psicológica, es decir, se intenta lograr que las demás personas hagan las cosas que no quiere que hagan, por ejemplo, adular a tu jefe o empleador para conseguir un aumento de salario en tu trabajo. En el contexto del crimen cibernético, es ampliamente descrito como un método no técnico utilizado por los cibercriminales para obtener información, realizar fraudes u obtener acceso ilegítimo a los equipos de las víctimas. La ingeniería social se basa en la interacción humana y está impulsada por personas que usan el engaño con el fin de violar los procedimientos de seguridad que normalmente se deberían haber seguido [6]. La mayoría de las veces, los ataques se realizan por medio de correo electrónico o por teléfono. Los atacantes se hacen pasar por otra persona y convencen a la víctima para entregar información sensible de la organización

o sus contraseñas. Como es un tema más humano, las herramientas tecnológicas que implementan las compañías no pueden prevenir los ataques. Por eso, los atacantes recurren a este tipo de tácticas para vulnerar sistemas muy seguros y complejos [7].

El conocido hacker de sombrero blanco Kevin Mitnick dijo que no tenía mucho sentido invertir recursos en tratar de romper la seguridad de los sistemas. Es más rentable realizar ataques de ingeniería social par-a tener acceso al sistema.

Según Digital Guardian, el 97% de los ataques informáticos no aprovechan una falla en el software, sino que usan técnicas de ingeniería social para conseguir las credenciales necesarias para vulnerar la seguridad informática. Por eso, a veces poco importan las medidas de seguridad tecnológicas que se implementen, si las personas están mandando su clave por correo electrónico. Como parte de la estrategia de seguridad de cualquier compañía, se debe hacer un gigantesco esfuerzo para evitar que los criminales informáticos implementen técnicas de ingeniería social para entrar a los sistemas [7].

En un nivel mucho más elevado, los estados-nación están participando activamente en campañas de ingeniería social, o al menos las usan como parte de ataques mucho más sofisticados: las amenazas persistentes avanzadas (APT). Este tipo de espionaje online, cumple un rol importante en los esfuerzos cibernéticos de países como los Estados Unidos y China, como lo reveló una publicación de Wired. Cuando el objetivo del intruso es el fraude o el espionaje, preferentemente ataca el sistema de personas con un puesto alto dentro la organización, de modo de tener acceso a datos confidenciales [6].

La ingeniería social afecta a todos, pero los estafadores la utilizan cada vez más para atacar las grandes corporaciones y las Pyme: 2014 se describió como el año en que los cibercriminales pasaron al sector empresarial. Un informe de la industria de principios de 2015 reveló que se está usando la ingeniería social para atacar específicamente a los mandos medios y altos ejecutivos. La razón es porque son como una "mina de oro", explicó en aquel entonces Richard De Vere, consultor de ingeniería social y pentester en The AntiSocial Engineer Limited. "Si estás preparando un correo electrónico de phishing, LinkedIn es una mina de oro de donde puedes sacar los datos de los mandos medios y altos ejecutivos", le dijo a SC Magazine. "Las herramientas automatizadas pueden hacer rápidamente una lista de cientos de direcciones de correo electrónico, con los datos de los usuarios y sus credenciales de VPN/OWA/Active Directory" [6].

Existen diferentes tipos de ingeniería social, a continuación, se describen las más comunes:

**a) *Phishing:***

Se deriva del término en ingles pescar. Los criminales informáticos envían correos con 'anzuelos' para ver si alguien cae en la trampa. Con mucha inteligencia, los atacantes se hacen pasar por un miembro del equipo de TI o algún ejecutivo para pedir las credenciales de acceso al sistema a una víctima desconcertada. Por ejemplo, alguien crea una cuenta con la dirección de correo muy similar a la del presidente de la compañía (reemplazando la l con I) y pide le información a diferentes subalternos.

Para prevenir el 'phishing' es necesario educar a los empleados. Según el ejecutivo de .CO Internet, se puede mitigar el riesgo *"gestionando planes de acción claros de concientización a todo el personal, así como incidentes relativos a este flagelo en particular"*. No podemos asumir que todos los empleados conozcan las técnicas de 'phishing' y, aun así, no sobra reforzar los conocimientos con cierta periodicidad [7].

**b) *Acceso no Autorizado:***

Los atacantes son tan atrevidos que muchos se ponen una corbata y crean una identificación falsa para entrar a las instalaciones de la compañía como un ejecutivo más. Como bastantes empresas implementan tarjetas de seguridad, los atacantes saben que las convenciones sociales son más importantes que la seguridad y esperan que algún empleado legítimo le 'tenga la puerta' para poder entrar sin pasar por los controles de seguridad.

Este ataque ha sido ampliamente usado para robar información, dejar dispositivos como 'keyloggers' o troyanos y hacer reconocimiento para realizar un ataque más especializado. Aunque suene un poco descortés, no hay que dejarle la puerta abierta a nadie o por lo menos, verificar que la otra persona ponga su tarjeta para que compruebe su identidad. Las personas que están en las recepciones tienen que estar muy pendientes de que todo el mundo realice adecuadamente el proceso de entrada [7].

