UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

"SEGURIDAD PARA LA PREVENCIÓN DE DELITOS, CULTURA INFORMÁTICA Y PRIVACIDAD DE LOS DATOS PERSONALES."

TESIS
PARA OBTENER EL GRADO DE
INGENIERO EN REDES

PRESENTA
EDMUNDO LÓPEZ MATOS

DIRECTOR DE TESIS
MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORES
MSI. LAURA YÉSICA DÁVALOS CASTILLA
MTI. MELISSA BLANQUETO ESTRADA
MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
DR. JAIME SILVERIO ORTEGÓN AGUILAR

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2014

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO DE TESIS ELABORADO BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

UNIVERSIDAD DE QUINTANA ROO
DCI DIVISIÓN DE CIENCIAS E INGENIERÍA

COMITÉ DE TRABAJO DE TESIS

DIRECTOR:

MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORA:

MSI. LAURA YÉSICA DÁVALOS CASTILLA

ASESORA:

MTI. MELISSA BLANQUETO ESTRADA

UNIVERSIDAD DE QUINTANA ROO
SERVICIOS ESCOLARES
TITULACIONES

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2014

AGRADECIMIENTOS

Ante cualquier cosa agradezco la ayuda de Nuestro Padre Celestial que me ha concedido la oportunidad y la capacidad para poder alcanzar esta meta en mi vida, por la guía e inspiración que me brindó para poder desarrollar este trabajo, y poder utilizar el conocimiento y las habilidades que he desarrollado al servicio de muchas otras personas.

A mis padres, quienes han sido mis mejores maestros en la vida, y representan para mí un gran ejemplo de trabajo arduo, rectitud y dedicación. Por su constante consejo y preocupación para que alcanzara una formación tanto académica como personal, brindando conocimiento e inculcando hábitos y valores que me han permitido llegar a ser la persona que soy hoy en día. Por el apoyo y sustento que me brindaron para lograr alcanzar esta meta en mi vida, y por todo su amor incondicional.

A mis hermanos, y a toda mi familia y amigos, que han estado presentes a lo largo del desarrollo de este trabajo y que han influenciado mi vida con su ejemplo y sus consejos. Por aquellos que siempre estuvieron ahí para animarme a fin de cerrar este ciclo de mi vida y de mi formación.

A mis maestros, que han sido una fuente inagotable de guía e instrucción en estos años durante mi estadía en la universidad. Por sus consejos, ánimo y apoyo en cada una de las actividades que he realizado en esta casa de estudios.

DEDICATORIA

El presente trabajo está dedicado e inspirado en la seguridad y tranquilidad de todas las personas que son importantes para mí, esperando poder establecer el inicio de una nueva conciencia y servir como un precursor para las nuevas generaciones que vienen y que retomen estas ideas con el fin de beneficiar a la mayor cantidad de personas posible.

A mi familia, por todo lo que han hecho por mí para hacer esto posible.

RESUMEN

La tecnología cambia constantemente brindándonos mayores comodidades y capacidades para llevar a cabo las tareas diarias, pero junto con ella los peligros y amenazas que existen con su interacción aumentan y se vuelven más complejos. En estos días, la información personal almacenada en nuestros dispositivos electrónicos o en nuestros perfiles en la red empieza a tener mayor valor e interés para los atacantes, lo que lleva a tener implicaciones cada vez más reales, pues han pasado de afectar equipos y archivos, a causar pérdidas monetarias, presión social o psicológica, e incluso el poner en riesgo la vida e integridad de las personas.

Este documento resalta la importancia de mejorar la seguridad de los usuarios en la red y de crear una buena cultura informática a través de campañas de concientización como parte de un programa de seguridad mayor a implementarse en la Universidad de Quintana Roo, según se encuentra en el documento "*Manual de Seguridad para Instituciones de Educación Superior: estrategias para la prevención y atención (2011)*" de la Asociación Nacional de Universidades e Instituciones de Educación Superior, tomando en cuenta algunas pautas y consejos de la *National Institute of Standards and Technology*.

Se definieron algunas de las amenazas y riesgos más comunes que existen en la red así como el impacto que pueden tener en los usuarios, cito parte de la legislación actual existente en los medios correspondientes, con el fin de evitar la comisión de algún delito y aplicar las penas adecuadas a los infractores.

Explico la manera de crear el programa para una campaña de concientización efectiva, y analizo diversos factores, recursos y directrices para llevar esta campaña a la práctica con el fin de impulsar una cultura informática y concientizar a los usuarios sobre los riesgos a lo que pueden verse expuestos al hacer un mal uso de los medios y tecnologías de información actuales.

