UNIVERSIDAD CENFOTEC

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

PROGRAMA DE CULTURIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN EN TIGO COSTA RICA

Presentada por:

Ing. Alexander Fonseca Caravaca

Abril 2018

i. Derechos de autor

Yo, ALEXANDER FONSECA CARAVACA con IDNº 109470702; declaro que el documento de grado denominado "PROGRAMA DE CULTURIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN EN TIGO COSTA RICA", se ha desarrollado de manera íntegra, respetando derechos intelectuales de las personas que han desarrollado conceptos mediante las citas en las cuales indican la autoría, y cuyos datos se detallan de manera más completa en la bibliografía.

En virtud de esta declaración, me responsabilizo del contenido, autenticidad y alcance del presente documento.

San José, Costa Rica, abril 2018

ii. Dedicatoria

“La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar”.
Thomas Chalmers

Dedico este trabajo principalmente a Dios, por darme la vida y permitirme llegar hasta este momento tan importante de mi formación profesional.

A mi esposa e hijas por el sacrificio, su amor, permanente cariño y comprensión para poderme realizar. Son, han sido y serán mi motivación, inspiración y felicidad.

A mis padres y hermanas, por ser un pilar importante y demostrarme siempre su cariño y apoyo incondicional, sin importar las opiniones.

HOJA DE APROBACION DE PROYECTO

TITULO DEL PROYECTO:

"**PROGRAMA DE CULTURIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN EN TIGO COSTA RICA**".

Autor: Ing. Alexander Fonseca Caravaca

_____

Ing. Ignacio Trejos Zelaya

Lector 1

_____

Ing. Arturo Ramirez Hegg

Tutor

_____

Ing. Aaron Mon NG Martinez

Lector 2

Contenido

Índice de Imágenes Pág.

iii. Resumen

El constante crecimiento y los cambios rápidos de las tecnologías de la información, el acatamiento obligatorio a los requerimientos legislativos y leyes en temas relacionadas con la protección de los datos de clientes, del negocio y financieros, etc. Mantiene gran presión a las empresas de hoy en día. Se requiere mejorar aspectos relacionados con la gestión de la información, así como los conocimientos sobre las formas de implementar ambientes de protección ante las amenazas y vulnerabilidades que el ciberespacio expone en la actualidad.

Las implementaciones de herramientas colaborativas en seguridad tecnológica como hardware, software y aún más, implementar mecanismos de control que apoyen al garantizar una adecuada administración y "*Seguridad de la Información*". Esto sin importar el giro del negocio (público, privado, u otro).

Este enorme crecimiento origina cada vez sistemas de protección tecnológica más complejos de administrar. Por consiguiente, existe un desmedido aumento en la exposición a los riesgos y amenazas a los que se enfrenta una organización, en conjunto con sus colaboradores y administradores. Las vulnerabilidades pueden tener una cantidad innumerable de factores que las ocasionan. De igual forma, soluciones para mitigar o bien disminuir la probabilidad de materialización de estos riesgos y que una persona con intenciones desconocidas, tome provecho de las mismas.

Uno de los principales actores que está expuesto o bien que propicia vulnerabilidades, lo representa el personal que colabora en la obtención de las metas y objetivos de las organizaciones. Este en reiteradas ocasiones es señalado como "El eslabón más débil en la cadena de la seguridad". Ellos por múltiples situaciones puede ser el causante de incrementar las amenazas y vulnerabilidades, además de aumentar los riesgos en las organizaciones. Muchas veces esto se debe principalmente a la falta de conocimiento en el manejo adecuado de la información que genera, o bien manipula día a día, en su posición de trabajo.

En el presente trabajo, se mencionan algunas de las principales organizaciones, estándares y normas a nivel internacional que desarrollan guías, controles para la elaboración de programas y/o planes de concientización y entrenamiento para la difusión de la "*Seguridad de la Información*" empresarial. Asimismo, se pretende identificar cómo se debe inscribir un programa de un esquema de gestión de la "*Seguridad de la Información*". Ya que la conciencia del riesgo y los métodos de defensa disponibles son la primera línea de defensa para la "*Seguridad de la Información*" y los sistemas conectados a nuestra red.

Un programa de entrenamiento debe facilitar consejos prácticos sobre cómo formar conciencia sobre la "*Seguridad de la Información*" en los diferentes grupos receptores, especialmente en los colaboradores y usuarios de las diferentes tecnologías del negocio.

Así cómo mejorar la conciencia de "*Seguridad de la Información*" al ilustrar los procedimientos necesarios para planificar, organizar y ejecutar iniciativas de sensibilización sobre la "*Seguridad de la Información*". Para ello se dividirá el programa en etapas de planificación y evaluación; ejecución y administración: evaluación y ajuste.

iv. Referencia de Siglas y Abreviaturas

CMM/SSE: Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas
FIPS: Federal Information Processing Standard
IDS: Sistema de detección de intrusiones
IEC: Comisión Electrotécnica Internacional
IPS: Sistema de prevención de intrusiones
ISO: Organización Internacional de Normalización
MIC: Millicom International Cellular
NIST: National Institute of Standards and Technology
SGSI: Sistema de Gestión de Seguridad de la Información
TIC: Tecnologías de Información y Comunicación

1. CAPITULO I INTRODUCCIÓN

El presente trabajo será realizado en Millicom Tigo Costa Rica, empresa del sector de las telecomunicaciones. La finalidad del proyecto se enfoca en la definición de un marco de trabajo que permita de forma, tanto metodológica como efectiva, lograr un mayor y mejor control sobre la "*Seguridad de la Información*", así como los activos tecnológicos que rodean a la totalidad de los colaboradores del negocio.

La "*Seguridad de la Información*" consiste en proteger uno de los principales activos del negocio: la información. Esto es un requisito indispensable para la existencia de cualquier negocio o empresa. Esta es utilizada en cada uno de los procesos empresariales, y dependen de la forma en que sea almacenada, procesada y presentada.

La gestión de la "*Seguridad de la Información*", así como muchas otras áreas del negocio, actualmente están muy ligadas a las personas, ya que ésta, solamente tiene sentido cuando es utilizada o interpretada por las personas. Son estas últimas quienes deben conocer la adecuada gestión de este recurso.

Todas las áreas de negocio utilizan el capital humano para obtener o procesar la información. Esto con el objetivo de potenciar su actividad específica. De ahí la importancia que toma la "*Seguridad de la Información*", la cual requiere que el personal involucrado cuente con la adecuada capacitación y conocimiento para la gestión de los recursos informáticos.

Ante esto, no se puede proteger de forma adecuada la información, sin una correcta cultura y entrenamiento del recurso humano. El proteger los activos empresariales no es, ni debe ser una responsabilidad solamente de las áreas de seguridad y/o tecnológicas, sino que se debe compartir a lo largo y ancho de la organización. Cada área debe jugar un papel de importancia en cuanto a la seguridad. Por ejemplo, el área de marketing debe de enfocarse en proteger temas de imagen corporativa; el área comercial debe proteger los datos de los clientes; tecnologías de información debe ocuparse de una correcta protección de los sistemas utilizados por el negocio, entre otros.

Expuesto lo anterior, se puede mencionar que para lograr una adecuada y segura gestión de los datos, es de gran relevancia cómo se entrene y concientice al recurso humano en los temas relacionados.

Al implementar un modelo de entrenamiento y culturización en "*Seguridad de la Información*", es indispensable enfocarse en estándares, modelos y normas internacionales que toman como referencia una serie de mejores prácticas para asegurar una adecuada gestión de la "Seguridad de la Información" del negocio.

La empresa crea una imagen de prestigio y de interés al resaltar entre las demás. De esta forma, se buscar un avance significativo en la confianza de los clientes para con ellos, así como un diferenciador del negocio. Al conocer la obtención de dicha implementación o el tener una certificación relacionada.

Aplicar la gestión de "*Seguridad de la Información*" enfocada en el recurso humano es de gran importancia, por la información que tiene la empresa Millicom Tigo Costa Rica, la cual es una empresa que maneja gran cantidad de datos de sus clientes.

El realizar este trabajo de graduación busca mejorar la gestión de los datos de forma integral. Se expone, por último, que al implementar dicho programa y profundizar en los lineamientos bases de las normas y estándares de la industria, brindará grandes experiencias sobre distintos temas competentes y realidades desconocidas sobre el ambiente laboral y el tratamiento con recurso humano, para transmitir ideas y tecnologías.

1.1 Antecedentes del problema

Desde tiempos antiguos, el hombre ha resguardado y protegido con recelo la información y sus conocimientos. Esto a causa de la ventaja y poder que ésta le otorga sobre los demás. Por ejemplo, se estima que los inicios de la criptografía como método de protección de datos, datan desde los años 600 al 500 antes de Cristo. Se utilizaron jeroglíficos y/o cifrados por sustitución mono alfabéticos para enviar o dar mensajes y que fuesen entendidos solamente por aquellos que conocían el método de interpretación de los mismos.

A inicios de los años 1900, las tropas alemanas protegían la información que se transmitía a sus soldados utilizando métodos de ocultamiento o cifrados más complejos, por medio de la máquina de su creación "Enigma". Con este dispositivo brindaban confidencialidad a los mensajes que enviaban a sus tropas ya que solamente podían ser interpretados o entendidos por quienes debían conocer los mismos, acción que les permitió ganar muchas batallas.

Actualmente, con el auge de las Tecnologías de Información y Comunicación, las organizaciones se enfrentan a nuevos y complejos retos relacionados con la protección de la información privada ya que ésta tiende a estar más expuesta. Es por esto que la protección de los datos ha adquirido una importancia fundamental y muchas empresas han debido incluir en sus objetivos las inversiones y presupuestos en tecnologías que buscan proteger y gestionar de forma adecuada la información.

La tarea de la "*Seguridad de la Información*", así como muchas de las aristas de la gestión empresarial, depende principalmente de seres humanos quienes colaboran para la organización.

La información del negocio toma sentido solamente cuando es utilizada por las personas. Al fin son éstas, quienes en última instancia, deben utilizar adecuadamente este activo de la empresa. Ante esto, la probabilidad de proteger de forma adecuada la información disminuye si no existe una cultura empresarial en "*Seguridad de la Información*" inculcada en el recurso humano.

Por esto surge la pregunta: **¿Es posible controlar las intenciones de las personas en cuanto al manejo de la información?**

1.2 Definición y descripción del problema

En la actualidad, un gran número de personas y entre ellos colaboradores en las empresas desconoce sobre temas de "*Seguridad de la Información*" y su gran ámbito de alcance. Diversidad de estudios realizados, los cuales de forma constante revelan que hoy, la mayor cantidad de eventos considerados como ataques de "*Seguridad de la Información*" provienen del interior de las propias empresas. Las causas pueden ser variadas como (introducir software malicioso (malware) que permita a un tercero manipular datos e información sin autorización (ejemplo, robar, divulgar, modificar o destruir datos), deficiencia en controles de accesos a aplicativos y/o datos, fraude y robo de información, desconocimiento de políticas y sus sanciones, falta de formación y concienciación…).

De la misma manera se ejecutan ataques a través de la técnica conocida como ingeniería social. Esto se debe a que resulta más fácil obtener las credenciales de accesos de un usuario al interior de la compañía, que vulnerar las arquitecturas de seguridad lógica, perimetral, sistemas de seguridad y cifrado. En algunas organizaciones, con tan sólo recorrer un par de lugares de trabajo, se pueden encontrar contraseñas escritas, expuestas y/u ocultas y pegadas en la pantalla o bien debajo de los teclados.

La principal finalidad de crear un programa que se enfoque en entrenar, culturizar y sensibilizar en temas de "*Seguridad de la Información*" dentro de una entidad, tiene como objetivo primordial la búsqueda de la modificación de la conducta de los colaboradores respecto a este tema. Se busca medir por medio de encuestas y cuestionarios periódicos, así como el lanzamiento agendado de campañas de phishing e ingeniería social en las que se evalúe la aplicación de los conocimientos transmitidos en las sesiones virtuales y presenciales.

La tarea de definir y ejecutar un programa de sensibilización y entrenamiento que permita modificar verdaderamente la conducta de los empleados exige dedicar tiempo y recursos, en algunos casos, en cantidad considerable. Debe acompañarse también de la generación de políticas, procesos y procedimientos enfocados al objetivo que se busca.

Aunque en ocasiones no se sabe por dónde comenzar; en otras, se tienen limitantes como falta de dinero, tiempo, o tabúes. Ante cualquier iniciativa de esta índole, existe resistencia

o bien se escuchan expresiones del tipo "¡Eso no funcionará en esta empresa!". Es allí donde juega un papel determinante el apoyo de las altas gerencias y juntas directivas para que la implementación sea exitosa. De lo contrario, el camino se tornará escabroso.

Esta iniciativa busca la implementación de un programa que guíe y permita proteger la información, junto con los procesos y sistemas que hacen uso de ella. La confidencialidad, la integridad y la disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

1.3 Justificación

Las empresas privadas, así como cualquier organización maneja información sensible de gran importancia para el cumplimiento de metas y objetivos enfocados en la misión del negocio; procesos como el almacenamiento y manipulación de esta información; instalación de aplicativos y equipos tecnológicos, los cuales deben ser protegidos para permitir la integridad, disponibilidad y autenticidad de la información.

El creciente uso de las nuevas tecnologías ha propiciado la creación de un marco legal y jurídico que protege a todas las partes interesadas en el uso de estas tecnologías, el intercambio y tratamiento de la información a través de ellas.

Cada día surgen nuevas formas de delito informático que pueden afectar a la "*Seguridad de la Información*" en las empresas. Por ello, se debe cumplir con la legislación vigente en Costa Rica. Es uno de los requisitos que se deben satisfacer para implantar un Sistema de Gestión de "*Seguridad de la Información*". Su cumplimento protegerá de amenazas externas; permitirá respetar los derechos de los clientes y proveedores al evitar infracciones involuntarias con sus respectivos costes.

Aunado a eso, es de suma importancia que cualquier colaborador que genere, obtenga, transforme, conserve o utilice información de la organización en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la organización con propósitos propios de su labor, tendrán el derecho de su uso dentro del

inventario de información. Pero, deberán poseer una definición adecuada de los niveles de accesos a estos activos de información.

1.4 Viabilidad

Al ser Millicom una compañía transnacional, la estandarización de los procesos y procedimientos en los temas relacionados con la seguridad y manejo de la información en la totalidad de áreas del negocio, son de ejecución obligatoria. Ante esto, existe un compromiso por parte de la alta gerencia para apoyar los procesos de entrenamiento, sensibilización y cultura de la totalidad de los colaboradores que forman parte directa o indirectamente de la organización.

1.4.1 Punto de vista técnico

El desarrollo del programa busca brindar una mejora en la imagen y confianza de la empresa entre clientes, proveedores y socios. Poco a poco, exigen estos niveles de implementación para abrir y compartir sus sistemas de información con cualquier empresa. La existencia de un programa definido, implementado y medible busca alinear y estandarizar las estrategias y objetivos de seguridad entre las partes.