**c) *Baiting:***

Esta técnica consiste en dejar una USB en el parqueadero o en un sitio cercano a la oficina (como un café o un restaurante) para que algún empleado la lleve y la conecte a su computador. La USB, en principio, parece inofensiva, pero en realidad está cargada con malware que puede poner en peligro todo el sistema corporativo. Muchas compañías han deshabilitado los puertos USB de sus computadores, pero eso lo quita bastante funcionamiento al equipo. [7]

**2) *Malware*:**

El malware (del inglés malicious software), programa malicioso o programa maligno, también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

***1. Malware Infeccioso:***

Los tipos más conocidos de malware son *virus* y *gusanos*, se distinguen por la manera en que se propagan. El termino *virus informático*, se usa para designar un programa que, al ejecutarse, se propaga infectando otro software ejecutable dentro de la misma computadora. Los virus también pueden tener una carga útil que realice otras acciones a menudo maliciosas, como borrar archivos. Por otra parte, un gusano es un programa que se transmite a sí mismo, explotando vulnerabilidades en una red de computadores para infectar otros equipos, el principal objetivo es infectar a la mayor cantidad de usuarios. Nótese que el virus necesita de la

intervención del usuario para propagarse mientras que un gusano se propaga automáticamente.

***2. Malware Oculto:***

Para que un software malicioso pueda completar sus objetivos, es esencial que permanezca oculto al usuario. Por ejemplo, si un usuario experimentado detecta un programa malicioso, terminaría el proceso y borraría el malware antes de que este pudiera completar sus objetivos.

- ***Puertas Traseras:***

Una puerta trasera (en inglés, backdoor) es un método para eludir los procedimientos habituales de autenticación al conectarse a una computadora. Una vez que el sistema ha sido comprometido (por uno de los anteriores métodos o de alguna otra forma), puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro.

- ***Rootkits:***

Las técnicas conocidas como rootkits, modifican el sistema operativo de una computadora para permitir que el malware permanezca oculto al usuario. Por ejemplo, los rootkits evitan que un proceso malicioso sea visible en la lista de procesos del sistema o que sus ficheros sean visibles en el explorador de archivos. Este tipo de modificaciones consiguen ocultar cualquier indicio de que el ordenador está infectado por un malware. Originalmente, un rootkit era un conjunto de herramientas instaladas por un atacante en un sistema Unix donde el atacante había obtenido acceso de administrador (acceso root). Actualmente, el término es usado generalmente para referirse a la ocultación de rutinas en un programa malicioso.

- ***Troyanos:***

A grandes rasgos, los troyanos son programas maliciosos que están disfrazados como algo inocuo o atractivo que invitan al usuario a ejecutarlo ocultando un software malicioso. Ese software, puede tener un efecto inmediato y puede llevar muchas consecuencias indeseables, por ejemplo, borrar los archivos del usuario o instalar más programas indeseables o maliciosos.

**3.** ***Malware para obtener beneficios:***

Durante los años 1980 y 1990, se solía dar por hecho que los programas maliciosos eran creados como una forma de vandalismo o travesura. Sin embargo, en los últimos años la mayor parte del malware ha sido creado con un fin económico o para obtener beneficios en algún sentido. Esto es debido a la decisión de los autores de malware de sacar partido monetario a los sistemas infectados, alguno de los ejemplos de este tipo de malware es:

- ***Mostrar Publicidad:***

Los programas spyware son creados para recopilar información sobre las actividades realizadas por un usuario y distribuirla a agencias de publicidad u otras organizaciones interesadas. Algunos de los datos que recogen son las páginas web que visita el usuario y direcciones de correo electrónico, a las que después se envía spam.

Por otra parte, los programas adware muestran publicidad al usuario de forma intrusiva en forma de ventana emergente (pop-up) o de cualquier otra forma. Esta publicidad aparece inesperadamente en el equipo y resulta muy molesta.

Los hijackers son programas que realizan cambios en la configuración del navegador web. Por ejemplo, algunos cambian la página de inicio del navegador por páginas web de publicidad o página pornográfica, otros re direccionan los resultados de los buscadores hacia anuncios de pago o páginas de phishing bancario. El pharming es una técnica que suplanta al DNS, modificando el archivo hosts, para redirigir el dominio de una o varias páginas web a otra página web, muchas veces una web falsa que imita a la verdadera. Esta es una de las técnicas usadas por los hijackers o secuestradores del navegador de Internet. Esta técnica también puede ser usada con el objetivo de obtener credenciales y datos personales mediante el secuestro de una sesión.

**4.** ***Malware para Robar Información:***

Los keyloggers y los stealers, son programas maliciosos creados para robar información sensible. El creador puede obtener beneficios económicos o de otro tipo a través de su uso o distribución en comunidades underground. La principal diferencia entre ellos es la forma en la que recogen la información. Los keyloggers monitorizan todas las pulsaciones del teclado y las almacenan para un posterior envío al creador. Por ejemplo, al introducir un número de tarjeta de crédito el keylogger guarda el número, posteriormente lo envía al autor del programa y este puede hacer pagos fraudulentos con esa tarjeta. Los stealers también roban información privada pero solo la que se encuentra guardada en el equipo. Al ejecutarse, comprueban los programas instalados en el equipo y si tienen contraseñas recordadas, por ejemplo, en los navegadores web o en clientes de mensajería instantánea, descifran esa información y la envían al creador.

Los Ransomware también llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un “rescate” para poder recibir la contraseña que permite recuperar los archivos.

## IV. Estrategias de Formación

Una estrategia de aprendizaje o formación es el camino que se define para asegurar que las personas adquieran los conocimientos y desarrollen las habilidades críticas de éxito, que ayuden a cumplir las metas deseadas o se alcance el objetivo propuesto.

Para desarrollar la estrategia de aprendizaje es necesario cumplir tres pasos:

1. Definir en qué nivel contribuyen los conocimientos y habilidades a cerrar las brechas de los indicadores de negocio.
2. Desarrollo e implementación. (Creación de contenidos en detalle a partir de las prácticas de éxito y se realiza la definición de la metodología).
3. Evaluación y acompañamiento a la implementación.

Un momento de aprendizaje ocurre cuando coinciden el interés, la curiosidad y la necesidad de sus colaboradores y se traduce en un aprendizaje sin esfuerzo. Cuando se aprovecha un momento de aprendizaje, hay mayor probabilidad de que las personas entiendan, retengan y apliquen lo aprendido en el

puesto de trabajo.