Al final del documento pongo a disposición un ejemplo de sesión de las campañas de concientización que se realizó tomando en cuenta las estructuras citadas en el trabajo, así como las herramientas utilizadas para llevarlas a cabo y los resultados obtenidos después de las sesiones.

CONTENIDOS

CAPÍTULO 1 **6**

1.1 Introducción 6
1.2 Planteamiento del problema 7
1.3 Justificación 8
1.4 Objetivos 10
OBJETIVO GENERAL 10
OBJETIVOS PARTICULARES 10
1.5 Alcance 10

Capítulo 2 **11**

2.1 ANUIES: Estrategias para la prevención y atención de delitos 11
2.2 El valor de los datos: Riesgos y amenazas. 12
AMENAZAS GENERADAS POR CÓDIGO MALICIOSO 13
AMENAZAS GENERADAS POR PROBLEMAS CON LA PRIVACIDAD 14
2.3 Marco legal en México 18
CÓDIGO PENAL FEDERAL 19
CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE QUINTANA ROO 22
LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES 25

CAPÍTULO 3 **26**

3.1 Culturizar para la prevención de delitos 26
3.2 Estructura de una Campaña de Concientización 27
3.3 Ejemplo de una sesión de la campaña de concientización y cultura informática para la Universidad de Quintana Roo 33
PELIGROS Y AMENAZAS EN REDES SOCIALES: FACEBOOK 35
MEDIOS IMPRESOS 36
RESULTADOS DE LA CAMPAÑA DE CONCIENTIZACIÓN 40

Capítulo 4 42

Conclusiones y trabajo futuro 42

Bibliografía 44

SEGURIDAD PARA LA PREVENCIÓN DE DELITOS, CULTURA INFORMÁTICA Y PRIVACIDAD DE LOS DATOS PERSONALES

Capítulo 1

1.1 Introducción

Los sitios de redes sociales, están conformados por grupos de personas con intereses en común y que comparten información en Internet a través de un *software* que permite establecer relaciones de confianza entre los participantes, es decir, gracias a estos programas podemos compartir diferentes archivos e información con las personas que se encuentren dentro de nuestra red.

En los últimos años hemos podido observar un incremento considerable en el número de usuarios de éste tipo de servicios, los cuales permiten que las personas encuentren una nueva manera de conocerse entre sí logrando finalmente una amistad, lo que combinado con ciertas funcionalidades, como el hecho de compartir archivos, imágenes y/o videos, generan una sensación de cercanía entre los integrantes de las redes sociales. Sin embargo esta tecnología ha sido víctima de usuarios malintencionados que buscan obtener algún beneficio personal de dichos servicios (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2009)

El riesgo tecnológico se ha venido desarrollando de manera creciente en los últimos años debido al continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad, en conjunto con la falta de una cultura informática adecuada para el uso de estas nuevas herramientas. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2012)

Los delincuentes han aprovechado el avance de las tecnologías de la información como un medio para llegar a sus víctimas y obtener lo que necesitan de una manera más fácil o a mayor escala. Adicional a los ataques intencionados, se encuentra el uso incorrecto de la tecnología, que en muchas ocasiones es la mayor causa de las vulnerabilidades y los riesgos a los que se exponen los usuarios habituales de estos servicios así como las organizaciones en donde estos desempeñan sus actividades.

El riesgo tecnológico puede verse desde tres aspectos, primero a nivel de la infraestructura tecnológica (hardware o nivel físico), en segundo lugar a nivel lógico (riesgos asociados a software, sistemas de información e información) y por último los riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel.

El riesgo tecnológico puede ser causa y consecuencia de otro tipo de riesgos, una falla sobre la infraestructura puede implicar riesgos en otros ámbitos, como pérdidas financieras, multas, acciones legales, afectación sobre la imagen de la organización, causar problemas operativos o afectar las estrategias de la organización; así como también puede afectar en la seguridad, integridad y privacidad de los usuarios, viéndose involucrados en actos de extorsión, hostigamiento y fraude, entre otros. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2012)

1.2 Planteamiento del problema

El uso de los medios informáticos trae consigo ciertos riesgos que de no ser tratados de la manera correcta pueden poner en peligro la seguridad de la información y de las personas que la comparten. Tomando en cuenta el aumento en la cantidad de usuarios, y la solicitud constante de ayuda de su parte al departamento de cómputo de la universidad, se puede considerar que se requiere una mayor concientización hacia los usuarios sobre qué hacer para prevenir situaciones de riesgo informático.