1.4.2 Punto de vista operativo

La implementación del programa de culturización y concientización en "*Seguridad de la Información*" es una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la alta gerencia y direcciones.

El diseño de este programa se dirige a los objetivos y necesidades de la empresa, así como de su estructura. Estos elementos son los que van a definir el alcance de la implantación. Es decir, las áreas que van a verse involucradas en el cambio. En ocasiones, no es necesario un programa que implique a toda la organización, puede ser que sea sólo necesario en un departamento, una sede en concreto o un área de negocio.

1.4.3 Punto de vista económico

El programa de culturización en "*Seguridad de la Información*" tiene como base lineamientos definidos en diferentes documentos de la industria de la "*Seguridad de la Información*" reconocidos a nivel mundial. Por ejemplo, la norma ISO/IEC 27000 y su familia de documentos, la NIST, Estándares FIPS (Federal Infomation Processing Standard) y CMM (Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas), la extracción de las principales líneas bases de cada documento convierten este documento en una herramienta o metodología sencilla y de bajo coste que cualquier empresa puede utilizar. Estas normas y estándares permiten establecer políticas, procedimientos y controles con objeto de disminuir los riesgos de la organización. Para la implementación mencionada, en Millicom se definieron los procedimientos por seguir, así como los presupuestos y transferencias de conocimientos a los involucrados directos en las diferentes etapas.

1.5 Objetivos

La capacitación en "*Seguridad de la Información*" a los colaboradores de la empresa es de vital importancia, ya que en la actualidad la información es uno de los activos que poseen más valor. En las empresas en las cuales no existe una concientización y capacitación, la posibilidad de pérdida o fuga de datos, incrementa los riesgos de afrontar las difíciles consecuencias que esto conlleva.

Ante esto, se desarrolla el programa de concientización en *"Seguridad de la Información*" el cual tiene como uno de sus enfoques principales crear cultura y capacitar al recurso humano en temas de conciencia sobre los efectos de las acciones que impactan la seguridad de la empresa y su información, así como el entendimiento de toda la serie de conceptos a transmitir y entender sobre lo que se debe y no se debe hacer a la hora de manipular datos e infraestructuras del negocio.

1.5.1 Objetivo General

Diseñar e implementar un programa de culturización y concientización en *"Seguridad de la Información*" y entrenar al recurso humano en temas de conciencia sobre las acciones que impactan la seguridad de la empresa y su información.

1.5.2 Objetivos Específicos

- Ilustrar una estrategia sobre cómo planificar, organizar y ejecutar una iniciativa de concienciación sobre la "*Seguridad de la Información*".
- Establecer y definir las rutinas por seguir para realizar la capacitación y transferencia de conocimiento en "*Seguridad de la Información*".
- Diseñar un marco de trabajo y ejecución del programa de concientización en "*Seguridad de la Información*" para Tigo Costa Rica.
- Contribuir al desarrollo de la "*Seguridad de la Información*" para alentar a los usuarios a actuar de forma responsable y, por lo tanto, operar de forma más segura.
- Presentar plantillas y herramientas para ser utilizadas como puntos de partida por el equipo de sensibilización.
- Definir los lineamientos de introducción del personal a las tecnologías de la empresa.
- Crear una conciencia de seguridad aplicable a los activos de información.
- Reducir el riesgo de robo, fraude y mal uso de los medios a través de información vigente, de conocimiento público y la conciencia de seguridad dentro de la empresa.
- Accesar a la información a través de medidas de seguridad, por parte de los usuarios.
- Crear un ambiente de confianza estableciendo la cultura dentro de la compañía, con respecto a la seguridad de información que manipulan y corresponde al área gestionada.
- Mejorar la imagen de confiabilidad y seguridad de la empresa, siendo elemento diferenciador de la competencia.

1.6 Alcances y limitaciones

1.6.1 Alcances

El programa de culturización en *"Seguridad de la Información*" busca diseñar una metodología de transferencia de conocimiento a los colaboradores para crear cultura y conciencia sobre la adecuada gestión de los datos del negocio. Para ello, se definió una serie de aspectos fundamentales que definen la metodología de concientización y entrenamiento en "*Seguridad de la Información*"; la política de seguridad por seguir; la organización de la seguridad y los programas de concienciación y formación del personal.

1.6.2 Limitaciones

En cualquier proyecto, el recurso más importante son las personas. Idealmente, un proyecto debería tener disponible un número adecuado de personas, con las habilidades y experiencia correctas, comprometidos y motivados con el proyecto. Sin embargo, las cosas pueden ser diferentes, por lo que se han identificado estos riesgos.

- ¿El personal del proyecto está comprometido con la entera duración para lo que son necesarios?
- ¿Todos los miembros del equipo están disponibles en los tiempos requeridos?
- ¿El movimiento de personal de un mismo proyecto es suficientemente bajo como para permitir la continuidad del proyecto?
- ¿Se han establecido los mecanismos apropiados para permitir la comunicación entre los miembros del equipo?
- ¿El entorno de trabajo del equipo es el apropiado?

1.7 Productos esperados

Objetivos Específicos	Producto esperado	Referencia dentro del TFG	Lugar
• Ilustrar una estrategia de muestra sobre cómo planificar, organizar y ejecutar una iniciativa de concienciación sobre la "*Seguridad de la Información*".	Plan de sensibilización, capacitación y comunicación	Capitulo IV-Marco metodológico; Capítulo V-Desarrollo de la propuesta; del presente documento	Plataforma de comunicación interna, intranet
• Establecer y definir las rutinas por seguir para realizar la capacitación y transferencia de conocimiento en "*Seguridad de la Información*".	Encuestas, cuestionarios, laboratorios, charlas presenciales y virtuales.	Capítulo V-Desarrollo de la propuesta y Anexos.	Plataforma de Millicom University
• Diseñar un marco de trabajo y ejecución del programa de concientización en "*Seguridad de la Información*" para Tigo Costa Rica.	Definición de cronograma de ejecución de charlas virtuales y presenciales, e implementación de encuestas y cuestionarios, diseño de ambientes que permitan generar diferentes tipos de ataques dirigidos para	Capitulo IV; 4.4.2 Técnicas de Análisis de Información	Plataforma de comunicación interna, intranet

	medir el comportamiento de los colaboradores		
• Contribuir al desarrollo de la "*Seguridad de la Información*" para alentar a los usuarios a actuar de forma responsable y, por lo tanto, operar de forma más segura.	Diseño de un Plan de Sensibilización, capacitación y comunicación, que promueva el aumento en los índices de medición del nivel de madurez en temas relacionados con *"Seguridad de la Información*" en las herramientas de Millicom	Capitulo IV; 4.6 Descripción del Plan de sensibilización, capacitación y comunicación	Herramientas de nivel de madurez – Resultados de auditorías Millicom
• Presentar plantillas y herramientas para ser utilizadas como puntos de partida por el equipo de sensibilización.	Diseño de encuestas, cuestionarios, charlas y presentaciones.	Capitulo IV Marco metodológico, Capítulo V y Anexos	Plataforma de Millicom University
• Definir los lineamientos de introducción del personal a las tecnologías de la empresa.	Inclusión de Seguridad de la Información como parte de la inducción corporativa en todas las unidades del negocio	Capítulo V; Desarrollo de la Propuesta; 5.9 Proposición de valor	Plataforma de Millicom University
• Crear una conciencia de seguridad aplicable a los activos de información.	Diseño de estrategia para la ejecución de iniciativas y	Capitulo IV; 4.6 Descripción del Plan de sensibilización,	Herramientas de nivel de madurez – Resultados de

	programas de sensibilización, que promuevan el aumento de los niveles de madurez en "*Seguridad de la Información*"	capacitación y comunicación	Auditorias Millicom
• Reducir el riesgo de robo, fraude y mal uso de los medios a través de información vigente, de conocimiento público y la conciencia de seguridad dentro de la empresa.	Fomentar la conciencia e influir en el comportamiento de los colaboradores, para buscar disminuir la posible materialización de algunos riesgos críticos de seguridad y privacidad de la información.	Capítulo V, Desarrollo de la propuesta	Herramientas de nivel de madurez, control interno y resultados de auditorías Millicom
• Accesar a la información a través de medidas de seguridad, por parte de los usuarios.	Capacitar a las áreas técnicas sobre las líneas base definidas por los diferentes estándares y normas internacionales, enfocados a la protección y seguridad de la información.	Capitulo IV Marco metodológico, Capítulo V y Anexos	Plataforma de comunicación interna, intranet
• Crear un ambiente de confianza estableciendo la cultura dentro de la compañía, con respecto a la	Incremento de los niveles de madurez	Capitulo IV Marco metodológico, Capítulo V y Anexos	Herramientas de nivel de madurez, Control Interno y Resultados de Auditorias Millicom

seguridad de información que manipulan y corresponde al área gestionada.			
• Mejorar la imagen de confiabilidad y seguridad de la empresa, siendo elemento diferenciador de la competencia.	Diseño del programa de culturización en seguridad de la información.	Capitulo IV Marco metodológico, Capítulo V y Anexos	Herramientas de medición de imagen de mercadeo interno

2. CAPITULO II MARCODE REFERENCIA ORGANIZACIONAL Y SOCIOECONÓMICO

Millicom TIGO Costa Rica es una marca regional, con presencia en 15 países de América Latina y África. En ellos ofrecen servicios de internet, televisión por cable, telefonía fija, entre otros.

El nombre Tigo proviene del vocablo “Contigo”, que refleja la cercanía que tiene la marca con sus clientes alrededor del mundo. A nivel latinoamericano, Tigo opera en Guatemala, El Salvador, Honduras, Nicaragua, Colombia, Bolivia, Paraguay y Costa Rica. TIGO Costa Rica forma parte de Millicom International Cellular S.A. (MIC), con sede central en Luxemburgo. Las operaciones de MIC cuentan con más de 43 millones de clientes en Centroamérica, Suramérica y África. En un 90% de los mercados donde participa ocupa posiciones de líder, al ocupar el primero o segundo lugar.

2.1 Historia

Amnet, ahora Tigo, está presente en el mercado costarricense desde 1982, cuando su nombre era Cable Color. Fue la primera empresa en brindar servicio de televisión por cable en el país, específicamente en La Sabana, Escazú, Rohrmoser, Paseo Colón y Los Yoses.

En 1997, Cable Color fue adquirida por Amzak, compañía de capital canadiense-estadounidense y lanza su nueva marca Amnet. Luego, en 2008, Millicom International Cellular S.A. adquiere Amnet.

La compañía suma una serie de hitos en su historia, entre ellos:

- Primera en ofrecer canales digitales en 2003.
- Primera en enlazarse con el cable submarino maya en 2008. Por lo tanto, se convierte en la primera proveedora no estatal de internet en Costa Rica.
- En 2009, vuelve a innovar con el lanzamiento de su oferta de canales en alta definición.

- Para Tigo, este es el comienzo, y al mismo tiempo la continuación de un camino lleno de éxitos, que seguirá trayendo a los costarricenses productos que satisfagan sus necesidades y un mejor nivel de vida.

2.2 Tipo de negocio y mercado meta

Millicom TIGO Costa Rica es una empresa de telecomunicaciones que brinda servicios de internet, televisión paga y telefonía fija, con una participación en el 30% del mercado país. En cuanto a lo referente al mercado meta, TIGO Costa Rica no solo se enfoca en los hogares costarricenses con su marca Tigo Star, sino que también apunta al mercado corporativo por medio de Tigo Business.

2.3 Misión, Visión y Valores

Misión

"Facilitar la construcción de una vida de prosperidad y bienestar"

Visión

"Liderar la adopción del estilo de vida digital en Costa Rica"

Valores

"Pasión, confianza, innovación, integridad, simplicidad"

3. CAPITULO III ESTADO DE LA CUESTIÓN

Las personas son consideradas el elemento más débil y más propenso a falla en un sistema de seguridad. La falta de conciencia en los requerimientos de seguridad y las necesidades de control por parte de quienes gestionan y manipulan la información del negocio, administran los sistemas, operadores, programadores y usuarios, pueden representar el riesgo más importante para cualquier organización.

Los atacantes e intrusos pueden hacer uso de técnicas de ingeniería social y aprovechar la falta de conocimiento y conciencia de usuarios y operadores, para obtener información confidencial. En organizaciones donde no se ha implementado programas de concientización es común encontrar contraseñas escritas en papel de notas, debajo de los teclados, sobre el monitor del usuario, respaldos de información incompletos, errores de configuración en equipos, etc.

La idea fundamental de este proyecto se enfoca en la implementación de un modelo de trabajo repetitivo y enfocado en la *"Seguridad de la Información*". Este tiene como base de alcance crear la cultura y concientizar al recurso humano por medio de la definición y establecimiento de programas, metodologías, controles y políticas enfocadas en conservar la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

Un programa efectivo de sensibilización, capacitación y comunicación en "*Seguridad de la Información*" debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información. Estas, generalmente están plasmadas en las políticas y procedimientos de "*Seguridad de la Información*" que la entidad, requiere sean cumplidos por parte de todos los usuarios del sistema.

Cualquier incumplimiento a las políticas, debe imponer una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad, correspondiente a su rol de trabajo y responsabilidades dentro de la entidad.

SGSI: Las organizaciones en general, han ido tomando conciencia de la necesidad que tienen de soluciones en el ámbito de la "*Seguridad de la Información*", al tener en cuenta los objetivos de la empresa y aumentar el interés por esa "*Seguridad de la Información*" en los últimos años. De ahí nace la necesidad de las empresas de implementar SGSI (Sistemas de gestión de "*Seguridad de la Información*")

¿Qué es un SGSI? Se define como un programa que se enfoca en la definición de procesos, políticas, procedimientos, análisis, test, entrenamientos y transferencias de conocimiento, organizados de forma lógica y soportado por objetivos a nivel estratégico, estructurados principalmente por los requisitos presentados en los documentos internacionalmente reconocidos en el ámbito de la "*Seguridad de la Información*" y enfocados en la evaluación constante y mejora continua.

- "No se puede controlar lo que no se puede medir", Si los controles establecidos no se pueden medir, entonces no aportarán nada al SGSI.

Se toman como referencia, los principales estándares de seguridad orientados a la gestión y medición de la seguridad de los sistemas:

-Estándares FIPS (Federal Infomation Processing Standard) –140-1 y 140-2: Conjunto normalizado de códigos utilizados para asegurar los datos.

-SSE - CMM (Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas): Modelo derivado del CMM. Describe características fundamentales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas.

Primera versión en 1997 y actualización en 2003.

-La Serie 800 del NIST (National Insitute of Standards and Technology): Agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

-NIST SP 800 - 55 ("Métricas de Seguridad para Sistemas de Tecnologías de la Información"): Publicada en 2003 y revisada en 2007.

-NIST SP 800 - 80 “Guía para el desarrollo de métricas de seguridad de información”: Publicada en 2006.

ISO 27000

Formada por los estándares relacionados con la “*Seguridad de la Información*”, ya desarrollados o en fase de desarrollo.

- Ofrecen un marco de gestión de la “*Seguridad de la Información*”. Formando un conjunto de normas que especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI.