Si hablamos en términos de metodologías, tenemos tres alternativas. Las presenciales, basadas en momentos y lugares definidos y programados. Las virtuales, que pueden ocurrir en cualquier momento o lugar. O, por último, las mixtas, que mezclan ambos escenarios.

Pero aprovechar los momentos de aprendizaje no depende necesariamente de la forma como su estrategia de aprendizaje entregue el contenido, porque entregar información en un momento pre programado o no, no hace la diferencia cuando hablamos de aprender. La estrategia debe cumplir los siguientes requisitos para para aprovechar los momentos de aprendizaje:

***1) Involucrar al jefe directo y a los tutores:***

Es necesario entender que los "profesores" no son solo los facilitadores virtuales o presenciales. Las personas que hacen la diferencia cuando hablamos de aplicar lo aprendido son precisamente el jefe directo y los pares, porque son los que pueden identificar la necesidad y alentar el interés y la curiosidad de los aprendices en los momentos de aprendizaje. Recordarle a una persona que esa no es una buena práctica y mostrarle cómo hacerlo, o pedirle que repase un módulo de un curso virtual puede hacer toda la diferencia. Y eso no ocurre automáticamente; ocurre cuando hay un esfuerzo sistemático en comunicarle a los jefes y tutores su rol y, sobre todo, en enseñarles cómo ponerlo en práctica a través de planes de tutoría y seguimiento.

***2) Utilizar la tecnología adecuada:***

Las herramientas de soporte y ayuda en el desempeño toman mucha importancia cuando se quiere que el aprendizaje esté disponible siempre. En ese caso, herramientas de micro-aprendizaje como píldoras de conocimiento o impulsadores de aprendizaje son esenciales porque son respuestas rápidas frente a momentos de aprendizaje.

***3) Ser flexible:***

Es cierto que las metodologías virtuales dan flexibilidad porque el acceso al contenido es por demanda. Pero las metodologías presenciales también son flexibles cuando los facilitadores son capaces de aprovechar los momentos de aprendizaje dentro de los talleres o actividades de las sesiones en el salón de clase. De nuevo, esto no ocurrirá sin el esfuerzo consciente desde el diseño de la estrategia de aprendizaje.

Dentro del diseño de la estrategia de aprendizaje, se debe tener muy en cuenta la cultura de aprendizaje en la organización, Una cultura de aprendizaje es un entorno que celebra y da recompensas por aprender, incentiva a la persona a compartir libremente lo que saben, y los ayuda a cambiar basados en la adquisición de nuevas habilidades y conocimientos. No hay duda de que el aprendizaje probablemente fallará si está mal diseñado, el contenido es débil o la tecnología no funciona. Pero el aprendizaje definitivamente fracasará si la cultura no lo apoya. Cuando un gran aprendizaje se enfrenta a una cultura de aprendizaje débil, la cultura siempre ganará. Pero no tiene que ser de esa manera. Acá hay 10 pasos para construir una cultura de aprendizaje positiva. [8]

***1) Comenzar con los líderes:***

La cultura arranca arriba. Si la alta gerencia no apoya una cultura de aprendizaje, nadie más lo hará. Si usted está buscando un punto de quiebre, encuentre líderes que inviertan y premien los esfuerzos, incluso si el proyecto es pequeño o menos visible o significante de lo que usted quisiera. Se necesitan historias de éxito para expandir el mensaje.

***2) Expandir la misión:***

No se va a ningún lado si simplemente se equipara el aprendizaje con el entrenamiento. El aprendizaje, individual y organizacional, es mucho más amplio que los cursos. No cometa el error de hablar de aprendizaje haciendo únicamente entrenamiento. Piense más en el ecosistema de aprendizaje y rendimiento que en el índice del curso; luego actúe consistentemente.

***3) Conseguir la aceptación de la primera línea:***

Si quiere que sus colaboradores aprendan, asegúrese de que sus supervisores aprendan primero. No espere que ellos vayan detrás de algo que no entienden ni ellos mismo. Construya soporte para el aprendizaje y recompense a los gerentes que pongan el aprendizaje dentro de sus prioridades.

***4) Contar con el contenido correcto:***

Publicar mucho contenido no hace nada para motivar el aprendizaje si el contenido es confuso, no auténtico, sesgado, de bajo valor, difícil de acceder, incompleto o simplemente equivocado. La selección del contenido es probablemente lo más importante.

***5) Tener la tecnología correcta:***

No solo se trata de hacer que la tecnología funcione, sino de asegurarse de que es la tecnología correcta para el uso adecuado. Evite que la tecnología bloquee el camino del aprendizaje, o su uso excesivo. La tecnología es importante; el aprendizaje sin tecnología no es escalable, pero la tecnología sin el aprendizaje simplemente es un objeto brillante.

***6) Asegurar la disposición para aprender:***

Uno de los factores que llevan a una cultura de aprendizaje pobre es entregar programas de aprendizaje para personas que no están listas o no lo necesitan. Esto puede desmotivar. Asegúrese de que los aprendices tienes los pre-requisitos adecuados, tienen claras las metas de aprendizaje y tienen el tiempo y los recursos adecuados para aprender, que no están perdiendo el tiempo. Entrégueles incentivos valiosos para aprender y asegúrese de entender por qué pueden estar resistiéndose a sus esfuerzos.

***7) Comunicar el largo plazo:***

Lanzar un nuevo programa de aprendizaje puede ser más ruido que sustancia real. Por supuesto que es necesario promocionar los esfuerzos, pero asegúrese de que las estrategias de comunicación son de largo plazo, valiosas para los ojos de los aprendices y realmente ayudan a desarrollar su propia afinidad positiva para la estrategia de aprendizaje por sí misma; una afinidad que puede ser contagiosa si suficientes personas la compran.