En respuesta a los esfuerzos y a la necesidad de la Universidad de Quintana Roo de crear un programa de seguridad, será necesario definir la clase de riesgo informático al que se ven expuestos los usuarios de la Red Informática Universitaria (RIU) de la Universidad de Quintana Roo, campus Chetumal, y fomentar en ellos una cultura informática que permita reducir la incidencia en esos riesgos a través de campañas de concientización abordando las diferentes problemáticas que existan.

Se plantean las siguientes interrogantes: ¿Cuáles son los principales riesgos a los que se ven expuestos los usuarios al utilizar los servicios de Internet dentro de la Universidad? ¿Qué tipo de información comparten en esos medios? ¿Qué conocimiento se tiene en cuanto a los riesgos informáticos? ¿Qué medidas de prevención están implementando?

Con ayuda de los departamentos responsables de la red informática, se pretende realizar un análisis que nos permita identificar el uso de la red, así como el conocimiento de los usuarios en cuanto a las medidas de seguridad que deben tomar al hacer uso de los principales recursos informáticos con los que trabajan en la red. Para esto se contará con información provista por el departamento de cómputo de la universidad con respecto a los incidentes más comunes y el tipo de tráfico existente en la red, así como a las medidas preventivas que se han implementado en la universidad. También se realizarán encuestas a los usuarios finales para determinar la concientización que tiene en cuanto al uso de los medios informáticos y la seguridad de su información. El análisis de la red y la aplicación de las medidas preventivas necesarias se realizarán tomando en cuenta los cambios en la infraestructura tecnológica que ha implementado la universidad durante el año en curso.

1.3 Justificación

La universalización de las tecnologías de la información, ha traído la aparición de multitud de entornos en los que se manejan y almacenan nuestros datos personales. Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado, es necesario concienciar a los usuarios de las TIC de la importancia de la privacidad.

En México, a finales del año pasado, había un total de 51.2 millones de usuarios de internet, con las nuevas tecnologías móviles, estos números se han incrementado rápidamente, ya que 5 de cada 10 usuarios mexicanos se conectan a través de un *Smartphone*. El uso de las redes sociales en México sigue incrementando, ya que 9 de cada 10 usuarios hacen uso de por lo menos una de las redes más populares en el país. (Asociación Mexicana de Internet AC, 2014)

Los casos de robo de identidad en México y a nivel internacional van en aumento, esto como consecuencia de factores como el uso de nuevas tecnologías, el incremento en la demanda de compras por Internet y el uso de banca en línea, la falta de conciencia o tiempo destinado por los usuarios para la protección de sus datos personales o financieros y el desarrollo de técnicas más sofisticadas por los atacantes para la obtención ilícita de este tipo de información, quienes se aprovechan de Internet, de diversos medios digitales y sobre todo, de la falta de precaución del usuario para lograr sus objetivos.

Se estima que en México las pérdidas anuales por este delito están alrededor de los 9 millones de pesos, según estudios del IPN, lo que hace que el país se ubique entre los 10 primeros lugares en robo de identidad y los daños ligados a fraudes por suplantación de identidad, sin embargo, al no ser un delito tipificado no se tienen estadísticas confiables sobre su incidencia. (El Economista, 2014) La falta de denuncias de las víctimas impide establecer estadísticas, alertó el vocero nacional del Buró de Crédito, Wolfgang Erhardt. “¿Cuántos son? ¿Cuántas víctimas de robo de identidad hay? Nadie sabe porque es un fenómeno mundial que la gente no denuncia”, dijo. (Milenio, 2013)

Según los datos que mantiene la División Científica de la Policía Federal, hubo un aumento del 113% en incidentes de seguridad cibernética en 2013 comparado con el año anterior. Además, los datos preliminares sobre 2014 hasta ahora sugieren un aumento incluso más pronunciado en incidentes detectados: nada menos que un 300% más que en 2013. Cabe destacar que el marcado aumento en el corriente año se atribuye principalmente a las mejoras de los procesos de identificación de incidentes a nivel nacional y en la generación de nuevos vectores de ataque.

De los incidentes denunciados ante la Policía Federal Mexicana, y sin incluir incidentes que involucraron a ciudadanos particulares, aproximadamente el 31% fueron contra instituciones gubernamentales, el 26% contra entidades del sector privado, el 39% contra organizaciones académicas y el 4% contra otras entidades. (Organizacion de los Estados Americanos, 2014)

Debido a la diversa cantidad de usuarios y de acciones que se desarrollan en la red universitaria, la difusión de estos problemas y la creación de una cultura informática mediante la aplicación de campañas de concientización, debe ser una actividad constante para la formación de profesionistas capacitados para el uso de las tecnologías de la información en cualquier ámbito, así como para la reducción de esta clase de amenazas en nuestra casa de estudio.