- Para implementar un SGSI y afrontar un proceso de auditoría satisfactoriamente, se requiere el conocimiento e interpretación, al menos de la 27001, 27002 y 27006.

Las dos normas más importantes y base de la familia son la 27001 y la 27002.

- El resto de normas se consideran complementarias a la 27001 y la 27002.Surgiendo como apoyo para la implementación en temas específicos o el proceso de auditoría del SGSI.

ISO/IEC 27002:2005

Publicada en 2007, corresponde a la ISO/IEC 17799:2005.

Es una guía de buenas prácticas para la implementación de un SGSI, al describir los objetivos de control y controles recomendables respecto a la seguridad de información. No es certificable. Tiene 11 cláusulas de control de seguridad o dominios, que cubren los principales aspectos relacionados con la seguridad. Contiene 39 objetivos de control y 133 controles.

ISO/IEC 27004:2009

Publicada el 7 de diciembre del 2009. Especifica las métricas de seguridad y las técnicas de medida aplicables para determinar la eficacia y eficiencia de la implantación de un SGSI y de los controles relacionados.

Estas métricas se usan principalmente para la medición de los componentes de las fases del "Do" (Implementar y Utilizar) del ciclo PDCA.

- Nace para marcar criterios de cara a una correcta medición de la eficacia de un SGSI.

- No aporta una colección de métricas o indicadores por aplicar a cualquier SGSI, sino que establece una metodología para determinar la efectividad de un SGSI, mediante actividades y procesos sin establecer medidores o usar los resultados por conseguir.

ISO/IEC 27004:2009

Objetivos:

• Facilitar la mejora de la efectividad de la "*Seguridad de la Información*".

• Evaluar la efectividad de la "*Seguridad de la Información*" y su mejora continua.

• Lograr información objetiva y análisis para ayudar en la revisión de la gerencia, la toma de decisiones y justificar mejoras en los controles.

• Evaluar la efectividad de los controles de seguridad y los objetivos de control.

- ISO/IEC 27004 se basa en el modelo PDCA, están las mediciones especialmente orientadas al "Do" (Implementación y operación del SGSI), como una entrada para el "Check" (Monitorizar y revisar), y así poder adoptar decisiones de mejora del SGSI mediante el "Act".

2.4 MARCO TEORICO

Un programa de sensibilización debe ser elaborado teniendo en cuenta como objetivo relevante el alineamiento con la misión de la empresa y el valor que se busca para la creación de la cultura empresarial.

Para lograr un adecuado diseño deben ser identificadas las necesidades y las prioridades que tenga la compañía, respecto al tema de entrenamiento y sensibilización del recurso humano. Esto, con el fin de proponer un diseño apto del programa.

Las políticas y los procedimientos de "*Seguridad de la Información*" surgen como una herramienta organizacional para delimitar y apoyar las acciones de cada uno de los miembros de la organización. De esta forma, se pretende crear una cultura sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la organización. Deben considerarse como reglas por cumplir y surgen para evitar problemas. Además, se establecen para dar soporte a los mecanismos de seguridad implementados en los sistemas y en las redes de comunicación.

Un plan de seguridad en una organización debe estar soportado por políticas y procedimientos que definan el porqué proteger un recurso; que quiere hacer la organización para protegerlo y cómo debe procederse para poder lograrlo.

La gestión de la "*Seguridad de la Información*" debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este lineamiento constituye una adecuada gestión de "*Seguridad de la Información*", que podría considerarse, por analogía con una norma tan conocida, como por ejemplo la ISO 9001, como el sistema de calidad para la "*Seguridad de la Información*".

Cuando una empresa define la "*Seguridad de la Información*" como prioridad, establece medidas que ayuden a conseguirla. De manera inmediata se plantea la necesidad de instalar mecanismos, llamémosles físicos, que permitan controlar los riesgos asociados a la seguridad más inmediata. Mecanismos entre los que se encuentran las medidas físicas aplicables al espacio en el que se ubican los sistemas que contienen la información, así

como controles preventivos y detectivos que refuercen las implementaciones ejecutadas. Pero, es de suma importancia que las personas que interactúan, gestionan o administran los dispositivos implementados reciban conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

2.5 MARCO CONCEPTUAL

Se presentan algunas definiciones importantes relacionadas al programa de "*Seguridad de la Información*" que se busca diseñar.

Sensibilización: Es un proceso por el cual se busca crear conciencia e influenciar sobre una persona para que perciba el valor o la importancia de algo e impactar sobre el comportamiento o bien, reforzar buenas prácticas sobre un tema en particular.

Entrenamiento: Proceso utilizado para enseñar habilidades, que permiten a una persona ejecutar funciones específicas asignadas a su cargo.

Información: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente o hablada. Actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.

Riesgo: Se define como cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia. Adicionalmente, para el caso de las compañías, se puede definir como el monto que están dispuestas a perder en caso de que se dé una catástrofe.

Política: Declaración de alto nivel que expresa los objetivos por cumplir de la entidad respecto a algún tema en particular.

Políticas de Seguridad: Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la "*Seguridad de la Información*". Es la base del SGSI.

Organización de la "*Seguridad de la Información*": Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

Gestión de activos: Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata de que cuenten con un nivel adecuado de seguridad.

Seguridad de los recursos humanos: Orientado a reducir el error humano, ya que, en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con "*Seguridad de la Información*". Busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

Seguridad física y ambiental: Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

Gestión de comunicaciones y operaciones: Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

Control de accesos: El objetivo principal es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

Sistemas de información, adquisición, desarrollo y mantenimiento: Básicamente busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

Gestión de incidentes de "*Seguridad de la Información*": Tiene que ver con todo lo relativo a incidentes de seguridad. Busca que se disponga de una metodología de administración de incidentes, que es básicamente definir de forma clara, pasos, acciones y responsabilidades.

Gestión de continuidad del negocio: Lo que considera este control es que la "*Seguridad de la Información*" se encuentre incluida en la administración de la continuidad de negocio. Busca a su vez, contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

Cumplimiento: Busca que la empresa cumpla estrictamente con las bases legales del país, al evitar cualquier incumplimiento de alguna ley civil o penal, alguna obligación reguladora o requerimiento de seguridad. A su vez, asegura la conformidad de los sistemas con políticas de seguridad y estándares de la organización.

Administración de riesgos: Se llama así al proceso de identificación, análisis y evaluación de riesgos.

"*Seguridad de la Información*": Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además de otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden también considerarse.

Sistema de Gestión de "*Seguridad de la Información*" (SGSI): Un SGSI o ISMS, de sus siglas en inglés (Infomation Security Management System). Es la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la "*Seguridad de la Información*".

Control: El control es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que se realicen los ajustes o correcciones necesarias, en caso que se detecten eventos que escapan a la naturaleza del proceso.

Brecha: Se denomina al espacio o ruta por recorrer entre un estado actual y un estado deseado.

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el SGSI.

Confidencialidad: La información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Integridad: Mantenimiento de la exactitud, lo completo de la información y sus métodos de proceso.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados, cuando lo requieran.

Ingeniería Social: Es un tipo de ataque a la seguridad en la cual un individuo busca la forma de manipular a otro, con la finalidad de conseguir información que puede ser utilizada para acceder a uno o varios sistemas, e inclusive suplantar la identidad de la víctima.

Hackitivismo: Es una forma de protesta realizada por aficionados o profesionales de la seguridad informática (Hackers) con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general, haciendo uso de los fallos de seguridad de las entidades o sistemas.

Log: ("registro", en español) es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

4. CAPITULO IV MARCOMETODOLÓGICO

4.1 Tipo de Investigación

Este trabajo se considera de investigación aplicada porque toma como base diferentes normas y estándares internacionales que se pueden aplicar. Estos detallan las diversas estrategias posibles por seguir para crear una cultura organizacional en "*Seguridad de la Información*", de los cuales se han tomado extractos que estén alineado con el alcance investigativo.

4.2 Alcance Investigativo

Actualmente, las empresas a nivel nacional e internacional son blanco de múltiples amenazas y ataques dirigidos a los colaboradores. Por medio de estos ataques, los ciberdelincuentes buscan tomar ventaja del desconocimiento y poca cultura existente en las empresas sobre temas de "*Seguridad de la Información*". Esto, con el fin de apoderarse de la información, ya sea con fines de negociar los datos, conocer estrategias, tomar represalias, cobrar recompensa por recuperación de los datos o bien como un trofeo personal de los "hackers".

El propósito de este programa de entrenamiento es reforzar los conocimientos y crear conciencia en la totalidad de los colaboradores de TIGO Costa Rica por medio de transferencias de conocimientos, ejercicios de concientización y medición constante.

En la actualidad el nivel de madurez en temas de seguridad es medido por las auditorías, tanto internas como externas, los cuales identifican hallazgos de la necesidad de la implementación de dicho programa de concientización en "*Seguridad de la Información*" en la totalidad de la organización.

4.3 Enfoque

El enfoque de este documento busca crear una cultura organizacional en temas relacionados con la "*Seguridad de la Información*", por medio de la implantación de un programa que detalla prácticas periódicas de entrenamientos, charlas, encuestas y test, así como medición

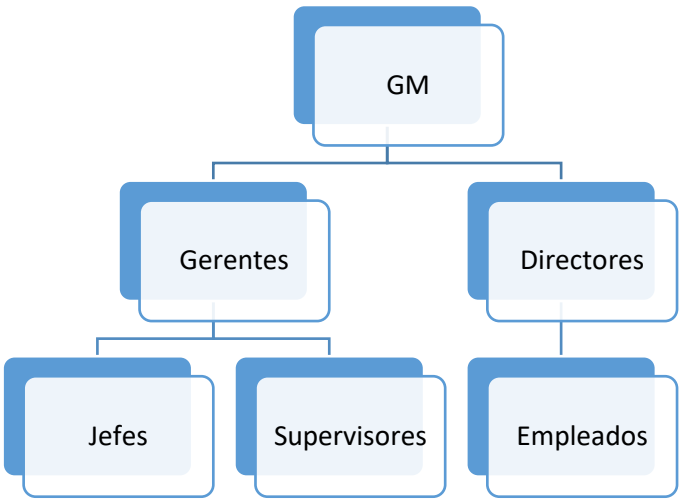
de los niveles de conocimiento de los colaboradores en los temas de mayor interés para el negocio.

Busca influir en el comportamiento de las personas que gestionan datos etiquetados como críticos para el negocio, crear conciencia en cuanto a los riesgos y responsabilidades que conllevan cada una de las posiciones a lo largo de la empresa.

4.4 Población y muestreo

Este programa está dirigido principalmente a grupos objetivo-específicos a lo interno del negocio, para que se pueda organizar iniciativas de sensibilización. De igual forma podría ser adoptado para transmitirse a los usuarios de los proveedores de servicio y contrato de TIGO Costa Rica.

Se definirá el tipo de muestra aleatoria simple. De esta forma se brinda la misma probabilidad a la totalidad de la población de ser elegida y agrupar por orden alfabético en segmentos de 100 colaboradores en cada muestreo. De esta forma, no se discrimina ni rango jerárquico, ni posición dentro de la empresa.



GM: El tomador de decisiones clave para la inversión en seguridad

Gerentes y Directores: Este grupo de usuarios no son expertos en seguridad, pero necesitan entender, apoyar e implementar los protocolos de "*Seguridad de la Información*".

Jefes y supervisores: A menudo no está técnicamente orientado. Este grupo de usuarios debe ser educado y entender la importancia de la *"Seguridad de la Información*". Esto les

permitirá implementar las políticas y controles de seguridad relevantes en sus áreas de negocios.

Empleados: Es el mayor número de usuarios dentro del grupo objetivo. Posiblemente, el más importante, como sugieren las investigaciones. La mayoría de las infracciones de "*Seguridad de la Información*" son causadas por un error humano

4.4.1 Instrumentos de recolección de datos

Una parte fundamental en la medición del comportamiento de los colaboradores ante la implementación del programa de culturización en "*Seguridad de la Información*" se obtiene de la recolección de datos, como elemento primario de la información. Para ello, existen diversas y variadas técnicas que apoyarán a obtener la información desde las fuentes primarias. En este caso, es el colaborador quien ofrece la información más confiable y real.

Entre los métodos por utilizar para la recolección de datos estarán los cuestionarios y encuestas, los cuales por medio de herramientas tecnológicas se harán llegar hasta los colaboradores. La utilización de estos permite analizar comportamientos y características claves de los colaboradores para cuantificar lo obtenido.

Las técnicas para la implementación se definirán en el cronograma de ejecución del programa de entrenamiento y sensibilización que se muestra en el diseño de dicho programa.

4.4.2 Técnicas de análisis de información

Se utilizan herramientas con el fin de poder abarcar la totalidad del negocio como

Gophish: Es una plataforma diseñada especialmente para crear campañas de ataques informáticos, como por ejemplo phishing. Con él se puede suplantar la identidad para obtener información confidencial o sensible del negocio, infectar equipos dentro de la arquitectura tecnológica y tomar control de ellos o bien monitorear de forma ocasional o constante el flujo de datos. Con Gophish se pueden crear fácilmente plantillas y definir los grupos objetivo, así como agendar los ataques de forma controlada y su distribución hacia diferentes segmentos de la red, departamentos u unidades organizativas. De igual forma la herramienta permite dar trazabilidad a los resultados de los ataques de forma detallada y en tiempo real.

Moodle: Es una herramienta de gestión de contenido de aprendizaje, la cual permite enviar de forma masiva o controlada las evaluaciones, quices, encuestas y cuestionarios. De forma simultánea tabular la información relacionada a cada envío como notas obtenidas, promedios, listados de avances y pendientes de ejecución.

Talent Center Millicom University: Herramienta interna de TIGO Costa Rica que permite registrar a los colaboradores y subir los módulos, talleres, presentaciones y videos a ser enviados a los diferentes grupos previamente definidos.

La conciencia del riesgo en los colaboradores y las diferentes formas disponibles de proteger la información. Deben de ser la primera línea de defensa para la seguridad del sistema de información y la red.

Un programa de entrenamiento debe proporcionar consejos prácticos sobre cómo generar conciencia sobre la "*Seguridad de la Información*" en los diferentes grupos a los cuales se les desea inculcar la cultura, especialmente en los colaboradores y usuarios de las diferentes tecnologías del negocio, así como mejorar la conciencia de "*Seguridad de la Información*"; ilustrar los principales procedimientos necesarios para planificar, organizar y ejecutar iniciativas de sensibilización sobre "*Seguridad de la Información*". Se busca implantar etapas definidas para procesos puntuales como planificar, evaluar, ejecutar y administrar.

La primera fase de planificación y evaluación se contempla como crítica para el éxito de cualquier programa. Es aquí donde las actividades clave se identifican y describen a los usuarios. En particular, este programa enfatiza la importancia de definir los objetivos y las metas de cada iniciativa; definir grupos objetivo; desarrollar un plan de comunicación; así como medir el éxito de los programas de concientización.

Además, cabe mencionar que plasmar un enfoque de gestión del cambio para las iniciativas de sensibilización es crucial, ya que ayuda a cerrar la brecha entre un problema particular y las respuestas humanas a la necesidad de cambiar.