***8) Proveer para la transferencia:***

Asegurarse de que lo que se aprende se puede aplicar es crítico. No solo se trata de poder hacer lo que se aprendió; también se trata de reconocer que lo que se aprendió es útil

para hacer mejor y de manera más fácil el trabajo. La conexión entre desempeño en el trabajo y aprendizaje es clave para construir una cultura de aprendizaje sostenible.

***9) Demostrar el éxito:***

Es mejor tener un pequeño éxito que un gran fracaso. Proyectos de demostración, pilotos, etc. son esenciales para construir soporte para el aprendizaje. Como se vio en el paso uno, la cultura comienza arriba, pero también es importante ver cómo funcionan las estrategias de aprendizaje y cómo pueden beneficiar. Mostrar éxito es mucho más poderoso que solo hablar de éxito.

***10) Medir resultados y retroalimentar:***

Es clave medir cuánto se aprendió, pero tal vez es más importante, desde una perspectiva cultural, medir el valor que las personas le dan al aprendizaje. Y, por supuesto, nada hablar más fuerte que el impacto positivo que el aprendizaje tiene en el desempeño de un individuo y de una organización. Así que vaya más allá de medir el nivel de aprendizaje de un curso. Encuentre el impacto real de la estrategia en los aprendices y en la organización.

Existen diferentes tipos de metodologías que nos permiten abordar una estrategia de aprendizaje, y de esta manera asegurar que el objetivo se cumpla. A continuación, se hablará de algunas de esas metodologías.

***1) El 70:20:10:***

Nace del reto que tienen las empresas para lograr que las personas aprendan a hacer su oficio y así ser mejores cada día, la metodología parte de la naturaleza humana, entendiendo que el ser humano realmente aprende haciendo el oficio, el 10 hace referencia a la porción más pequeña de aquello que se aplica y produce resultados en el negocio, ir a un taller o hacer un curso virtual, por ejemplo. El 20 nace cuando las personas empiezan a aplicar lo aprendido, cuando lo socializan con otros para empezar a obtener resultados, es decir compartiendo el conocimiento. Por último, encontramos el 70, el porcentaje de la metodología que indica que las personas aprenden haciendo. Lo que nos lleva a resumir la metodología en un 10% de recibir información y conocimiento en sesiones de aprendizaje forma, el 20% compartir con otros y el 70% aprender haciendo.

***2) 2x2x2:***

Sabemos que las personas olvidan el 75% de lo que recibieron en una capacitación a las 24 horas; el psicólogo Ebigauss a finales del siglo XIX lo denominó la Curva del Olvido. En investigaciones recientes sobre neurociencia cognitiva, el Profesor Art Khon propone la técnica 2x2x2 para lograr que se recuerde lo aprendido. Ésta utiliza impulsadores de aprendizaje enviando mensajes o preguntas a los participantes a sus pcs, tablets o celulares dos días, dos semanas y dos meses después del evento.

La técnica 2x2x2, y muchas otras, nos llevan a que las personas recuerden lo aprendido, pero el reto va más allá. Debemos asegurar que conviertan ese nuevo conocimiento en resultados y para eso tenemos que estructurar una estrategia de aprendizaje que vaya desde la definición de los contenidos necesarios hasta la evaluación de impacto en los resultados.

Ni el contenido, ni el diseño de las ayudas visuales o de los cursos virtuales, ni su plataforma para administrar o medir el aprendizaje serán suficientes si su metodología no contempla un concepto básico: los momentos de aprendizaje. ¿Cómo aprovecharlos? [8]

***3) Gamifacation:***

Hablar de gamification en el aprendizaje organizacional es cada vez más común. Se dice que el hecho de que las personas jueguen mientras aprenden aumenta la retención y, además, la diversión.

El aprendizaje tradicional se suele quedar corto en contenido para aplicar en el puesto de trabajo. Además, difícilmente logra encajarse e impactar en el día a día de los colaboradores una vez salen del salón de clase. Utilizar gamification para reforzar el aprendizaje de programas presenciales o virtuales permite aplicar los conocimientos en retos y escenarios reales en un ambiente seguro. Esto significa desarrollar y poner en práctica habilidades mientras se cambia el comportamiento.

Parece inocente decir que al jugar se aprende. Pero el sentido del logro y la retroalimentación constante - e inmediata - son determinantes en el impacto de una estrategia de aprendizaje en los colaboradores. Recurrir al gamification con metodología virtual no solo aumenta el grado de involucramiento cuando el contenido es interactivo y divertido; también permite reforzar los conocimientos y contextualizarlos a través de retroalimentación instantánea. Y la emoción de competir sanamente tampoco se puede obviar. Las tablas de líderes son un incentivo para involucrarse en el aprendizaje, publicando un ranking actualizado en tiempo real que permite que los pares se comparen, haciendo del aprendizaje un asunto social.

El gamification es un recurso versátil que se puede utilizar en un curso de ventas, de líderes, o de inducción. Cuando se encuentra con el contenido, la metodología, y el programa de refuerzo adecuado, puede causar un gran impacto en el éxito de una estrategia de aprendizaje. [8]

***4) Programa onboarding:***

Muchas organizaciones invierten recursos sustanciales en los programas de onboarding, que se entienden como un proceso por medio del cual las personas son socializadas con la cultura corporativa y se sienten bienvenidas. Mientras algunos gerentes piensan que un programa de Onboarding no significa nada más que la orientación corporativa – lo cual tiende a enfocarse en familiarizar a los nuevos empleados con las reglas de la organización (hora de entrada, cómo pedir permisos, etc.) - otros tienen una visión más amplia del concepto.