De acuerdo con las sugerencias brindadas por la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) en su documento "*Manual de Seguridad para Instituciones de Educación Superior: estrategias para la prevención y atención (2011)*", es necesario el desarrollo y aplicación de programas para la prevención y el manejo de situaciones de seguridad por parte del comité designado para ello en la Universidad de Quintana Roo. De acuerdo con las especificaciones dadas por este documento, algunos de los puntos que este programa puede contemplar son:

- Seguridad en instalaciones.
- Seguridad en las comunicaciones
- Procesos ante actos delictivos
- Informe de incidentes
- Directorio de emergencia

Como parte de este programa de concientización se pretende cubrir el aspecto relacionado con la Seguridad en las Comunicaciones, más específicamente se pretende desarrollar una mejor cultura en cuanto a la privacidad y seguridad de los datos de los usuarios en la RIU a través de campañas de concientización, junto con lo cual se espera ayudar con el cumplimiento de los siguientes puntos incluidos en los "Temas estratégicos de atención en el Consejo o Comité de Seguridad":

- Análisis, discusión y evaluación de los problemas relacionados con la inseguridad al interior del recinto de la institución.
- Desarrollo de programas de cultura de la prevención de la violencia, la drogadicción, la extorsión, entre otros.
- Análisis y desarrollo de estrategias en torno a:
    - Políticas, protocolos o manuales de atención específicos o campañas de difusión.
- Desarrollo de estudios para crear una cultura de la prevención.
- Realización de recomendaciones para mejorar la seguridad en la IES.

Se pretende integrar algunos puntos de la "Agenda de trabajo del Consejo o Comité de Seguridad":

- Programa de capacitación del personal de seguridad para enfrentar las nuevas situaciones de violencia.
- Difusión de medidas de prevención.
- Informes estadísticos de incidentes.
- Difusión de los delitos, para que la comunidad esté al tanto de las situaciones de violencia a las que está expuesta y participe en campañas de prevención.

Uno de los casos de éxito al aplicar este tipo de medidas ha sido la Universidad de Guadalajara:

“La región Centro occidente de la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) otorgó aproximadamente 110 mil pesos al programa “Universidad Segura” de la Universidad de Guadalajara, con el fin de fortalecer los talleres preventivos en las aulas universitarias; así lo informó Montalberti Serrano Cervantes, coordinador de Seguridad de la UdeG. El proyecto consiste en fortalecer una cultura de autoprotección, prevención y sensibilización en torno a la inseguridad pública. Incluye quince talleres preventivos, que se imparten en los salones de clases a los jóvenes, sobre todo a los de primer ingreso, que versan sobre medidas de prevención urbana, cuyo fin es enseñar a los muchachos a protegerse y a caminar por las calles de manera más segura, además de saberse proteger en Internet, para navegar en la Web con prudencia, previniendo peligros. [...] Por último, anunció que la Coordinación de Seguridad Universitaria fue invitada para impartir estos talleres en la Universidad de Guanajuato. 'Si funciona en ese estado, podría replicarse en otros', dijo.” (Asociación Nacional de Universidades e Instituciones de Educación Superior, 2014)

1.4 Objetivos

Objetivo General

Definir los posibles riesgos informáticos a los cuales se enfrentan los usuarios y proponer acciones preventivas que puedan aplicarse mediante campañas de concientización y que propicien una cultura correcta del uso de los recursos informáticos en la comunidad universitaria, con el fin de establecer las bases para la implementación de un programa de seguridad informática en el futuro.

Objetivos Particulares

- Analizar la estructura de seguridad con la que cuenta la red informática universitaria.
- Definir los riesgos informáticos que afectan la privacidad de nuestros datos en Internet.
- Analizar la legislación disponible con relación a los riesgos y delitos informáticos en el estado.
- Proponer estrategias de seguridad aplicables a la comunidad universitaria para mejorar la privacidad y la seguridad de las comunicaciones en la red.
- Establecer una estructura base que sirva para la implementación de campañas de concientización sobre los riesgos informáticos y la manera de prevenirlos.