Se incluyen plantillas y ejemplos de herramientas sugeridas para ayudar a los usuarios durante las diferentes fases de las campañas de sensibilización. De igual forma, también señala algunos posibles obstáculos que se podrían identificar para el éxito y proporciona consejos prácticos sobre cómo superarlos durante las fases de planificación e implementación. Además, describe los principales factores para el éxito de cualquier iniciativa de "*Seguridad de la Información*". Por ejemplo, se deben determinar las líneas

base para el estado actual antes de implementar o modificar el programa de concientización y obtener una adecuada difusión. Es de suma importancia en cualquier campaña de concientización, ya que crecerá en impacto al aumentar el número de personas que reciben el mensaje.

Con este documento se busca brindar herramientas valiosas para preparar e implementar la concientización entre los colaboradores de TIGO Costa Rica, lo cual es un primer paso importante para enfrentar este desafío.

Diseño

El programa de cultura está diseñado en varias etapas y tareas distribuidas en tareas puntuales a lo largo de dos años. Cada una de las etapas busca transmitir una enseñanza sobre temas precisos, alineados según un marco de gestión de seguridad. La información plasmada es indispensable conocer y transferir para poder tomar decisiones e influir en el comportamiento de las personas.

Imagen #1 Cronograma de entrenamiento y sensibilización

El programa de entrenamiento y concientización de "*Seguridad de la Información*" está compuesto por un kit de herramientas y materiales que buscan guiar de forma programada el proceso a lo interno de la empresa.

El primer paso de la formación del conocimiento inicia con un cuestionario de sensibilización. (**ver anexo 1-2**) Tienen como objetivo evaluar el nivel de conocimiento y conciencia en seguridad de los colaboradores. A la vez, despertar el interés por aprender más sobre los temas relacionados, así como crear la preocupación en los empleados sobre lo vulnerables que son y que deben de ser precavidos a la hora de ejecutar y manipular la información. Este primer paso se lanzará de forma sorpresiva por medio de la herramienta interna de entrenamiento "Centro de Talento". Se plantea el envío de encuestas de sensibilización con una periodicidad bimensual o bien trimestral.

El paso siguiente se enfoca en enviar a los colaboradores una encuesta de sensibilización (**ver Anexo 3**). Dicha encuesta será elaborada de forma bianual. La misma busca medir y evaluar sobre los conocimientos reales de cada individuo en lo que a "*Seguridad de la Información*" se refiere. Es tomado como punto de medición aspectos básicos de la seguridad y se exige obtener una nota superior al 80% para aprobar el proceso. De lo contrario, el colaborador deberá asistir a un proceso de formación en líneas base, y retomar la prueba en un periodo no mayor a los 3 meses. Con esta evaluación se busca formar conciencia de una realidad concreta, percatarse de ella, verla casi como si fuera un objeto que tuviese ante los ojos. El proceso de concientización es el medio por el cual se asegura que se conozca un programa de seguridad de información, así como sus políticas y normativas aplicables, "permean" en el personal de todos los niveles de la organización. De la efectividad de estos programas depende la velocidad de la organización para implementar adecuadamente la "*Seguridad de la Información*". Si todo es efectivo, se puede comparar con un jet, pero si no está resultando, el proceso es algo tortuoso, entonces es como si se usara un vehículo terrestre.

De forma paralela se trabajará en los equipos de cómputo como medio de contacto más directo hacia los colaboradores para crear conciencia, valiéndose de elementos visuales que servirán principalmente para sensibilizar y reforzar los principios básicos de la "*Seguridad de la Información*". Se diseñó una campaña de fondos de pantalla (**ver anexo 4**), en el cual

se incluyen una serie de consejos que buscan enfatizar los temas tratados y mencionados en las políticas de "*Seguridad de la Información*" de TIGO Costa Rica.

Los consejos son imágenes que se pueden publicar en el blog interno, en la intranet. Pueden ser enviadas por correo electrónico dentro de un marco de formación continua. Pueden ser impresas y utilizadas como posters. También pueden ser utilizadas como nuevos fondos de escritorio y/o salvapantallas. Se deja a la empresa la toma de decisión de cómo utilizar estos consejos de seguridad.

La idea se enfoca en «publicar» uno o dos consejos de seguridad cada mes, pero nunca más, porque no se debe saturar a los empleados con excesiva información.

Una idea opcional es organizar alguna actividad (a criterio de la empresa) que esté relacionada con el consejo que se publica cada mes. De esta manera, se consigue que los empleados, además de recordar y asimilar estos consejos, se involucren y los apliquen de alguna manera práctica.

Una vez creado el interés que se espera haber generado hasta este punto, se plantea realizar un proceso formativo, el cual consta de charlas presenciales, basado en presentaciones por medios de diapositivas (**ver anexo 5**). Estas serán agendadas por parte del área de "Rendimiento y desarrollo interno". Estas charlas están orientadas a ofrecer un crecimiento inductivo que buscará facilitar la integración a los nuevos colaboradores y brindar conocimiento sobre las políticas, el buen uso y aprovechamiento de los recursos tecnológicos. De igual forma, ofrecen un enfoque preventivo. Esto significa orientar y prever los cambios que se producen en el personal y prepararlos para enfrentar de forma exitosa las nuevas formas de ataque cibernético, virus, cambios en las metodologías de trabajo informático, actualizaciones e implementaciones de nuevos procesos en temas tecnológicos de la empresa. Por último, brindar un tipo de aprendizaje correctivo por ser orientado a solucionar problemas identificados, mediante los estudios de diagnósticos de los sistemas de la información de la empresa.

Como parte de las charlas presenciales se creó una Campaña Phishing (**ver Anexo 6**). Esta consiste en transmitir conocimiento sobre los diferentes métodos de identificar el tipo de ataque. Así mismo se diseñó un laboratorio, desde donde se enviará una serie de correos maliciosos que buscarán tratar de engañar a los colaboradores por medio de un fichero

infectado en un correo electrónico, el cual al ser ejecutado, muestra al usuario un portal Web advirtiéndole del peligro que supone lo que acaba de hacer.

Para realizar esta campaña se utilizarán cuentas de correo electrónico ficticias, pero con características que sean similares a las demás cuentas del negocio (nombre y apellidos de un empleado, o cuenta de un departamento área del negocio). Ejemplos: sistemas@empresa.com, Seguridad@empresa.com, o nombre.apellido@empresa.com
Empleando estos tipos de cuentas de correo, se enviar mensajes electrónicos en el que, mediante un texto previamente definido, se pide a las posibles víctimas que ejecuten el archivo que se incluye en el adjunto del correo electrónico. Al darle click al documento adjunto, se redireccionará el equipo de cómputo hacia un mensaje de advertencia sobre los riesgos de las acciones ejecutadas por el colaborador.
Este correo electrónico puede enviarse a todos los empleados o a un número determinado de destinatarios que de forma aleatoria serán parte del experimento, por supuesto sin su previo conocimiento.
Es recomendable, para dar credibilidad al correo, que éste lleve incluido en copia (campo CC) a algún cargo importante de la empresa. Antes, debe obtenerse el permiso explícito de esta persona para incluirlo en la prueba.
El asunto o descripción de correo debe ser el título con el que se requiere que lleguen los correos, por lo que debe ser lo más claro y creíble posible.

Resultado esperado

Se espera transmitir conocimientos y a la vez generar conciencia en los colaboradores sobre qué es la técnica del phishing, cómo identificarlo, los peligros relacionados con esta técnica de ataque. Con base en esto, crear una cultura sobre el uso responsable de los correos electrónicos, la información y los activos del negocio. Se busca modificar de forma paulatina los hábitos considerados como inseguros por aquellos comportamientos más seguros. Respectos a la protección de la información institucional, y las conductas que dictan menor riesgo.

4.5 Implementación

La gran mayoría de los colaboradores desconoce sobre temas de "*Seguridad de la Información*" y su ámbito de alcance. Actualmente numerosos estudios muestran que la mayor cantidad de ataques a la "*Seguridad de la Información*" provienen del interior de las propias empresas, de ahí la importancia de implementar programas que apoyen en la concientización y entrenamiento en los temas relacionados dentro de la entidad.

El programa de "*Seguridad de la Información*" comprende una seria de actividades, proyectos, iniciativas y recursos que serán requeridos para ser aplicados de manera conjunta y colectiva con las áreas del negocio, con el fin de proporcionar servicios de seguridad a la organización. Tiene como propósito llevar a la práctica el plan trazado que busca alcanzar los objetivos de protección de los activos y los datos.

Con el fin de alcanzar el éxito en las actividades definidas es necesario conocer el estado actual de la seguridad, así como tener clara la postura que se desea alcanzar con la ejecución del programa. Una referencia sobre el estado deseado de la seguridad suelen ser las buenas prácticas en la industria, plasmadas en estándares internacionalmente reconocidos.

4.6 Descripción del "Plan de sensibilización, capacitación y comunicación"

En la era digital en la que se vive y trabajamos actualmente, los ciudadanos y las empresas ven que las tecnologías de información y comunicación (TIC) agilizan y facilitan cada vez más nuestro vivir. Por ende, son consideradas cada vez más, como invaluables en las tareas diarias.

Al mismo tiempo, ante tan creciente interacción con las tecnologías, los ciudadanos y empresas se enfrentan constantemente a riesgos de exposición y violaciones a la "*Seguridad de la Información*", ya que las vulnerabilidades existentes en las tecnologías, la convergencia, el uso creciente de las conexiones siempre activas de usuarios y el desconocimiento de los riesgos crean brechas que día con día se ensanchan más y exponen la confidencialidad de los datos.

Estas brechas de seguridad pueden estar relacionadas con TI. Por ejemplo, a través de virus informáticos, o pueden estar socialmente motivadas, a través del robo de equipos. En una época cada vez más dependiente de la información digital, hay un número cada vez mayor de peligros. Una cantidad considerable de ciudadanos desconoce su exposición a los riesgos de seguridad.

Con el avance y la multiplicación de estos peligros, las soluciones de "*Seguridad de la Información*" de hoy, serán obsoletas mañana. El panorama de seguridad cambia continuamente. La mayoría de especialista en el área de la seguridad tecnológica indican según análisis y estudios que el ser humano es el eslabón más débil de cualquier marco de "*Seguridad de la Información*".

Ante esto, se evidencia que solo un cambio significativo en la percepción y comportamiento del usuario o la cultura organizacional puede reducir de manera significativa el número de faltas a la "*Seguridad de la Información*".

Es evidente que existe una deficiencia importante en la conciencia de la "*Seguridad de la Información*" de forma generalizada. Por ejemplo, la mayoría de usuarios, tanto en sus hogares como en sus lugares de trabajo, desconocen que sus computadoras personales pueden ser controladas sin su conocimiento por los hackers, para cometer fraude de identidad electrónica o como parte de una red organizada para lanzar ataques de denegación de servicio.

La principal finalidad de este trabajo es aconsejar y ayudar a TIGO Costa Rica a desarrollar una mejor comprensión de la sensibilización para ayudar a propagar la seguridad y el uso responsable de las TIC.

TIGO Costa Rica reconoce que incrementar la conciencia de los riesgos y las diferentes formas disponibles de asegurar la información es la primera línea de defensa para la seguridad de los sistemas y redes de información. Por lo tanto, la aplicación de este programa busca facilitar consejos prácticos para estar preparados e implementar iniciativas de sensibilización relacionadas con la "*Seguridad de la Información*". La información cubierta presenta consejos paso a paso para ayudar a formar la base de una campaña de concientización efectiva y específica.

Este programa se enfoca en resultados de estudios, análisis y resultados de auditorías realizados en la empresa durante varios años.

El programa debe explicar de forma clara y adecuada los lineamientos deseables por seguir para el uso de las tecnologías y la información. Estos deben ser expuestos en políticas y procedimientos relacionados con la "*Seguridad de la Información*" que la empresa busca sean cumplidos por sus colaboradores y usuarios de las tecnologías que apoyan al negocio.

Es de suma importancia que todo incumplimiento a las políticas debe conllevar una sanción, siempre y cuando el colaborador y/o usuario haya recibido de forma adecuada el entrenamiento y se le haya comunicado sobre el contenido de seguridad relacionado con aspectos como rol y responsabilidad que desempeña y para lo cual fue contratado.

Luego de lo anteriormente comentado, se han definido fases que se deberán llevar a cabo para la ejecución del plan de sensibilización, capacitación y comunicación:

Estrategia general para la ejecución de iniciativas y programas de sensibilización

A continuación, se detallan los procesos principales y necesarios para planificar y ejecutar una iniciativa de concienciación sobre "*Seguridad de la Información*", además de plantear y definir las etapas de planificar y evaluar, ejecutar y administrar, evaluar y ajustar.
Cada proceso ha sido analizado para identificar acciones y dependencias de tiempo determinado.
Este modelado de procesos proporciona una base para "poner en marcha" las actividades de análisis y planificación, ejecutar y evaluar un programa y una comprensión consistente y sólida de los principales procesos y actividades. También se presentan plantillas y herramientas para ayudar a los usuarios a comprender mejor cómo implementar la estrategia para ejecutar iniciativas y futuros programas.

Planificar y evaluar

Confirmar el equipo del programa: Se debe conformar un equipo para iniciar el proceso de planificación de un programa de concientización. El objetivo principal del equipo es planificar y organizar la iniciativa al completar la tarea prevista en esta primera fase.

Adoptar un enfoque de gestión del cambio: Es crucial adoptar un enfoque de gestión del cambio en una iniciativa de sensibilización, ya que ayuda a cerrar la brecha entre un problema en particular y las respuestas humanas a la necesidad de cambiar, incluso en el caso de un cambio cultural.

El uso de los principios básicos de la gestión del cambio (comunicaciones específicas, participación, capacitación y evaluación) ayudará a asegurar que se cumplan los objetivos de las iniciativas de sensibilización, así como a proporcionar una plataforma sólida para programas futuros o posteriores.

El cambio debe ser administrado de manera integral para garantizar que los esfuerzos se integren y que el cambio logre beneficios reales y perdurables. Para apoyar un programa de concientización, es importante acordar los siguientes principios para el cambio:

- Identificar y envolver a las partes interesadas clave en la toma de decisiones, planificación, implementación y evaluación.
- Establecer un objetivo claro para el punto final de cambio, en consulta con las partes interesadas clave
- Definir claramente los roles y las responsabilidades.
- Vincular e integrar elementos clave del cambio
- Gestionar las barreras de riesgo y de dirección para cambiar
- Proporcionar liderazgo en todos los niveles para el proceso de cambio
- Comunicación de manera oportuna, honesta y clara
- Permitir la flexibilidad en los enfoques para adaptarse a las diferentes necesidades de las partes interesadas
- Recursos, soporte y gestión del cambio
- Apoyo con capacitación y desarrollo para garantizar un cambio en el comportamiento y la cultura
- Aprender de experiencias previas y actuales, desarrollar capacidades para el cambio y celebrar el logro

Obtención de apoyo de gestión y financiación adecuados: Obtener el apoyo de la gerencia y el patrocinio para el programa de concientización es quizás el aspecto más crucial de toda la iniciativa. Es vital construir un consenso entre los tomadores de decisiones para que el programa de concientización sea importante y digno de financiamiento. Aquí es donde entra en juego el concepto de gestión de las partes interesadas. Si las partes interesadas clave no respaldan los objetivos y las metas, la iniciativa no avanzará

Identificar el personal y el material necesarios para el programa: En esta etapa del proceso, es hora de determinar qué se necesita en términos de personal y materiales. Un primer paso lógico es comenzar a buscar dentro de la organización los recursos apropiados. El personal dentro de IT, RH, Comunicaciones, Capacitación y Desarrollo probablemente tengan experiencia y antecedentes más adecuados para un programa de concientización

Consejos y lecciones aprendidas de colegas y / u otros miembros que manejan materiales y experiencia. Además, la consulta con ellos cumple un propósito de gestión de las partes interesadas, ya que puede ayudar a obtener su apoyo para la ejecución del programa en el futuro. No involucrar a colegas puede ponerlos inadvertidamente en contra.