Un programa de onboarding es una oportunidad para facilitar la socialización de una persona con la cultura corporativa. Los nuevos empleados son socializados de formas planeadas y de formas no planeadas. Las formas planeadas pueden incluir briefs por parte del departamento de recursos humanos, jefes directos y tutores dentro de una capacitación en el puesto de trabajo. Las no planeadas pueden incluir conversaciones casuales o historias narradas por los compañeros de trabajo, sobre la organización, los jefes u otros compañeros.

Ahora bien, con cada nueva contratación, la cultura corporativa cambia ligeramente. Ese proceso de socialización inversa y se llama personalización. La personalización es más fuerte en el caso de la alta gerencia. Un nuevo CEO, por ejemplo, puede tener un efecto dramático en la organización de acuerdo con qué es lo que ella o él consideran importante o no importante

Un programa de onboarding debería incluir:

•Misión, metas estratégicas y competidores.
•Estructura organizacional.
•Políticas y reglas de trabajo de recursos humanos.
•Salario y beneficios.
•Descripción del trabajo y metas de desempeño.
•Cronograma de la estrategia de aprendizaje.

También debería incluir otros temas como:

•Tour físico o virtual por las instalaciones.
•Presentar al nuevo empleado con las personas clave y compañeros.
•Tour del espacio de trabajo específico.
•Regulaciones de seguridad (fuego, tormentas, seguridad laboral, etc).
•Asuntos sanitarios (cualquier peligro o situación en el lugar de trabajo).

Diferentes stakeholders desempeñan distintos roles en un programa de Onboarding. Es por eso por lo que es importante clarificar quién debe hacer qué. El departamento de recursos humanos debe familiarizar a los trabajadores con las políticas de la organización, las reglas, los salarios, los beneficios y las instalaciones. El jefe directo debe aclarar las responsabilidades y los estándares de desempeño. El facilitador debe aclarar los requerimientos diarios y los procesos. Y el tutor debe hacer sentir al nuevo trabajador bienvenido, presentándole a las personas clave y asegurándose de que sea invitado a eventos formales e informales. Con esas responsabilidades claras, alguien debe asegurarse de que cada grupo haga lo que le corresponde. Una forma de asegurar esto, es capacitando a cada grupo sobre qué y cómo ejercer su rol. [8]

**5) *PRP:***

PRP resume tres buenas prácticas, tres ideas que implican alto desempeño, alta eficiencia en el aprendizaje y una cultura de aprendizaje altamente desarrollada. Y, sobre todo, tres pilares sobre los que se construye el aprendizaje como un estilo de vida dentro de una organización.

Una brecha se define como la distancia entre donde estoy y el lugar donde quiero llegar, esto no ayuda a entender que cada persona decide que camino de aprendizaje tomar y que por lo tanto es responsable de su recorrido y de su destino. La organización, en ese contexto, entrega las herramientas para que eso suceda.

PRP resume:

**a) *Planes de Desarrollo Personalizados:***

Cada colaborador es libre de definir qué quiere aprender dentro de la organización, de acuerdo con sus metas personales y profesionales.

**b) *Responsabilizar a los Empleados de su Aprendizaje:***

Cada colaborador debe responder no solo por su aprendizaje, si no por el aprendizaje de los demás, actuando a veces como alumno y otras veces como mentor.

**c) *Premiar el Aprendizaje:***

Es importante hacerlo a través de estímulos no monetarios. Por ejemplo, compartir y resaltar los triunfos y aprendizajes con los demás, o desarrollar dinámicas de juego.

Como caso de éxito para este tipo de metodología, contamos con la experiencia de Twitter, ellos lo hicieron apoyados en una herramienta llamada Pathgather, el cual le permite a cada colaborador organizar los recursos del LMS para armar caminos de aprendizaje. Las fuentes de conocimiento pueden estar dentro o fuera de la organización, y cada uno estructura su propio currículum para mejorar sus habilidades y desempeño. Avanzar en los caminos de aprendizaje de Pathgather, curiosamente, no está relacionado con certificaciones o títulos. En vez, el proceso de aprendizaje se relaciona con una dinámica de juego y por eso el aplicativo da puntos conforme se avanza. Dentro de Twitter, el refuerzo positivo de aprender está relacionado con la satisfacción de llevar algo nuevo al puesto de trabajo y la construcción de redes y de una comunidad a través de relaciones entre pares. Ahora, para impulsar el desarrollo personal a través de la retroalimentación y la socialización, Twitter desarrolló otra herramienta llamada Porfolio. Básicamente, permite que cada colaborador solicite evaluaciones 360º en cualquier momento y que escoja a qué pares quiere incluir en el proceso. Así, el proceso de retroalimentación es continuo y es responsabilidad de cada persona dentro de la organización. Para Twitter, el desarrollo y crecimiento de sus colaboradores es prioritario. Por eso, entregar los recursos para que el aprendizaje sea un estilo de vida dentro de la organización equivale a dar la oportunidad de crecimiento, antes de que sus colaboradores se aburran y vayan a otro lugar en donde eso sí sea posible. [8]

Tenemos que tener en cuenta que independiente de la estrategia de aprendizaje elegida, el conocimiento trasmitido debe ser mantenido en el tiempo. Para lograr esto, se debe garantizar dentro de la estrategia, un programa de refuerzo, que permita continuidad al proceso de aprendizaje.

Un programa de refuerzo comienza justo después de un evento de aprendizaje y tiene dos rasgos esenciales: aumenta la retención y demuestra el éxito del aprendizaje. ¿Cómo? A través de contenido rápido, relevante y atractivo relacionado con los objetivos de la estrategia de aprendizaje. Para esto se debe seguir los siguientes consejos.