1.5 Alcance

El proyecto se ha diseñado para establecer medios de difusión y campañas con recomendaciones que permitan mejorar la seguridad y la privacidad en el uso de los recursos informáticos. A través de estas acciones se espera ayudar en la implementación de un programa de seguridad para la universidad así como el propiciar una cultura informática que permita a los usuarios usar de manera eficiente y segura los recursos que tiene a su disposición en la red, no se pretende con esto dar fin a los problemas de seguridad y de rendimiento de la red, sino más bien concientizar a los usuarios sobre los riesgos a los que se ven expuestos y las acciones a realizar para evitarlos y así crear un ambiente más seguro en la interacción diaria en la red.

Capítulo 2

2.1 ANUIES: Estrategias para la prevención y atención de delitos

La Asociación Nacional de Universidades e Instituciones de Educación Superior de la República Mexicana A.C. (ANUIES) es una asociación no gubernamental, de carácter plural, que congrega a las principales instituciones de educación superior del país, tanto públicas como particulares, cuyo común denominador es su voluntad para promover el mejoramiento integral en los campos de la docencia, la investigación y la extensión de la cultura y los servicios.

La ANUIES coordina de manera propositiva y participativa, con respeto a la autonomía y pluralidad de las instituciones asociadas, el desarrollo de la educación superior; contribuye a su fortalecimiento con declaraciones, aportaciones y directrices; participa con las autoridades educativas en la formulación de planes y programas nacionales de educación superior, e impulsa la creación de organismos especializados para el mejoramiento de la calidad educativa.

La agenda de trabajo de la ANUIES se empalma con la agenda del país en áreas como la ampliación de la cobertura, la innovación y la calidad educativas, el desarrollo integral de los estudiantes, la vinculación de la educación superior con los sectores social y productivo, la búsqueda de mejores esquemas de financiamiento y la rendición de cuentas, y más recientemente, sobresale la preocupación por la seguridad de los integrantes de las comunidades educativas en los campus universitarios. (ANUIES, 2013)

ANUIES ha integrado el *Manual de Seguridad para Instituciones de Educación Superior*, que incorpora la revisión y comentarios de las secretarías federales de Seguridad Pública y de Gobernación, así como aportaciones de las Instituciones de Educación Superior (IES) asociadas a la ANUIES. Este manual proporcionará instrumentos de apoyo en materia de seguridad con el propósito de contar con datos de las características y magnitud de la inseguridad de las IES, sobre todo porque esa información contribuirá a la definición de protocolos específicos de prevención y atención por tipo de incidente, pero principalmente porque permitirá que la comunidad conozca y participe en su atención y prevención de manera corresponsable.

Uno de los principales retos de las instituciones de educación superior, junto con la formación académica, es el de trascender en la sociedad. La educación superior no se circunscribe a las aulas; por considerarse un bien público, sus resultados inciden en diversos ámbitos ligados al desarrollo de la sociedad y por supuesto a su bienestar. Debido a la constante integración de los medios electrónicos, en especial de las redes sociales, como una herramienta de interacción con un número cada vez mayor de usuarios, uno de los hitos de las instituciones de educación superior debe ser el de fomentar en la comunidad universitaria el uso, de manera consciente, segura y con un impacto positivo, de los diversos medios de comunicación en la red a los que tenemos acceso hoy en día.

Tomando en cuenta esto, y en vista de los diferentes desafíos en cuanto a la seguridad en Internet, el presente trabajo propone incluir dentro de las prácticas de seguridad de la Universidad de Quintana Roo

los protocolos relacionados con una mejor cultura informática y la privacidad de los datos personales, para la prevención de delitos informáticos.

Es prudente, por lo tanto, analizar a lo que nos referimos con “prevención de delito”. La Dirección General de Prevención del Delito de la Procuraduría General de Justicia del Estado de Quintana Roo (PGJE, 2014) lo define de la siguiente manera:

“*Prevención es la acción y efecto de prevenir, por lo tanto, es la disposición que se hace de forma anticipada para minimizar un riesgo. El objetivo de prevenir es lograr que un perjuicio eventual no se concrete.*

Un delito es una acción u omisión voluntaria o imprudente que se encuentra penada por la ley. Por lo tanto, el delito supone un quebrantamiento de las normas y acarrea un castigo para el responsable.

Por consiguiente, ‘Prevención del delito’ no es más que tomar medidas y realizar acciones para evitar una conducta o un comportamiento que puedan dañar o convertir a la población en sujetos o víctimas de un ilícito”

2.2 El valor de los datos: Riesgos y amenazas.

Piense por un momento: ¿Qué pasaría si se extraviara o alguien robara su equipo de cómputo o su *smartphone*? ¿Qué sería lo que habría de más valor en él? Seguramente tendría en él fotografías de acontecimientos importantes, documentos de valor académico, empresarial, o personal; identificaciones, cuentas bancarias, claves de seguridad, datos personales que dicen quiénes somos, en donde vivimos, cuáles son nuestros gustos, quien es nuestra familia o que personas son importantes para nosotros.