Evaluar soluciones potenciales: Al evaluar las posibles soluciones, una consideración principal es si el programa de concientización se mantendrá en la casa o fuera de ella. Con el tiempo, el uso de la contratación externa como una decisión estratégica ha aumentado. Ahora, las organizaciones y las instituciones reconocen mejor las áreas de operación en las que se destacan y las que pueden realizar de manera efectiva los socios externos. Este cambio trae consigo el desafío de decidir si subcontratar; identificar qué se puede subcontratar; la naturaleza de la relación de tercerización y la selección de socios que no amenacen el éxito de programas e iniciativas futuras.

Seleccionar soluciones y procedimientos: El resultado final del paso de evaluación puede no haber producido un gran éxito, sino una decisión de mantener algunas partes del programa en la casa, subcontratar otras partes a uno o más proveedores externos. Parte del paso de selección implica negativas; quizás una aclaración adicional del presupuesto, el precio y los términos, así como también lo que se debe producir y en qué marco de tiempo.

Preparar plan de trabajo: Una vez que la solución ha sido seleccionada y el equipo designado, se recomienda preparar un plan de trabajo. En esta etapa, el plan de trabajo

incluirá solo las principales actividades para las cuales se revisará tan pronto como se desarrolle el programa.

Definir metas y objetivos: Es importante comenzar a prepararse para cualquier programa de conciencia de seguridad y determinar lo que aspira lograr. Se debe tomar en cuenta que hasta que los objetivos sean claros; será problemático tratar de planificar y organizar un programa y la evaluación del programa es claramente imposible. Seguidamente, se incluye una serie de preguntas para ayudar a facilitar el establecimiento de las metas y objetivos del programa.

Para determinar lo que intenta lograr durante una iniciativa de sensibilización, piense cuidadosamente sobre las siguientes preguntas básicas:

- ¿Existe actualmente algún programa de "*Seguridad de la Información*" o este esfuerzo es una nueva iniciativa en su organización? Quizás no exista otro programa de "*Seguridad de la Información*". Pero, ¿existe algún otro programa de concienciación que pueda usarse como un ejemplo probado o un punto de partida?
- ¿El programa se enfocará únicamente en la concientización o incluirá entrenamiento y educación, o una combinación de estos?
- ¿Cuáles son los temas específicos que cubrirá el programa? ¿Qué temas relacionados también podrían incluirse?
- ¿En qué frecuencia el programa agregará individuos? ¿Es la frecuencia adecuada para mantener el tema de la "*Seguridad de la Información*" en la mente de las personas?
- ¿Cuál es el nivel adecuado de información (y detalle) para proporcionar consejos valiosos a las audiencias objetivo? ¿Debería ser en profundidad o es suficiente una visión superficial?

Definir grupo objetivo: Es fundamental definir la audiencia específica a la que apunta la iniciativa de sensibilización. Las preguntas para ayudar a definir grupos objetivo incluyen:

- ¿A quién se dirige el programa de sensibilización?
- ¿Las necesidades de los grupos meta son las mismas, o tienen diferentes requerimientos de información? ¿Hay grupos que requieren información radicalmente diferente?

Ejecutar y administrar

Confirmar el equipo del programa: La segunda fase, el programa pasa al modo de ejecución. Cada miembro del equipo de concienciación tendrá que desempeñar un papel específico para implementar y gestionar la iniciativa. Antes de iniciar el programa, se debe confirmar el equipo responsable, tanto de la ejecución como de los resultados.

Revisar el plan de trabajo: Antes de iniciar el programa, se debe actualizar el plan de trabajo y determinar los hitos del programa para que cumplan con las metas y los objetivos, así como los requisitos presupuestarios.

Lanzar e implementar el programa: El trabajo realizado en los pasos anteriores se combina con aquellos en los que la fase anterior puede haber parecido dura y burocrática. Pero, en este punto, todo el tiempo dedicado a decidir los requisitos, diseñar la solución y perfeccionar el resultado, dará sus frutos ya que la implementación será más fluida y más efectiva.

Con un plan bien diseñado y los recursos adecuados para entregarlo, ha llegado el momento de solicitar el apoyo de los colegas internos y proveedores externos elegidos para desarrollar y ejecutar el programa, con el objetivo de obtener los beneficios de la conciencia en información de seguridad.

Entregar comunicaciones: La sensibilización se trata de comunicar a los grupos destinatarios seleccionados. Ahora es el momento de implementar el plan de comunicaciones. Es igualmente importante recopilar comentarios sobre las comunicaciones que el programa ha entregado. Esta retroalimentación proporcionará información valiosa que debe tomarse en consideración para futuros ciclos de entrega de comunicaciones.

Documentar las lecciones aprendidas: A medida que el programa se ha lanzado e implementado, es importante capturar las lecciones aprendidas durante esta segunda fase. El procedimiento completado al final de la Fase 1 debe repetirse. Será interesante comparar la evolución histórica del programa desde esta perspectiva de aprendizaje.

5. CAPITULO V DESARROLLO DE LA PROPUESTA

Proyecto de entrenamiento y concientización de "*Seguridad de la Información*".

Versión Control

Date	Version	Description	Autor
05 de febrero del 2018	1.0	Primer borrador	Alexander Fonseca Caravaca

ApprovalHistory

Approved	Revised	Position
		Country Manager
		ChiefOperationsOfficer
Observations:		
Date:	Día, Mes, Año	
VersionApproved:	<1.0>	

Imagen #2Cuadro de revisión de versiones

5.1 Blueprintlevel 1

Título: Programa de concientización y entrenamiento de "*Seguridad de la Información*".

Audiencia: Colaboradores TIGO Costa Rica

Autor: Alexander Fonseca Caravaca – Chief Infomation Security Officer-CR

5.2 Conocimiento del negocio

Una de las mayores amenazas a la "*Seguridad de la Información*" en realidad podría venir desde dentro de una empresa u organización. Los ataques internos se consideran algunos de los más peligrosos, ya que estas personas ya están bastante familiarizadas con la infraestructura. No son siempre trabajadores descontentos o espías corporativos, la única amenaza. A menudo los intentos no malintencionados, por estar desinformados causan un daño mayor.

La atención se centrará en los usuarios no informados que pueden hacer daño a su red al visitar sitios web infectados con malware, en respuesta a correos electrónicos de phishing. El almacenamiento de su información de acceso en una ubicación no segura, o incluso dar información confidencial cuando el empleado es expuesto a ingeniería social.

Una de las mejores maneras de hacer que los empleados de la empresa no cometan errores costosos en lo que se refiere a la "*Seguridad de la Información*" es instituir las iniciativas de formación de seguridad y concientización en toda la empresa. Pero, no debe limitarse a sesiones de entrenamiento, y estilo salón de clases, la conciencia de seguridad, sitios web (s), consejos útiles a través de e -mail, o incluso carteles. Estos métodos pueden ayudar a asegurar los empleados a tener una sólida comprensión de la política de seguridad de la empresa, procedimientos y mejor prácticas.

5.3 Objetivo

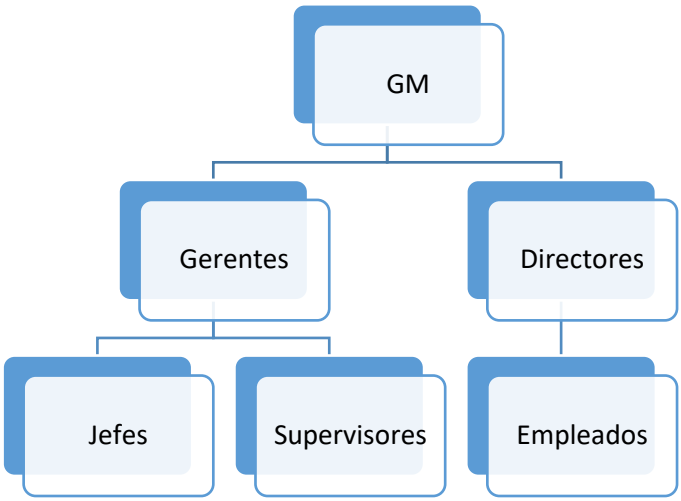
- Aumentar la "*Seguridad de la Información*" mediante cambios en el comportamiento de los colaboradores en sus espacios de trabajo, de cara a la tecnología brindada por la compañía para el cumplimiento de sus deberes.
- Proteger la información confidencial propiedad de TIGO mediante la aplicación de mejores prácticas con respecto al manejo de la información confidencial.
- Despertar en el personal de TIGO la necesidad de proteger la información mediante el cumplimiento de la política y así contar con controles asociados a elementos de información.
- Definir los roles y responsabilidades para el cumplimiento del presente estándar de concientización.

5.4 Alcance

Este programa pretende abarcar la totalidad de colaboradores a lo interno del negocio. Se enfoca en organizar iniciativas que buscan sensibilizar al recurso humano sobre los riesgos relacionados con las tecnológicas y la gestión de la información. Este programa de igual forma podría ser adoptado para transmitirse a los usuarios en pequeñas y medianas empresas que presten algún servicio a TIGO Costa Rica.

Como parte del alcance se definieron de forma estratégica la distribución de grupos según la criticidad de la información del negocio que manejan y el poder de decisión. Esto con la finalidad de clasificar las metodologías por seguir durante los procesos de entrenamiento e inducción.

El siguiente diagrama muestra los agrupamientos realizados:



GM: El tomador de decisiones clave para la inversión en seguridad, es quien gestiona la información más crítica del negocio y área responsable de la operación país.

Gerentes y directores: Este grupo de usuarios no son expertos en seguridad, pero necesitan entender, apoyar e implementar los protocolos de "*Seguridad de la Información*". Gestionan en su día a día información crítica y sensible del negocio.

Jefes y supervisores: A menudo no está técnicamente orientado, Este grupo de usuarios debe ser educado y entender la importancia o "*Seguridad de la Información*". Esto les permitirá implementar las políticas y controles de seguridad relevantes en sus áreas de negocios.

Empleados: Es el mayor número de usuarios dentro del grupo objetivo. Posiblemente, el más importante. Sugieren las investigaciones que la mayoría de las infracciones de "*Seguridad de la Información*" son causadas por un error humano.

5.5 Responsabilidades

Oficial de Seguridad de la Información

- El Oficial de Seguridad de la Información se asegurará que todo el material desarrollado e incluido dentro del "Plan de Concientización de Seguridad de la Información" llegue a cada uno de los colaboradores en el tiempo indicado.
- El Oficial de Seguridad de la Información asegurará la eficiencia del material

enviado a cada uno de los colaboradores de TIGO.

- El Oficial de Seguridad de la Información implementará los medios que permitan la realimentación al presente plan, por parte de los colaboradores.
- El Oficial de Seguridad se asegurará que el plan esté vigente y pueda ser modificado en cualquier momento, en caso de ser necesario.
- El Oficial de Seguridad de la Información deberá de conocer en todo momento el estatus de ejecución del Plan de concientización de "*Seguridad de la Información*".

Gerencias

- Trabajar en conjunto con el Oficial de Seguridad de la Información en la implementación del Plan de Concientización de "*Seguridad de la Información*".
- Cumplir con su rol como custodio de la información cuando sea aplicable dentro de la ejecución del plan.
- Considerar el reforzamiento de temas incluidos en el plan para aquellos puestos que así lo ameriten.
- Asignación de tiempo para sus colaboradores, a fin de que puedan participar de la ejecución del plan.
- Asegurarse que todos los colaboradores a su cargo, así como personal subcontratado o terceros, a los cuales les aplique, hayan pasado por el proceso de capacitación y concientización necesarios, antes de brindarles acceso a la información de TIGO.
- Asegurarse que cada colaborador a su cargo, así como personal subcontratado conozca las reglas específicas con respecto a la "*Seguridad de la Información*" en TIGO.
- Trabajar para reducir la posibilidad de incidentes de *"Seguridad de la Información*" de los usuarios por falta de sensibilización y capacitación a los usuarios.

Usuarios

Los usuarios constituyen el filtro más importante ante la comisión de incidentes por parte de colaboradores y terceros en TIGO:

- Entender y cumplir con las políticas y procedimientos relacionados con la "*Seguridad de la Información*".
- Participar de los entrenamientos relacionados con la "*Seguridad de la Información*" activa, para aquellos sistemas en los cuales cuenta con acceso.
- Reportar cualquier requerimiento de capacitación relacionado con la "*Seguridad de la Información*".
- Reportar el comportamiento extraño por parte del equipo de cómputo asignado, así como cualquier incidente de "*Seguridad de la Información*".

Algunos de los elementos más importantes para cubrir en el programa de concientización de seguridad son:

1. La importancia de la formación en temas de seguridad.
2. La política de seguridad de la organización.
3. Incumplimientos a políticas.
4. Clasificación y manejo de datos.
5. Espacio de trabajo y escritorio.
6. Gestión y uso adecuado de contraseñas
7. Protección contra virus, tormentas de virus, otros tipos de virus y su comportamiento.
8. Phishing
9. Fraudes
10. Malware
11. Intercambio de archivos.
12. Derechos de autor.
13. Utilización del WEB
14. Monitoreo sobre el uso de internet.
15. Respaldos y recuperación.
16. Ingeniería social y sus diferentes técnicas.

17. Teletrabajo
18. VPN
19. Accesos, mínimo privilegio
20. Seguridad a nivel de redes inalámbricas.

5.6 Modelo de negocio

Las campañas en "*Seguridad de la Información*" consisten en general, en actividades de sensibilización y sesiones educativas dirigidas a públicos específicos. Estas sesiones son buenas oportunidades para empezar a informar a los departamentos de su información, responsabilidades de seguridad. La función de recursos humanos en conjunto con el equipo de seguridad es la concienciación de los nuevos empleados. La formación debe incorporar material que demuestra la importancia de la seguridad de la empresa.

5.7 Usuarios finales

La mayoría de las organizaciones proporcionan múltiples capas de defensa en profundidad. Por lo general, las tecnologías tales como firewalls, antivirus, IPS/IDS. Sin embargo, las amenazas tecnológicas pueden pasar por alto fácilmente estas capas defensivas que apuntan a los empleados. Estos utilizan técnicas como el phishing, descargas no autorizadas, llamadas telefónicas o correos de ingeniería social, aplicaciones con troyanos o memorias USB infectadas, etc.