**1) *Cree Fricción:***

Esa es la forma de hacer el contenido atractivo, en lugar de decir, muestre, cuando los aprendices ven como se hace algo, se involucran y se crea un entorno de aprendizaje activo. Deje que los aprendices hagan conexiones, eso los invita a tomar un rol activo en el proceso, en vez de funcionar como almacenadores de información. Y por último se debe tener en cuenta que también sea social, la fricción no solo debe ser personal, cuando las personas pueden compartir dudas y sus triunfos para recibir retroalimentación, el aprendizaje y su puesta en práctica se potencializan.

**2) *Cree Círculos de retroalimentación:***

La idea es conectar a los aprendices con sus jefes inmediatos, para que estos puedan dirigir su proceso de

aplicación de lo aprendido de una manera acertada. Dependiendo de la estrategia, es posible diseñar:

- Sistemas de puntuación.
- Barras de progreso general.
- Encuestas.

**3)** ***Cree objetivos de refuerzo basados en metas:***

El punto de partida para diseñar un programa de refuerzo, y de cualquier tipo, siempre debe ser el punto de llegada deseado, con un destino claro, el programa se diferencia de un sistema de recordatorios, porque cada contenido estará encaminado hacia las brechas que se quiere cerrar. Pensar en refuerzo es pensar en ese 90% de aprendizaje que normalmente olvidamos al diseñar e implementar estrategias de aprendizaje. [8]

El impacto que tiene la estrategia de aprendizaje debe medirse, pero probablemente las organizaciones decidan no hacerlo (o no al nivel deseado), básicamente porque es difícil, costoso y sus beneficios parecen ser más un mito que una realidad. Por lo que se exponen las siguientes razones por las que realmente debería realizarse la medición.

**1)** ***Alinear el aprendizaje con lo que es importante para el negocio:***

La brecha que existe entre los departamentos de recursos humanos y la alta gerencia se explica en parte porque los primeros no saben hablar el lenguaje de los segundos. Medir el impacto del aprendizaje a distintos niveles permite usar la información para explicar cómo éste contribuye a los indicadores del negocio: el valor monetario asociado al ausentismo o la rotación, la productividad bruta derivada del aumento en el compromiso, o en últimas el Retorno Sobre la Inversión ROI de una estrategia implementada, pueden hacer del aprendizaje un aliado estratégico de su organización.

**2)** ***Administrar mejor el presupuesto:***

Muchas personas reaccionan negativamente cuando alguien no respalda la idea de que el aprendizaje es una inversión y no un gasto. ¿La verdad? Muchos programas de aprendizaje sí son un gasto y las organizaciones no tienen la capacidad de identificarlos como tal. Medir el impacto de un programa permite saber cuáles aportan valor a la organización y cuánto valor aportan. Esta información permite tomar decisiones. Por ejemplo, frente a un recorte en el presupuesto destinado a aprendizaje dentro de su organización, no sería acertado eliminar una estrategia de aprendizaje en marcha que tiene un retorno positivo sobre la inversión. Sin medición, sus ojos estarían vendados.

**3)** ***Mejorar las estrategias de aprendizaje en marcha:***

No basta con saber que una estrategia aporta valor real a una organización. Imagine que esa estrategia en marcha puede aportar más valor. Con información derivada de la medición, es posible identificar falencias en el contenido o metodología de un programa e implementar acciones para mejorarlo, sabiendo que van a redundar en un mayor retorno.

**4)** ***Hacer pronósticos acertados:***

Un sistema de medición puede, en el nivel más básico, identificar el valor monetario del aumento en el grado de compromiso medido a través de una encuesta. Pero una medición completa del Retorno Sobre la Inversión (ROI) para programas de alto valor dentro de una organización, le permite analizar la ganancia potencial de invertir en una estrategia de aprendizaje antes de implementarla, comparado con el costo presupuestado.

Es importante tener en cuenta que una estrategia de aprendizaje puede fallar, esto sucede si la estrategia está mal diseñada, el contenido es débil o la tecnología que la soporta no funciona, y definitivamente puede fracasar si la cultura dentro de la organización no la apoya. Ahora se debe preguntar ¿qué aleja a mi organización de una cultura de aprendizaje robusta? y ¿qué puedo hacer para superar esos obstáculos?

Existen tres importantes barreras, que entre más se evidencien dentro de una organización, es menos probable que la organización reporte un alto desempeño. Es decir, lo que se quiere evitar:

1) La comunicación organizacional no resalta la importancia del aprendizaje.
2) Los valores corporativos no incluyen el aprendizaje.
3) El aprendizaje está excluido de los procesos de planeación estratégica.

Derrumbar estas (y otras) barreras implicará dar paso para que su organización pueda construir una cultura de aprendizaje robusta. Para eso, los líderes, los colaboradores, el equipo de aprendizaje y desarrollo y la organización deberán poner de su parte. Veamos qué puede hacer cada uno.

Los líderes.

1) Enseñarse los unos a los otros.
2) Ser consejeros del área de aprendizaje y desarrollo.
3) Ser responsables de demostrar activamente la importancia del aprendizaje.

Los colaboradores.

1) Compartir el aprendizaje de una manera fácil.
2) Seguir planes de desarrollo personalizado asociados a recompensas.
3) Hacerse responsables de su aprendizaje.

El equipo de aprendizaje y desarrollo.

1) Ser parte de las iniciativas de planeación de talento.
2) Alinearse con la estrategia del negocio.
3) Saber medir y medir lo importante.

La organización.