Cuando hablamos de Internet, hablamos acerca de datos que compartimos en una gran red de comunicación a nivel mundial: paginas empresariales, blogs personales, álbumes en línea de fotos, documentos compartidos en la nube, redes sociales que informan a los demás de nuestras actividades, nuestros gustos, nuestros pasatiempos, nuestra formación académica, quienes somos, que papel jugamos en el entorno donde vivimos; la universalización de las tecnologías de la información, ha traído la aparición de multitud de entornos en los que se manejan y almacenan nuestros datos personales, es por ese motivo por el cual las empresas y, cada día en mayor número, los usuarios cotidianos de Internet, toman mayores medidas de prevención para la protección y aseguramiento de sus datos.

¿Qué pasaría si toda esa información cayera en manos de personas mal intencionadas?, y aun peor, ¿qué riesgos podríamos correr nosotros al dejar el acceso libre para que millones de personas cuenten con esa información acerca de nosotros?

Uno de los ejemplos más actuales está relacionado con la extracción de datos desde cuentas en línea por fallos en la seguridad. La compañía Apple sufrió un tropiezo en su sistema de seguridad que afectó gravemente su imagen y ya le ha costado una pérdida de valor bursátil de 25.000 millones de dólares. Un centenar de actrices y modelos han visto circular por la red fotografías y vídeos que creían a buen resguardo. Las imágenes fueron robadas de iCloud, el servicio que permite a los usuarios de Apple

almacenar contenidos y acceder a ellos desde cualquier dispositivo. (El País, 2014) Son estos hechos los que nos permiten ver hasta dónde puede llegar a afectar nuestra reputación e integridad estos datos, sin tomar en cuenta la información confidencial y bancaria que se pudo haber obtenido, nadie está exento de este tipo de riesgos.

Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado, es necesario concientizar a los usuarios de las tecnologías de la información sobre los riesgos en Internet y la importancia de la privacidad.

AMENAZAS GENERADAS POR CÓDIGO MALICIOSO

Cuando pensamos en los ataques en la red lo primero que viene a nuestra mente son programas de computadora que nos roban información o bloquean nuestros equipos. Los delincuentes han encontrado maneras de propagar códigos maliciosos como virus o *spyware* a través de las redes sociales y otros medios.

Cuando hablamos de código malicioso nos referimos a un código informático que provoca infracciones de seguridad para dañar un sistema informático. El código puede permitir que un cibercriminal tenga acceso remoto no autorizado al sistema atacado. (Kaspersky Lab, 2014)

El problema es que haciendo uso de estos servicios pueden elevar sus probabilidades de éxito pues explotan la confianza generada entre los usuarios de la misma red. A continuación se explicarán algunos de las herramientas que se utilizan para realizar este tipo de ataques:

Virus: Es un programa malicioso que requiere la intervención del usuario para ejecutarse o propagarse. Se copia en el equipo sin el consentimiento del usuario para causar acciones maliciosas y suele esconderse dentro de ciertos procesos del sistema operativo. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2014)

Gusano: Código malicioso que puede replicarse y distribuirse a sí mismo a través de una conexión de red de manera automática. Puede tomar acciones dañinas tales como consumir recursos de sistemas de red o locales causando problemas en los servicios. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2014)

***Spyware*:** Aplicación espía que recopila información sobre una persona u organización, como los hábitos de navegación, comportamiento en la web u otras cuestiones personales de utilización del sistema del usuario, las cuales se instalan y se ejecutan sin el conocimiento del usuario. Posteriormente, los datos son enviados al atacante.

Troyano: es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera (en inglés *backdoor*) que permite la administración remota a un usuario no autorizado. Algunas de las funciones de un troyano pueden incluir: robo de información personal, información bancaria, contraseñas, códigos de seguridad; monitorización del sistema y seguimiento de las acciones del usuario; captura de mensajes de texto entrantes y salientes; captura del registro de llamadas; habilidad para acceder

(consultar, eliminar y modificar) la agenda de contactos; habilidad para efectuar llamadas y enviar SMS; conocimiento de la posición geográfica del dispositivo mediante GPS; captura de la cámara; etcétera. (Kaspersky Lab, 2014)