5.8 Requerimientos funcionales

- Es importante plasmar y dar a conocer la importancia sobre crear cultura en "*Seguridad de la Información*" así como la implementación de un programa que apoye en la culturización de los colaboradores en "*Seguridad de la Información*", y de esta manera entender el por qué los empleados y la empresa requieren este programa.
- Actualmente se llevan a cabo entrenamientos básicos de "*Seguridad de la Información*" para nuevos empleados. Se desean extender estas capacitaciones con temas adicionales a toda la compañía.

5.9 Proposición de valor

- Se propone capacitar a todo el personal en temas claves y básicos establecidos por los diferentes estándares y normas internacionales relacionados a "*Seguridad de la Información*" como mínimo. Se requerirá que todo el personal tome la capacitación anual. Además, de la formación, este programa de sensibilización y educación incluirá lo siguiente:
    - Campañas de fondos de pantalla
    - Encuestas de sensibilización.
    - Evaluaciones de conciencia no programadas periódicamente para asegurar el cumplimiento de la capacitación.
    - Encuestas de opinión para mejorar el entrenamiento del programa de sensibilización y educación.
- En este momento se está capacitando al personal nuevo en "*Seguridad de la Información*" como parte de la inducción corporativa en todas las unidades de negocio.

- No importa lo mucho que la organización invierta en tecnología de seguridad. A menos que la gente sea entrenada y que sepa que seguirá siendo vulnerable a los ataques humanos. Los usuarios más importantes son los empleados, a los cuales se les debe extender el conocimiento en cuanto a la "*Seguridad de la Información*".

5.10 Canales

- Los canales por utilizar para llevar a cabo este programa son:
    1. Fondos de pantalla.
    2. Entrenamientos online.
    3. Entrenamientos en sitio.
    4. Boletines y videos (Intranet).

5.11 Recursos clave

Consideramos que todos los recursos son claves, por ende, requieren formar parte en nuestra propuesta de valor, de igual forma nuestros canales de distribución así como los usuarios finales y los consultores técnicos.

Es requerido obtener todo tipo de apoyo para implementar esta propuesta algunos puntos clave son:

- Capital para las capacitaciones especializadas para GM, GM-1, GM-2.
- Desarrollo de material de ayuda (fondos de pantalla, posters, entre otros) proporcionados por Marca.
- Tiempo del recurso para participar en las actividades remotas y en sitio.
- Permiso para utilizar los recursos existentes en la compañía para distribuir mensajes de "*Seguridad de la Información*" (correo, Yammer, Intranet).

5.12 Actividades clave

Algunas de las actividades que visualizamos como importantes y necesarias de desarrollar de manera óptima para la implementación de este modelo son las siguientes:

- Encuestas de sensibilización.
- Evaluaciones de conciencia no programadas periódicamente para asegurar el cumplimiento de la capacitación.
- Encuestas de opinión para mejorar el entrenamiento sobre el programa de sensibilización y educación.
- Entrenamientos en sitio.
- Entrenamientos on-line.

5.13 Patrocinadores principales

La "*Seguridad de la Información*" debe de ser una responsabilidad compartida de todos los niveles de la organización. Por ende, es requerido el apoyo de todas las áreas para una adecuada gestión del programa de culturización en "*Seguridad de la Información*", pero debe estar dirigida por un plan y debe contar con una adecuada coordinación.

Para lograr esto es requerido el soporte y compromiso de la alta Dirección, lo cual es un factor clave para poder llevar a cabo un buen plan de capacitación.

A continuación, se detalla el cuadro de patrocinadores considerados como claves para realizar una implementación adecuada:

Posición	Importancia	Nivel de Compromiso Meta	Estrategias de Compromiso
General Manager	High	High	Punto de apoyo clave para el cumplimento de la campaña de seguridad.
Chief Technical Officer	High	High	Apoyo general al programa de concienciación de "*Seguridad de la Información*".
Infomation Security Officer	High	High	Mostrar valor del proyecto, cumplimiento, proyecto, mantener comunicaciones cortas y eficientes.
Internal Control	Medium	Medium	Interesados en cumplimiento.
Marketing / Communications	Medium	High	Este grupo es la clave para una comunicación exitosa. Coordinar con ellos con anticipación para asegurar que se está siguiendo la política de comunicación corporativa.
Human Resuorces (Tigo People)	Medium	High	Explique el valor sobre cómo puede ayudar a educar a la gente sobre las políticas. Facilitador de capacitaciones (online/en sitio).

Imagen #3 Cronograma de principales patrocinadores

5.14 Estructura de costos

Dentro de los costos analizados con mayor detalle de importancia, los cuales son inherentes a este modelo de programa se consideran los siguientes:

- Costo de licencias o material de capacitación (no in-house)
- Desarrollo de material visual (Marca)
- Premios para los concursos por realizar. (Recursos Humanos)

5.15 Resumen del producto / servicio (derivado del resumen de la idea)

Las campañas en "*Seguridad de la Información*" consisten en general en actividades de sensibilización, sesiones educativas y diversos tipos de ataques dirigidas a públicos específicos. Estos últimos buscan medir la efectividad del programa de culturización. Las sesiones de sensibilización y educativas son buenas oportunidades para empezar a informar a los departamentos sobre cuál es su información y responsabilidades de seguridad. La función de recursos humanos en conjunto con el equipo de seguridad es la concienciación de los empleados, la formación debe incorporar material que demuestra la importancia de la seguridad de la empresa.

5.16 El propósito de la idea

Capacitar al personal en "*Seguridad de la Información*" para mejorar la seguridad general de la empresa, que los usuarios finales aprendan a identificar y responder a las amenazas de seguridad correctamente y conozcan el rol que ellos tienen en la "*Seguridad de la Información*" de la compañía.

5.17 Modo de ejecución

El programa de entrenamiento y concientización será realizado haciendo capacitaciones físicas y online y en distintas actividades que ayudarán a mejorar el nivel de conciencia en el personal sobre la "*Seguridad de la Información*".

Imagen #4 Cronograma de entrenamiento y sensibilización

6. CAPITULO VI CONCLUCIONES Y RECOMENDACIONES

6.1 Conclusiones

Cada día las empresas se enfrentan a nuevos retos en donde salvaguardar la privacidad, confidencialidad y disponibilidad de la información es más ardua, y donde la preparación ante la ocurrencia de eventos es cada vez más exigente. Es por ello que existe la necesidad de incorporar este programa para definir y dirigir las estrategias y métodos que garanticen una gestión segura de los procesos de negocio.

Según Objetivos

Objetivo 1- "Ilustrar una estrategia sobre cómo planificar, organizar y ejecutar una iniciativa de concienciación sobre la "*Seguridad de la Información*"."

- Con la investigación desarrollada se detalla la metodología a seguir para el diseño e implementación de una estrategia de "*Seguridad de la Información*", la cual está enfocada en los riesgos y a la vez está alineada con las necesidades del negocio, y permitió reforzar la integridad, confidencialidad y la disponibilidad de la información, considerada como crítica para TIGO.

Objetivo 2- "Establecer y definir las rutinas por seguir para realizar la capacitación y transferencia de conocimiento en "*Seguridad de la Información*".

- La definición de técnicas y/o métodos es fundamental para el mejoramiento continuo de cualquier proceso de gestión de seguridad, inclusive el de capacitación y sensibilización del recurso humano.

Objetivo 3 –"Diseñar un marco de trabajo y ejecución del programa de concientización en "*Seguridad de la Información*" para Tigo Costa Rica."

- Como resultado de esta propuesta el Departamento de Capital Humano apoya y se esfuerza y permitirá abarcar la totalidad del negocio y de esta manera llegar a los usuarios finales, quienes son clave para el desarrollo de un "*Programa de culturización en Seguridad de la Información*".

Objetivo 4 –"Contribuir al desarrollo de la "*Seguridad de la Información*" para alentar a los usuarios a actuar de forma responsable y, operar de forma más segura."

- Con la implementación de este programa de concientización en Seguridad, permitirá mantener un personal entrenado adecuadamente que puede responder más ágilmente ante los incidentes de seguridad. Puede ayudar a contener y evadir eventos negativos de una manera óptima y por consiguiente, ayuda a disminuir los riesgos.

Objetivo 5 –"Presentar plantillas y herramientas para ser utilizadas como puntos de partida por el equipo de sensibilización."

- Las herramientas y pruebas simples, así como los entrenamientos y charlas pueden ayudar a que las personas se acuerden de permanecer alerta.

Objetivo 6 –"Definir los lineamientos de introducción del personal a las tecnologías de la empresa."

- Con base al análisis realizado en este programa se plantea abarcar los temas que se consideran de mayor relevancia como base en brindar la sensibilización del recurso humano, con lo que permitirá modificar el comportamiento de las personas.

Objetivo 7 –"Crear una conciencia de seguridad aplicable a los activos de información."

- Con este trabajo permitió reforzar una cultura de seguridad, en todos aquellos colaboradores que sean parte del programa y deseen ponerlo en práctica.

Objetivo 8 –"Reducir el riesgo de robo, fraude y mal uso de los medios a través de información vigente, de conocimiento público y la conciencia de seguridad dentro de la empresa."

- Todas las compañías están expuestas a sufrir algún tipo de robo o fraude y es difícil detectarlo y frenarlo. A pesar de esto, se ha visto que este riesgo se mitiga sustancialmente cuando la empresa cuenta con un programa integral que permite combinar diferentes mecanismos de cambio cultural.

Objetivo 9 –"Accesar a la información a través de medidas de seguridad, por parte de los usuarios."

- Con base en los análisis realizados se determinan los temas claves que enruten el programa de sensibilización expuesto hacia el enfoque que permitió modificar el comportamiento de las personas, mientras tanto, el entrenamiento se basa en enseñar a realizar labores y acciones específicas.

Objetivo 10 –"Crear un ambiente de confianza y reglas claras dentro de la compañía, con respecto a la seguridad de información que manipulan los colaboradores en cada una de las áreas del negocio."

- Con respecto al presente "Programa de Culturización en Seguridad de la Información", TIGO Costa Rica buscó diseñar e implementar la formación de los colaboradores en materia de seguridad.

Objetivo 11 –"Mejorar la imagen de confiabilidad y seguridad de la empresa, como elemento diferenciador de la competencia."

- La imagen corporativa nos muestra lo que podemos esperar de una empresa o marca. Así, la imagen corporativa ayuda al cliente a elegir con la seguridad de que quedará satisfecho con el resultado que ofrece TIGO para gestionar y manipular la información brindada.

6.2 Recomendaciones

Al finalizar el presente proyecto de investigación y demostrando todo el análisis desarrollado, expongo una serie de recomendaciones que se deberían de tomar en cuenta para la implementación y operación continua de la culturización en "*Seguridad de la Información*" y que son de gran importancia como se detalla a continuación

Según Objetivos

Objetivo 1 "Ilustrar una estrategia sobre cómo planificar, organizar y ejecutar una iniciativa de concienciación sobre la "*Seguridad de la Información*". "

- Al implementar este "Programa de culturización en seguridad de la información", se desea con la sensibilización, lograr enfocarse en modificar el comportamiento de las personas, mientras tanto el entrenamiento se orienta en enseñar a realizar labores y acciones específicas.

Objetivo 2 - Establecer y definir las rutinas por seguir para realizar la capacitación y transferencia de conocimiento en "*Seguridad de la Información*".

- Debe de existir un compromiso por parte del negocio para dar el adecuado seguimiento y ejecución a los cronogramas y sesiones establecidas en este "***Programa de culturización en seguridad de la información***", esto con el fin de dar la continuidad a los procesos de aprendizaje y evaluación, ya que de no ser efectivos se puede no alcanzar los propósitos definidos.

Objetivo 3 - Diseñar un marco de trabajo y ejecución del programa de concientización en "*Seguridad de la Información*" para Tigo Costa Rica.

- Es importante plasmar y dar a conocer la importancia sobre crear cultura en "*Seguridad de la Información*" así como la implementación de un programa que apoye en la culturización de los colaboradores en "*Seguridad de la Información*", y de esta manera entender el por qué los empleados y la empresa requieren este programa.

Objetivo 4 - Contribuir al desarrollo de la "*Seguridad de la Información*" para alentar a los usuarios a actuar de forma responsable y, operar de forma más segura.

- Adoptar este tipo de programas y brindar la continuidad en el tiempo, otorga evidencia sobre las acciones realizadas por el negocio para la mejora continua en cuanto a lo que la "*Seguridad de la Información*" se refiere.

Objetivo 5 - Presentar plantillas y herramientas para ser utilizadas como puntos de partida por el equipo de sensibilización.

- Es fundamental ser conscientes en todas las aristas del negocio sobre la importancia de formar a los empleados en materia de "*Seguridad de la Información*" para los intereses como organización, así como también en materia de protección de datos personales. Tomando como punto de referencia, toda la información que trata la organización: datos de facturación, tarifas, márgenes, sistemas de producción, clientes, proveedores, acuerdos, etc.

Objetivo 6 - Definir los lineamientos de introducción del personal a las tecnologías de la empresa.

- Ante la vertiginosa evolución de las tecnologías es requerido que nuestros colaboradores deban estar en un continuo proceso de formación en "*Seguridad de la Información*". Sobre todo, si la organización tiene una alta dependencia de la tecnología. No sólo eso, sino que en muchos casos los colaboradores se convierten, en asesor de los clientes de la organización en el uso de la tecnología y sus necesidades de seguridad, incluyendo por ejemplo el uso de herramientas para gestionar información en la nube.

Objetivo 7 - Crear una conciencia de seguridad aplicable a los activos de información

- La adecuada definición de métricas es fundamental para el mejoramiento continuo de cualquier proceso de gestión de seguridad, incluye también el de capacitación y sensibilización.

Objetivo 8 - Reducir el riesgo de robo, fraude y mal uso de los medios a través de información vigente, de conocimiento público y la conciencia de seguridad dentro de la empresa.

- Existe personal específico, el cual es quien precisa más formación en materia de seguridad y con un mayor grado de especialización. Es de suma importancia identificarlo y poner a su disposición los recursos y mecanismos adecuados para formarse o autoformarse en aspectos relacionados con la seguridad ya que brindan soporte a los procesos de negocio de la organización.

Objetivo 9 - Accesar a la información a través de medidas de seguridad, por parte de los usuarios.

- Implementar y mantener un "Programa de culturización en seguridad de la información", otorga el beneficio de contar con un personal con un nivel de entrenamiento adecuado, lo cual es equivalente a personal que puede responder de forma más ágilmente ante los incidentes de seguridad que se presenten; puede ayudar a contener, disminuir y evadir eventos negativos de una manera óptima, por consiguiente, ayuda en la disminución de los riesgos.

Objetivo 10 - Crear un ambiente de confianza y reglas claras dentro de la compañía, con respecto a la seguridad de información que manipulan los colaboradores en cada una de las áreas del negocio.