1) Usar el poder del aprendizaje en los procesos de contratación para atraer talento.
2) Dar tiempo para aprender. La probabilidad de que una compañía top asegure la disponibilidad del aprendizaje en horario laboral es del doble, comparado con organizaciones de bajo rendimiento.
3) Usar el aprendizaje para involucrar y retener a los colaboradores valiosos. Cuando el aprendizaje de los colaboradores está alineado con sus metas personales y profesionales, la retención aumenta. [8]

## V. PROPUESTA DE ESTRATEGIA PARA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Enmarcados en la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO\IEC

27001, debemos tener en cuenta que una buena estrategia de aprendizaje, cuyo objetivo sea comunicar el programa del SGSI, sensibilizar a los usuarios finales y generar conciencia sobre la importancia de la seguridad de la información, tanto en el trabajo como en el día a día de las personas, logrará fortalecer el SGSI de cualquier organización, y así apalancar su sostenibilidad en el tiempo.

En un sistema de gestión apalancado por un plan PHVA (Planear – Hacer – Validar - Actuar), de debe definir una estrategia de aprendizaje que apoye cada una de las fases del sistema, teniendo en cuenta las buenas prácticas descritas en el capítulo 4.

Es importante tener en cuenta para que una estrategia de aprendizaje en seguridad de la información tenga éxito, el objetivo de la estrategia no solo debe centrase en los objetivos de SGSI de la empresa, también debe tener un contenido enfocado en la sensibilización hacia la utilidad de las buenas prácticas en el día a día de las personas, y como estas ayudan a proteger su entorno familiar.

De acuerdo con la teoría de estrategias de aprendizaje, vista anteriormente, lo primero que se debe establecer es el contenido que se desea trasmitir, esto se obtiene de la definición del SGSI y de las condiciones actuales de la empresa. Además, se debe sumar contenido basado en las necesidades que presentan las personas por fuera de las instalaciones de la empresa, y sean útiles para ellos.

Basado en las estadísticas presentadas en el primer capítulo, se puede establecer que los delitos informáticos van en crecimiento en el país, y que los ciberdelincuentes no solo atacan empresas, también se especializan en personas naturales, con métodos que buscan robar información sensible como números de cuentas y claves de entidades bancarias, secuestro de información personal para posteriormente extorsionar al propietario entre otras; para esto, los delincuentes utilizan diferentes técnicas, la mayoría de veces acompañas de *ingeniería social*, por lo que se recomienda, que gran parte de la formación a usuarios finales, se centre en este tema, claramente sin dejar atrás las políticas establecidas por la compañía, y una gama de especificaciones técnicas que se considere, las personas deban saber.

Es importante tener en cuenta que la necesidad de formar a los colaboradores en seguridad de la información no solo es un requisito normativo, en realidad nace de la alineación del SGSI con el negocio, y una empresa que entienda el vínculo completamente, está en la capacidad de alinear el aprendizaje al SGSI y a los objetivos de negocio. Una estrategia de aprendizaje alineada al SGSI se construye cuando el equipo encargado del área de seguridad y apoyado por el departamento de recursos humanos de la empresa definen las expectativas de la formación, y las traducen en habilidades y conocimientos, para esto se pueden seguir los siguientes hitos.

***1) Alianza entre Seguridad de la Información y la Gerencia de Talento humano:***

Ocurre cuando ambos son capaces de hablar el mismo idioma: el de los objetivos del negocio y el SGSI. Entonces se crea un vínculo que parte de la visión estratégica de la organización, atraviesa el plan de negocios de los equipos ejecutivos, luego las iniciativas de los líderes de departamento y finalmente aterriza en el aprendizaje. Con los objetivos del negocio como eje de la alianza, es posible entender y profundizar en las necesidades del SGSI.

***2) Entender las necesidades del SGSI:***

Pueden ser problemas (brechas operacionales entre una meta y un resultado) u oportunidades (metas operacionales futuras). Cuando se identifica una necesidad del SGSI que se quiere impactar, la gerencia y recursos humanos definen qué significa éxito en esas situaciones problemáticas u oportunidades. Precisamente, el éxito es el resultado de impactar positivamente un objetivo del SGSI y define las metas de la estrategia de aprendizaje.

***3) Trazar metas:***

Las metas de una estrategia de aprendizaje alineadas con el negocio representan tres cosas:

•El resultado buscado, o cómo los cambios en el desempeño deben impactar los objetivos del negocio.
•El rol que el aprendizaje va a desempeñar en el proceso.
•Un barómetro para evaluar el éxito.

Y por supuesto, cada meta debe ser SMART.

•Específica: ligada a iniciativas del negocio particular.
•Medible: se puede verificar su progreso y resultado.
•Alcanzable: se cuenta con los recursos necesarios.
•Relevante: genera valor para la alta gerencia.
•Limitada en el tiempo: tiene un plazo definido para cumplirse.

***4) Requerimientos de desempeño:***

Los requerimientos de desempeño son las habilidades y conocimientos específicos que, puestos en práctica, llevan al desempeño deseado.

***5) Contenido:***

La pregunta de fondo es: ¿este tema apunta directamente a los requerimientos de desempeño definidos? Hacerse esa pregunta reiterativamente es la clave para elaborar un mapa temático que responde a las necesidades del negocio y que articula la estrategia de aprendizaje.

***6) Mediciones:***

Desarrollar un plan de medición implica definir los intervalos de recolección de datos y los métodos para recolectar y procesar la información.

Una vez se tenga definido el contenido, basado en los pilares aconsejados previamente, se debe proceder a crear ese contenido, teniendo en cuenta la metodología escogida, en el capítulo 4 se abordan diferentes tipos de metodologías en los cuales se puede sostener la estrategia, es conveniente utilizar diferentes metodologías para la transmisión del conocimiento, teniendo en cuenta que la población objetivo no es homogénea, ya que puede encontrarse dividida por generaciones, niveles de conocimiento o áreas de conocimiento. El uso de la metodología también debe tener en cuenta el momento el que se planea impactar al usuario, no se puede utilizar la misma metodología y el mismo contenido, para un usuario que ingresa nuevo a la organización, que para uno que lleva un tiempo prolongado trabajando con la misma. Por último, también se debe tener en cuenta el tamaño de la compañía y la ubicación de esta, la metodología debe

contemplar la cantidad de usuarios que se deben capacitar, y el lugar de ubicación de esos usuarios.