Spam: Envío indiscriminado y no solicitado de publicidad, aunque también se lo emplea para la propagación de códigos maliciosos o para cometer *phishing*, principalmente a través de correo electrónico y últimamente hace uso de la mensajería instantánea, mensajes de celular, correos de voz y redes sociales. Representa un riesgo para la seguridad y tiene efectos secundarios, como el impacto negativo en la productividad del personal por la lectura de los mismos y el aumento del consumo de recursos. (ESET, 2014)

***Phishing*:** Es un conjunto de técnicas y mecanismos empleados por los intrusos o *hackers* con el propósito de robar información personal de un usuario y así poder suplantar su Identidad. Generalmente se hace pasar por una persona o empresa de confianza utilizando una aparente comunicación oficial electrónica como sitios web falsos con la apariencia de la página oficial, correos electrónicos, sistemas de mensajería instantánea o incluso llamadas telefónicas. Los atacantes buscan datos personales, información financiera como números de tarjeta, claves usuario, etc. (UNAM - CERT, 2009)

Un ejemplo que tenemos es el virus de la Policía Federal de México, el cual nos va a bloquear la computadora para pedirnos un rescate con el fin de estafar a usuarios inexpertos. Este virus se encuentra presente en muchísimos países, solamente cambia el nombre y la cantidad de la multa que debe pagarse. Puede llegar a infectar nuestro ordenador por navegar en sitios web maliciosos, o sitios web infectados por algún virus. Mediante mensajes de correo electrónico *spam* donde adjuntes archivos infectados o tengan enlaces maliciosos. Aprovecharán las vulnerabilidades de nuestro ordenador para introducirse e infectarnos con este problemático virus. Una vez infectados con el virus nos toma el control de la computadora bloqueando los componentes básicos como el menú Inicio, el Administrador de Tareas o el escritorio de Windows. Luego nos mostrará un mensaje pidiendo a la víctima pagar un rescate para desbloquear la computadora infectada. (El Universal, 2013)

AMENAZAS GENERADAS POR PROBLEMAS CON LA PRIVACIDAD

No todos los riesgos y los ataques en Internet se centran en programas de computadora que se instalan en nuestros equipos, existen diferentes amenazas y peligros a los cuales nos vemos expuestos al hacer un mal uso de los medios de comunicación en la red, por no tomar buenas medidas de seguridad, o por no tener una buena configuración de privacidad.

La privacidad no quiere decir que la información que publicamos en la red sea necesariamente “secreta”, entendemos por privacidad la habilidad de cada individuo de controlar que información revela de uno mismo en el conjunto de Internet, y de controlar quien puede acceder a ella. (Oficina de Seguridad del Internauta)

Las redes sociales se han convertido en una herramienta fundamental para la comunicación y colaboración de muchos proyectos escolares así como profesionales, sin embargo, estos medios también necesitan ser supervisados y regulados a fin de tener la suficiente privacidad como para evitar ciertos riesgos y amenazas que empiezan a ser cada vez más comunes hoy en día.

Los sitios de redes sociales basan su funcionamiento en la creación de un perfil personal y el establecimiento de relaciones de confianza entre los integrantes lo que permite establecer grupos donde es posible compartir datos. Entre la información compartida encontramos datos personales como: nombres, país, intereses, fotografías y en ciertos casos, es posible obtener la dirección o teléfono de una persona.

Desafortunadamente no todos los usuarios de estos servicios tienen buenas intenciones. Los casos de acoso y acecho en ocasiones ocurren como consecuencia de la información publicada, ya que los usuarios no son restrictivos con las personas que pueden acceder su red de amigos, de esta manera es posible obtener la información necesaria para acosar a una persona o un medio más para realizarlo.

A continuación analizaremos algunos de los principales peligros en los sitios de redes sociales y en la red en general que ocurren al no tener estas acciones en consideración.

Acoso: El acoso tradicional ocurría en directo, y la víctima podía encontrar cierto refugio en su hogar o en otro entorno. Sin embargo, ahora la persecución puede continuar en casa o donde sea, a través de la computadora o nuestro dispositivo móvil. Una gran diferencia es el anonimato que a veces facilita la red. A través de las redes sociales, acosadores encuentran un lugar ideal para acechar a sus víctimas, pues en este medio pueden conocer las actividades que realizan sus víctimas hasta tener contacto con ellos. Constituye un delito penal. El acoso mayormente se presenta entre personas adultas pero también existen los casos en los que el atacante mayor de edad acosa a usuarios jóvenes. Estos ataques pretenden causar angustia emocional, preocupación, y no tiene propósito legítimo para la elección de comunicaciones. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2009)