- Los usuarios finales son clave para el desarrollo de un programa de gestión de la "*Seguridad de la Información*", capacitar y concientizar a nuestros colaboradores acerca de las amenazas y vulnerabilidades a los que están expuestos; disminuye la probabilidad que se produzcan incidentes de seguridad que puedan tener un mayor impacto para la organización.

Objetivo 11 - Mejorar la imagen de confiabilidad y seguridad de la empresa, como elemento diferenciador de la competencia.

- Obtener el apoyo y compromiso de la alta dirección es un factor clave para poder llevar a cabo un buen programa de capacitación, y deben formar parte de todo el proceso.

- Tradicionalmente la "*Seguridad de la Información*" en las organizaciones se ha entendido como un gasto que no aporta valor al negocio, pues es muy difícil ver el retorno de la inversión en medidas que no se perciben como productivas.

6.3 Bibliografía

- Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. PDF- (Luis Gomez Fernandez-ISBN: 978-84-8143-901-4)
- Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005 (Alberto G. Alexander)
- http://www.iso27000.es/download/doc_iso27000_all.pdf
- https://advisera.com/27001academy/es/knowledgebase/lista-de-apoyo-para-implementacion-de-iso-27001/
- ISO/IEC 27035, Information Technology. Security Techniques. Information Security Incident management.
- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.
- ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
- NIST (National Institute of Standard and Technology) Special Publication 800-50 Building an Information Technology Security Awareness and Training Program.
- www.isaca.org

6.4 Referencia

- Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. PDF- (Luis Gomez Fernandez-ISBN: 978-84-8143-901-4)
- Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005 (Alberto G. Alexander)
- http://www.iso27000.es/download/doc_iso27000_all.pdf
- https://advisera.com/27001academy/es/knowledgebase/lista-de-apoyo-para-implementacion-de-iso-27001/
- I. Brightman, J. Buith. "Treading Water. The 2007 Technology, Media & Telecommunications Security Survey", Deloitte, 2007.
- ISO/IEC 27035, Information Technology. Security Techniques. Information Security Incident management.
- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.
- ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
- IT Governance Institute. "Information Security Governance: Guidance for Boards of Directors and Executive Management", 2º Ed. EE. UU., 2006.
- J. Burgos. "Modelo para el Control de Riesgos de Seguridad de la Información en Áreas de Tecnologías de la Información y Comunicaciones (TIC)".
- M. Farias-Elinos, M. C, Mendoza-Diaz y L. Gómez-Velazco. "Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática". Techno-Legal aspects of Information Society and New Economy: an Overview. Information Society book series, 2003.
- NIST (National Institute of Standard and Technology) Special Publication 800-50 Building an Information Technology Security Awareness and Training Program.
- Peltier, T. R. "Information Security Risk Analysis", CRC Press, 2005.
- www.isaca.org

ANEXOS

Anexo 1- Test de Seguridad de la Información

Descripción

Prueba de inteligencia sobre temas alusivos de "*Seguridad de la Información*" (nivel básico), donde puedes averiguar el nivel de conocimiento como profesional.

El test consta de 15 preguntas, con la capacidad de responder y elegir de manera efectiva en relación con definiciones positivas sobre temas de seguridad, los que posiblemente se pueden presentar en su entorno personal y laboral.

2018

TEST DE SEGURIDAD DE LA INFORMACIÓN

CAPACITACIÓN: SEGURIDAD DE LA INFORMACIÓN

VERSIÓN: TIGO CR-2018

NOMBRE:

1. Las conexiones SSL permiten el establecimiento de comunicaciones seguras en internet, la navegación web, el correo electrónico, la mensajería instantánea y otros sistemas de transferencia de datos.

   ○ Verdadero ○ Falso ○ No sabe

2. El objetivo del malware es infiltrarse o dañar una computadora o sistema de información sin el consentimiento del usuario.

   ○ Verdadero ○ Falso ○ No sabe

3. La ingeniería social tiene como objetivo evitar el fraude, el espionaje industrial y el robo de identidad a un usuario.

   ○ Verdadero ○ Falso ○ No sabe

4. ¿El hackitivismo ayuda al fortalecimiento empresarial y gubernamental?

   ○ Verdadero ○ Falso ○ No sabe

5. En una empresa se comienza a planificar estrategias de acceso a las dependencias, políticas de respaldo, protección de los equipos ante el fuego, agua, etc. ¿La empresa implementa Seguridad Física?

   ⬭ Verdadero ⬭ Falso ⬭ No sabe

6. La certificación de la norma ISO/IEC 27001 es obligatoria para toda compañía.

   ⬭ Verdadero ⬭ Falso ⬭ No sabe

7. ¿Es correcto el significado de la sigla SGSI – Software de Gestión de Sociedades de la Información?

   ⬭ Verdadero ⬭ Falso ⬭ No sabe

8. ¿Cómo se puede clasificar la información en un análisis de riesgo? R/: En Alto riesgo, Medio riesgo y Bajo riesgo, también puede ser como confidencial, pública y privada)

   ⬭ Verdadero ⬭ Falso ⬭ No sabe

9. El objetivo de la protección de datos es garantizar la publicación, la integridad y la disponibilidad.

   ⬭ Verdadero ⬭ Falso ⬭ No sabe

10. ¿La palabra “cracker” significa compartir conocimientos y crear programas?

    ⬭ Verdadero ⬭ Falso ⬭ No sabe

11. El IPS es el dispositivo encargado de ejercer el control de acceso en una red informática, con el objetivo de proteger a los sistemas de ataques y abusos

    ⬭ Verdadero ⬭ Falso ⬭ No sabe

12. Un programa es una secuencia de instrucciones estructuradas y ordenadas las cuales un computador puede interpretar y ejecutar.

⬭ Verdadero ⬭ Falso ⬭ No sabe

13. La sigla TIC hace referencia a: Técnicas Informáticas de la Computación

⬭ Verdadero ⬭ Falso ⬭ No sabe

14. La "*Seguridad de la Información*" garantiza la privacidad de la información y la continuidad de los servicios de la empresa.

⬭ Verdadero ⬭ Falso ⬭ No sabe

Anexo 2- Cuestionario de concientización

Descripción

La conciencia empieza con un ejercicio que va a permitir evaluar el nivel de concienciación en seguridad de nuestros empleados, a la vez que despertar su interés por aprender más. Estos ejercicios toman la forma de ataques sorpresa.

Esta herramienta puede ser enviada al inicio del programa y a mediados de año, momento en el cual se espera haber creado algún conocimiento base en los colaboradores.

2018

CUESTIONARIO CONCIENTIZACIÓN

CAPACITACIÓN: SEGURIDAD DE LA INFORMACIÓN

VERSIÓN: TIGO CR-2018

NOMBRE:

Tigo está realizando un estudio para ayudar a determinar formas de educar sobre cuestiones de "*Seguridad de la Información*". Se le agradece si pudiera dedicar 10 minutos a responder unas breves preguntas sobre la "*Seguridad de la Información*".

1. ¿Cómo accede a internet?
    a. _____ Una conexión de acceso telefónico
    b. _____ Conexión ADSL (banda ancha)
    c. _____ Internet de la compañía

2. Dónde usa su computadora (marque todo lo que corresponda):
    a. _____Casa
    b. _____Oficina
    c. _____Ubicación de acceso público (centro de estudio, bibliotecas; centro comunitario)
    d. _____Internet café
    e. _____Internet centro telefónico
    f. _____Otro (Indicar dónde) _____

3. Muchas personas definen la seguridad como protección contra los efectos adversos. Con esto en mente, en una escala de uno a cinco. Con uno se valora muy preocupado y cinco menos preocupado. ¿Qué tan preocupado está usted por la seguridad de sus activos de tecnología de la información (computadora, periféricos, datos electrónicos, etc.)?

1	2	3	4	5
Muy		Algo		Menos

4. ¿Cuál de los siguientes cree que representa la mayor amenaza para las tecnologías de la información? Puede seleccionar cualquiera que aplica:

   a._____ Virus y gusanos

   b._____Correo no deseado y otro correo electrónico no solicitado

   c._____Hackers

   d._____Esquemas fraudulentos

   e._____Software malicioso (spyware)

   f. _____Hardware defectuoso

   g._____Otro_____

5. ¿Sabía que Tigo Costa Rica evaluará las amenazas potenciales para la tecnología de información del público y que ésta podría ayudarlo a diseñar un plan para protegerlo de amenazas potenciales?

   a. Sí, soy consciente de esto
   b. No, no estoy al tanto de esto

6. En una escala de uno a cinco, donde uno tiene mucho conocimiento y cinco es el que menos sabe, clasifique su conocimiento de los pasos que se pueden seguir para proteger sus activos de tecnología de la información:

1	2	3	4	5
Muy		Algo		Menos

7. ¿Tiene alguna de las siguientes opciones para proteger su computadora y sus datos electrónicos? Por favor indique todo lo que aplique.
    a. _____Un software de virus que se actualiza regularmente
    b. _____Firewall
    c. _____Filtro Antispam
    d. _____Prácticas de password seguro
    e. _____Proceso de respaldo regular de datos
    f. _____Cifrado de navegador de Internet actualizado
    g. _____Otro, por favor indique_____

8. ¿Cuál sería la mejor manera de proporcionarle información sobre cómo protegerse de posibles peligros? En otras palabras, ¿es más probable que recoja información de:
    a. _____Correo electrónico
    b. _____Anuncios de televisión
    c. _____Periódicos locales
    d. _____ Boletines informativos
    e. _____ Reuniones presenciales
    f. _____ Carteles
    g. _____ Otro (por favor describa) _____

Muchas gracias por participar en esta encuesta. Se planea usar sus respuestas para ayudar a desarrollar información con el fin de crear conciencia sobre la importancia de la "*Seguridad de la Información*".

Anexo 3-Encuesta Sensibilización

Descripción

Al igual que el cuestionario de sensibilización, con esta herramienta buscamos evaluar el nivel de concienciación y conocimientos en seguridad de los empleados, a la vez que despertar el interés por aprender más. Estos ejercicios se enviarán de forma programada a grupos definidos de forma previa con el fin de controlar y medir la funcionalidad de cada proceso de entrenamiento.

Esta herramienta puede ser enviada durante cualquier etapa del programa.

2018

ENCUESTA DE SENSIBILIZACIÓN

CAPACITACIÓN: SEGURIDAD DE LA INFORMACIÓN

VERSIÓN: TIGO-CR 2018

NOMBRE:

NOTA:

INSTRUCCIONES: Marque con una **"X"<u>todas las opciones</u>** que correspondan.

<u>SELECCIÓN MULTIPLE</u>

1. **¿Cuáles son los <u>pilares</u> de la "*Seguridad de la Información*"?**
    a. Seguridad
    b. Integridad
    c. Disponibilidad
    d. Confidencialidad

2. **¿Seleccione las mejores prácticas para el manejo de dispositivos móviles?**
    a. Mantener un formulario con el inventario de dispositivos
    b. Cifrar la información de los dispositivos
    c. Bloquear la instalación de aplicaciones maliciosas
    d. Resistente al agua

3. **¿Quién es el ingeniero social?**
    a. Mediante el engaño hurta información
    b. Hurta información mediante el uso de computación avanzada
    c. Ingeniero encargado de asegurar la seguridad
    d. Ninguna de las anteriores

4. **¿Cuáles características debe contar un log para ser útil?**
    a. ID
    b. Fecha y hora
    c. Identificación del usuario
    d. Ninguna de las anteriores

5. **¿Quién es el dueño de la información de TIGO?**
    a. Yo
    b. El Estado
    c. TIGO

6. **¿Cuáles son los niveles en los que se clasifica la información de nuestra empresa?**
    a. Pública
    b. Interna
    c. Segura
    d. Confidencial
    e. Clasificada

7. **Técnicas conocidas como "Espacio de trabajo seguro":**
    a. Bloquear la computadora cuando no la puedo custodiar.
    b. Guardar información pública bajo llave
    c. No olvidar información confidencial en las impresoras.
    d. No dejar información confidencial en los pasillos.

8. **¿Cuáles son los tipos de permiso más utilizados para la gestión de soporte remoto?**
    a. Permiso administrativo
    b. Permiso técnico
    c. Permiso presidencial

9. **¿Cuál es una función del comité de respaldos?**
    a. Analizar solicitudes de respaldo, priorizar y costear.
    b. Ejecutar los respaldos.
    c. Catalogar la información
    d. Definir qué información se respalda

10. **Mejores prácticas con respecto a la gestión de la infraestructura y sistemas de TIGO.**
    a) Validar la revisión o seguimiento de las bitácoras de las herramientas anti malware
    b) Revisión por parte de TI de la instalación de software no autorizado en la organización
    c) Implementar controles de borrado remoto para los dispositivos móviles
    d) Ninguna de las anteriores

11. **¿Por qué es importante la "*Seguridad de la Información*" en la empresa?**

Anexo 4-Campaña de fondos de pantalla

Descripción

La idea principal de esta campaña es utilizar imágenes y gráficos que contengan consejos y temas que refuercen los conceptos principales, según las normas y estándares en los que se enfoca el programa. De esta forma, se pretende concientizar a los colaboradores para que se consideren una parte activa de la seguridad de la empresa.

Dicho material se puede utilizar para ser configurado como fondos de pantalla, descansa pantallas al bloquearse los equipos, como pósteres impresos o bien, como trípticos que combinen gráficos y texto para apoyar en la transmisión de los aspectos importantes de seguridad que se desean.

2018

CAMPAÑA DE FONDOS DE PANTALLA

APLICADA A EQUIPOS DE USUARIO FINAL

VERSIÓN: FEB 2018

SEGURIDAD DE LA INFORMACIÓN

Imagen #5- Fondo de pantalla a TIGO lo protejo YO

Campaña de Escritorio limpio

Imagen # 6- Campaña escritorio limpio

Campaña de respaldo

Imagen # 7- Campaña de respaldos

Imagen # 8- Campaña de respaldos

Imagen # 9- Campaña de respaldos

Campaña password

Imagen # 10- Campaña de password seguro

Imagen # 11- Campaña de password seguro

Campaña confidencialidad

Imagen # 12- Campaña de confidencialidad

Imagen # 13- Campaña de confidencialidad

Imagen # 14- Campaña de confidencialidad

Campaña uso de equipos

Imagen # 15- Campaña uso de equipos

Imagen # 16- Campaña Uso de equipos

Campaña Manejo información física

Imagen # 17- Campaña manejo información física

Campaña consejos del mes

Imagen # 18-Campaña consejos del mes

Imagen # 19-Campaña consejos delmes

Imagen # 20-Campaña consejos del mes

Anexo 5-Charlas Presenciales

Descripción:

El programa de concientización inicia con una serie de charlas con las cuales se busca asegurar que la *"Seguridad de la Información"*, así como sus políticas, procesos y procedimientos, "permean" en el personal de todos los niveles de la organización.