Teniendo en cuenta lo anteriormente expuesto, se recomienda tener una estrategia de capacitación con metodologías hibridas, la tendencia actual indica que se pueden utilizar metodologías digitales, como el *gamification* expuesto en el capítulo 4, que permite digitalizar los contenidos y apoyados en un LMS (Learning Management System), entregando capsulas de conocimiento a los usuarios, o incluso cursos completos de actualización, pero esto se aconseja para poblaciones que tienen un conocimiento avanzado del tema, es aconsejable utilizar este tipo de metodologías para realizar actualizaciones anuales o semestrales a los usuarios, con el fin de fortalecer el conocimiento adquirido previamente, este tipo de metodologías permiten la sostenibilidad en el tiempo de la estrategia de aprendizaje.

Para usuarios nuevos, personas que empiezan a hacer parte de la compañía, es aconsejable introducir el tema de seguridad de la información, desde el programa de inducción u *O onboarding*, expuesto en el capítulo 4, esto permite que el usuario desde el ingreso a la compañía adquiera el conocimiento necesario sobre las políticas y estrategias de seguridad implementadas por la compañía, así como los temas que se hallan definido como necesarios dentro del contenido del programa. Para el programa de inducción es recomendable utilizar una metodología de sensibilización presencial, por parte del área encargada de administrar y gestionar el SGSI, pero también es necesario, que la capacitación durante el proceso de inducción, este acompañada por algún método de medición de adquisición del conocimiento, como una evaluación, ya que se debe garantizar que las personas obtuvieron el conocimiento básico antes de iniciar sus labores, la ejecución de evaluaciones, también es una buena práctica para tener evidencias de la transmisión de conocimiento a los empleados de la compañía y así responde futuras auditorias.

## VI. Conclusiones

1) Capacitar a los usuarios finales, no solo con énfasis en conocimiento técnico, sino también en toma de conciencia de la importancia de la seguridad de la información tanto en el trabajo como en su vida personal, ayuda a garantizar la transferencia del conocimiento, como la maduración del SGSI.
2) La estrategia de aprendizaje debe contener diferentes tipos de metodologías, para garantizar que los diferentes segmentos de la población adquieran el conocimiento deseado, se aconseja para el programa de inducción, una capacitación presencial por parte del área encargada de la administración del SGSI acompañado de una evaluación, por otra parte se aconsejan capsulas de conocimiento por medios digitales, para los colaboradores que ya se encuentran en la operación, buscando realizar un refuerzo para la estrategia de aprendizaje.
3) La ingeniería social está presente en la mayoría de los ataques cibernéticos, que ocurren actualmente en el país, los contenidos de capacitación a usuarios finales deberían tener este elemento como columna vertebral, ya que es donde más se impacta al usuario.
4) Los contenidos de la capacitación, deben estar segmentados de acuerdo a la población a la que van dirigidos, en el caso de programas de inducción u onboarding, se debe diseñar un programa con un contenido que garantice al usuario, el conocimiento mínimo requerido antes de iniciar su trabajo, especial énfasis en políticas de la empresa; los contenidos para usuarios más experimentados de la operación deben ser ligeros y dinámicos, y pueden ser enviados a través de medios digitales y por último los contenidos a usuarios de tecnología y altos directivos, debe tener un énfasis en sus roles.

## Referencias

[1] Tecnosfera, "A diario se registran 542.465 ataques informáticos en Colombia," El Tiempo, 27 Septiembre 2017. [En línea]. Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370. [Último acceso: 5 Enero 2018].

[2] Portafolio, "Colombia registró 198 millones de ataques cibernéticos en el 2017," Protafolio, 27 Septiembre 2017. [En línea]. Available: http://www.portafolio.co/tendencias/colombia-es-uno-de-los-paises-mas-afectados-por-ataques-ciberneticos-510128. [Último acceso: 6 Enero 2018].

[3] Tecnosfera, "El 63 % de las grandes empresas identificaron incidentes digitales," El Tiempo, 3 Octubre 2017. [En línea]. Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/resultados-del-estudio-impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017-137222. [Último acceso: 5 Enero 2018].

[4] ESET, "ESET Security Report Latinoamérica 2017", 2017. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf. [Último acceso: 6 Enero 2018].

[5] ENTER.CO, "ENTER.CO", ENTER.CO, 12 02 2018. [En línea]. Available: http://www.enter.co/especiales/empresas/amenazas-seguridad-2018-symantec/. [Último acceso: 14 02 2018].

[6] ESET, "5 cosas que debes saber sobre la Ingeniería Social," 6 Junio 2016. [En línea]. Available: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/. [Último acceso: 13 Enero 2018].

[7] ENTER.CO, "LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO," 2016 Julio 2016. [En línea]. Available: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/. [Último acceso: 13 Enero 2018].

[8] P. e. d. Aprendizaje, "P y B Estrategas en Aprendizaje," PyB, [En línea]. Available: http://www.pyb.com.co/. [Último acceso: 01 02 2018].

**Gutierrez Trujillo. Pablo Cesar** nació en Popayán – Cauca, el 18 de febrero de 1991, es ingeniero en Automática

Industrial, titulo obtenido en la Universidad del Cauca año 2013, actualmente se encuentra en proceso de obtener el título de Especialista en Seguridad Informática de la Universidad Piloto de Colombia