2018

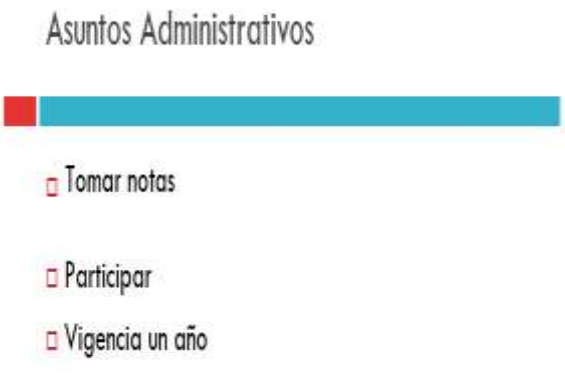
CHARLAS PRESENCILES

APLICADA DE FORMA Y PRESENCIAL

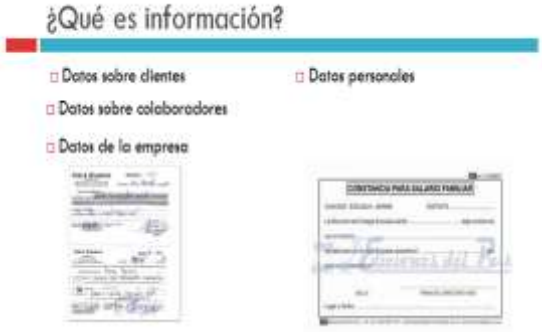
VERSIÓN: 2018-2019

SEGURIDAD DE LA INFORMACIÓN

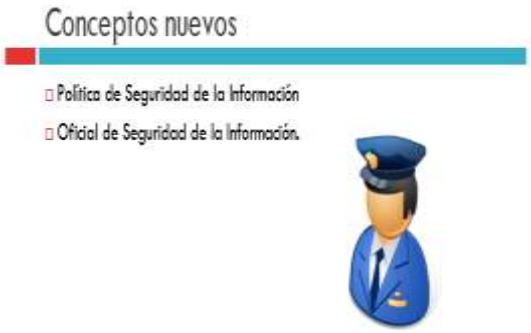
Imagen#21-Charla presencial-Diapositiva-1



Imagen#22-Charla presencial-Diapositiva-2

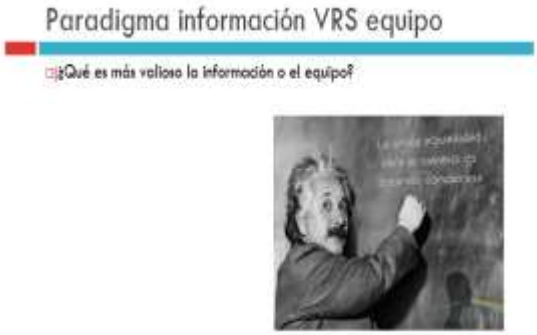


Imagen#23-Charla presencial-Diapositiva-3



Imagen#24-Charla presencial-Diapositiva-4

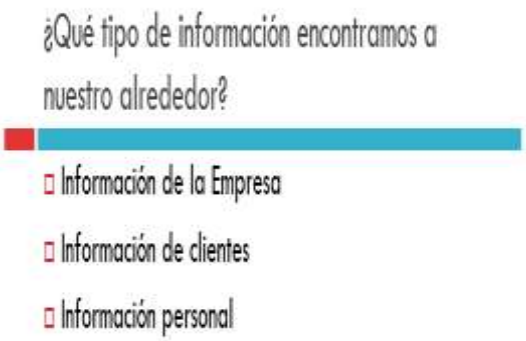
Imagen#25-Charla presencial-Diapositiva-5



Imagen#26-Charla presencial-Diapositiva-6

Imagen#27-Charla presencial-Diapositiva-7

Imagen#28-Charla presencial-Diapositiva-8



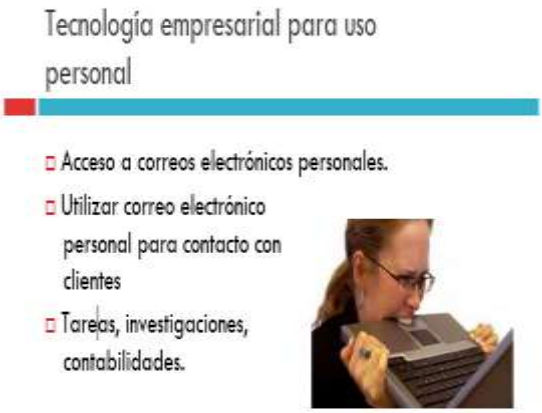
Imagen#29-Charla presencial-Diapositiva-9

Imagen#30-Charla presencial-Diapositiva-10

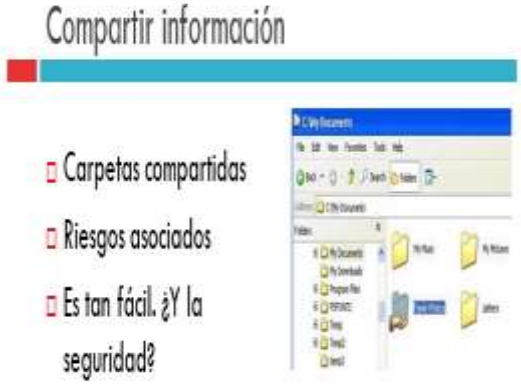
Imagen#31-Charla presencial-Diapositiva-11

Imagen#32-Charla presencial-Diapositiva-12

Imagen#33-Charla presencial-Diapositiva-13



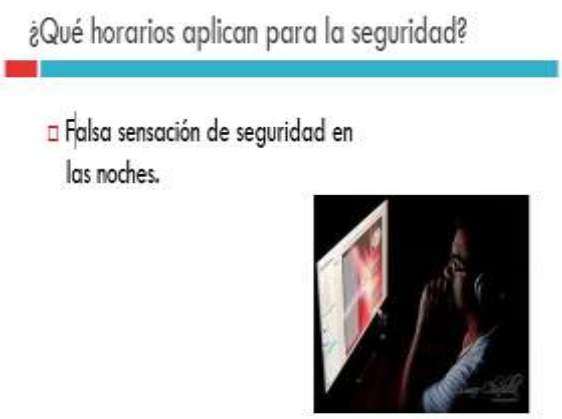
Imagen#34-Charla presencial-Diapositiva-14



Imagen#35-Charla presencial-Diapositiva-15

Imagen#36-Charla presencial-Diapositiva-16

Imagen#37-Charla presencial-Diapositiva-17



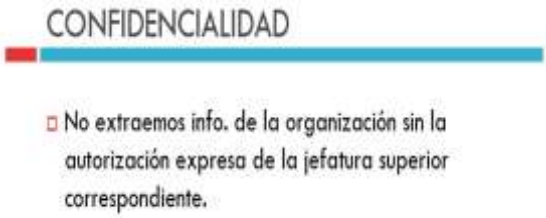
Imagen#38-Charla presencial-Diapositiva-18

Imagen#39-Charla presencial-Diapositiva-19

Imagen#40-Charla presencial-Diapositiva-20

Imagen#41-Charla presencial-Diapositiva-21

Imagen#42-Charla presencial-Diapositiva-22



Imagen#43-Diapositiva-23

Imagen#44-Diapositiva-24

Imagen#45-Charla presencial-Diapositiva-25

Imagen#46-Charla presencial-Diapositiva-26

Imagen#47-Charla presencial-Diapositiva-27

Imagen#48-Charla presencial-Diapositiva-28

Hackers

- Tipos de hackers
- Sociedades hackers

Imagen#49-Charla presencial-Diapositiva-29

Hackers

- Ataques, breve descripción
- Correo
- Celulares
- Internet
- Toda la tecnologia.

Imagen#50-Charla presencial-Diapositiva-30

Hackers

- ¡Método de ataque!
- De lo más fácil a lo más complicado.

Imagen#51-Charla presencial-Diapositiva-31

Ingeniero social

- Es el arte del engaño
- Se basa en 4 principios: *Kevin Mitnick
  - Todos queremos ayudar
  - Inicialmente existe confianza en las personas
  - No nos gusta decir que no
  - A todos nos gusta que nos alaben

Imagen#52-Charla presencial-Diapositiva-32

Ingeniero social

- Enmascaramiento
  - Teléfono
  - Presencial
  - Utilizando medios electrónicos

Imagen#53-Charla presencial-Diapositiva-33

Ingeniero social

- Tail-gating
- Piggy-backing
- Permiso con o sin consentimiento de ingreso

Imagen#54-Charla presencial-Diapositiva-34

Ingeniero social

- Búsqueda de información en la basura

Imagen#55-Charla presencial-Diapositiva-35

Ingeniero social

- Espiar por encima del hombro

Imagen#56-Charla presencial-Diapositiva-36

Ingeniero social

- Seguimiento de cerca

Imagen#57-Charla presencial-Diapositiva-37

Ingeniero social

- Búsqueda de información en la web y redes sociales

Imagen#58-Charla presencial-Diapositiva-38

Ingeniero social

- Cadenas de correos
- Spam
- Scam
- SMS

Imagen#59-Charla presencial-Diapositiva-39

Adquirir tecnología, ¿Moda?

- Investigar previo a adquirir tecnología, a nivel personal e institucional.

Imagen#60-Charla presencial-Diapositiva-40

Espacio de trabajo seguro

- Bloqueo computador
- Escritorio limpio
- Papel tapiz limpio
- Información en las impresoras
- Resguardo información confidencial

Imagen#61-Charla presencial-Diapositiva-41

Espacio de trabajo seguro

- Información en pizarras.
- Gavetas con seguro.
- Información abandonada.
- Portátil con candado.
- Celular resguardado.
- Oficinas personales se resguardan como si no existiera la puerta.

Imagen#62-Charla presencial-Diapositiva-42

Seguridad física

- Respetamos la demarcación
- Acompañamos a visitantes en todo momento.
  - Restringida
  - Interna
  - Pública

Imagen#63-Charla presencial-Diapositiva-43

Controles de acceso físico

- Servicios Administrativos debe implementar controles de acceso físico, según el inventario de áreas enviado por las jefaturas.
- Las jefaturas enviarán mensualmente un reporte a la Gerencia sobre incumplimientos y desviaciones encontradas en el control de acceso físico.

Imagen#64-Charla presencial-Diapositiva-44

Destrucción segura de la Información

- Papelería
- CD/DVD
- Llaves maya
- Discos duros

Imagen#65-Charla presencial-Diapositiva-45

Credo de las contraseñas

- No escribirás tu contraseña
- No compartirás tu contraseña
- Crearas contraseñas complejas.
- Serás responsable por el uso de tu contraseña.

Imagen#66-Charla presencial-Diapositiva-46

Imagen#67-Charla presencial-Diapositiva-47

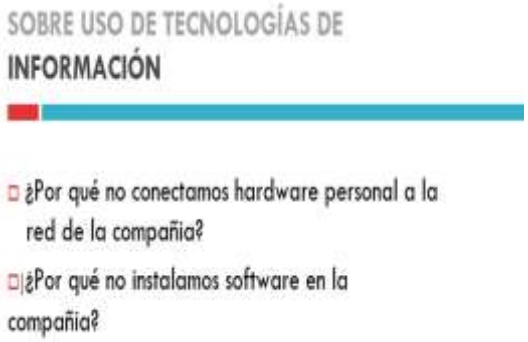
Imagen#68-Charla presencial-Diapositiva-48

Imagen#69-Charla presencial-Diapositiva-49

Imagen#70-Charla presencial-Diapositiva-50

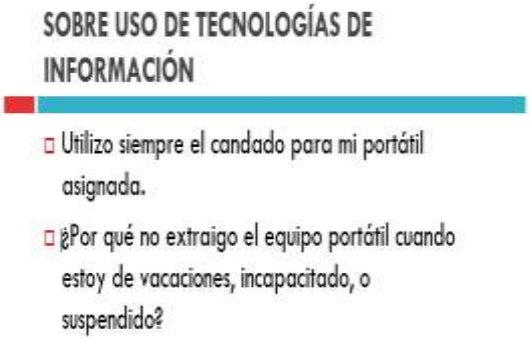
Imagen#71-Charla presencial-Diapositiva-51

Imagen#72-Charla presencial-Diapositiva-52



Imagen#73-Charla presencial-Diapositiva-53

Imagen#74-Charla presencial-Diapositiva-54



Imagen#75-Charla presencial-Diapositiva-55

Imagen#76-Charla presencial-Diapositiva-56

Imagen#77-Charla presencial-Diapositiva-57

Imagen#78-Charla presencial-Diapositiva-58

Imagen#79-Charla presencial-Diapositiva-59

Imagen#80-Charla presencial-Diapositiva-60

Anexo 6-Campaña Phishing

Descripción

La campaña de Phishing inicia con una serie de ejercicios que buscan evaluar el nivel de conciencia y conocimiento sobre el tipo de ataque mencionado. Se enfoca en elaborar un laboratorio en el que se utilizan herramientas que permiten lanzar un ataque dirigido a usuarios seleccionados del negocio. Se usa la suplantación de identidad de una cuenta de correo, válida para lo interno del negocio y con el propósito de capturar información de autenticación de los usuarios que serán parte del laboratorio.

Este proceso estará acompañado de un proceso de charlas presenciales y virtuales que será impartida por el personal del área de Seguridad lógica. Simultáneamente se subirá a la plataforma de entrenamiento interno.

2018

CHARLA PRESENCIAL CAMPAÑA DE PHISHING

APLICADA DE FORMA WEB Y PRESENCIAL

VERSIÓN: AGO 2018

SEGURIDAD DE LA INFORMACIÓN

Calendario

Calendario de pruebas de phishing		
Tareas		
Desarrollo de KIT de capacitación	07-feb	17-ago
Instalación configuración gophish	07- feb	11- feb
Configuración de campaña 1	14- feb	18- feb
Configuración de campaña 2	14- feb	18- feb
Configuración de campaña 3	14- feb	18- feb
Pruebas de campaña	21- feb	25- feb
Implementación de campaña1	28- feb	01-mar

Revisión de resultados	02-abr	06- abr
Aplicación de KIT de capacitación	09- abr	27- abr
Implementación de campaña2	30- abr	03-may
Revisión de resultados	13- may	17- may
Aplicación de KIT de capacitación	20- may	30- may
Implementación de campaña3	04-jun	22-jun
Revisión de resultados	25- jun	04-ago
Aplicación de KIT de capacitación	06-ago	17-ago

Herramientas:

Gophish .3.

Kit de capacitación

Temario:

1. Defunción del phishing.
2. ¿Qué tipo de información roba? Y métodos de propagación.
3. Ejemplos de correos maliciosos.
4. Evaluación de consecuencias del phishing.
5. Técnicas para evitar ser víctimas del phishing.

Imagen#81-Diapositiva-1-Capacitación Phishing

Imagen#82-Diapositiva-2-Capacitación Phishing

Imagen#83-Diapositiva-3-Capacitación Phishing

Imagen#84-Diapositiva-4-Capacitación Phishing

Imagen#85-Diapositiva-5-Capacitación Phishing

Imagen#86-Diapositiva-6-Capacitación Phishing

Imagen#87-Diapositiva-7-Capacitación Phishing

Imagen#88-Diapositiva-8-Capacitación Phishing

Imagen#89-Diapositiva-9-Capacitación Phishing

Imagen#90-Diapositiva-10-Capacitación Phishing

Anexo 7 Carta de Aplicabilidad