***Grooming*:** Se trata de la persuasión de un adulto hacia un niño con la finalidad de obtener una conexión emocional y generar un ambiente de confianza para conseguir satisfacción sexual a través de imágenes eróticas o pornográficas del menor. Muchas veces los adultos se hacen pasar por niños de su edad e intentan entablar una relación para, luego, buscar realizar encuentros personales, en algunos casos, con fines sexuales. El medio de contacto del agresor con el menor en muchas ocasiones se da a través de salas de chat, mensajería instantánea y redes sociales. (ESET, 2014)

***Ciberbullying*:** Es el uso de información electrónica y medios de comunicación tales como correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos móviles, y páginas de Internet difamatorias para acosar a un individuo o grupo, mediante ataques personales u otros medios. Se ha vuelto muy frecuente entre menores y jóvenes que lo utilizan para molestar a sus compañeros de clases. Uno de los casos que más impacto ha causado sobre el *bullying* y el *ciberbullying* ha sido el de la joven Amanda Todd, que a sus 15 años optó por quitarse la vida debido a la violencia que sus compañeros ejercieron sobre ella; dejo todo registrado en un video publicado en YouTube. (PantallasAmigas, 2012)

Sexting: El *sexting* consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles. Cuando se envían este tipo de imágenes y videos, se pierde por completo el control sobre ellos, ya sea que otras personas tengan acceso a ellos o se haga llegar a la persona equivocada, en cualquier situación, este material en manos de personas mal intencionadas puede llegar a ser perjudicial de muchas maneras para los propietarios originales. Aun con todas las implicaciones, esta es una práctica que está en

incremento por los jóvenes y los adolescentes, pudiendo tener implicaciones legales en algunos lugares si están involucrados menores de edad. (PantallasAmigas, 2014)

Robo de identidad: Usualmente los usuarios de redes sociales publican información personal, sin embargo, si los contenidos publicados no son protegidos de manera adecuada, estableciendo restricciones para que sólo las personas autorizadas puedan tener acceso, o bien, resguardando de manera correcta las claves de acceso y las medidas de seguridad al momento de navegar, es posible que usuarios malintencionados utilicen esta información en situaciones de robo de identidad, para obtener mayor información acerca de los usuarios, o bien obtener algún beneficio por parte de aquellos que le conocen. Nadie está exento de ser víctima de robo de identidad y más en México donde de acuerdo al IFAI, al 53 por ciento de la población "no le preocupa" o "le preocupa muy poco" lo que sucede con el manejo de sus datos personales. "Por un lado nos falta muchísimo en cuanto a la cultura de protección de datos, no es algo que tengamos nosotros interiorizado, no lo vemos como un derecho", señaló Alfonso Oñate secretario Protección de Datos del IFAI. (Noticieros Televisa, 2013)

Difamación: Debido a que los sitios de redes sociales no comprueban la identidad de la persona que crea un perfil, un usuario malintencionado podría generar un perfil de una persona en particular y publicar información falsa con el objetivo de difamarla. Además de ello y dado que es posible enviar mensajes a otros contactos que sean visibles al público, usuarios malintencionados podrían publicar información que sea vergonzosa para un usuario o grupo de usuarios. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2009)

Cámara Web: El uso de la cámara web es cada vez más común en los equipos domésticos, sobre todo cuando se trata de equipos portátiles que la llevan integrada de serie, y ahora con mayor alcance al estar presente en casi todos los teléfonos celulares. Si bien ofrecen algunos interesantes atractivos para la comunicación cara-a-cara en la Red e incluso para la creatividad artística o la difusión audiovisual de noticias; el uso inadecuado de la cámara web puede ocasionar serios problemas, sobre todo cuando son usadas por menores de edad. A través de programas de código malicioso pueden ser activadas remotamente sin nuestro consentimiento para obtener imágenes y audio que no deseamos compartir y que puede ser grabado por aquellos que toman el control de nuestro dispositivo. El uso inadecuado de las cámaras web y la falta de precauciones, facilita el trabajo de aquellos que buscan cometer delitos, en especial aquellos relacionados con el *grooming* y la extorsión. (PantallasAmigas, 2010)

Geo etiquetas: Debido a los avances de la tecnología, hoy en día es cada vez más común que las personas cuenten con dispositivos inteligentes (cámaras o *smartphones*) con acceso la red y dispositivos GPS que pueden etiquetar sus publicaciones o fotos brindando así información que tal vez no queremos compartir con todo el mundo, como los lugares que frecuentamos, el lugar en donde trabajamos o en donde vivimos. Redes sociales como Flickr, Twitter y Facebook han popularizado y facilitado el consumo de esta tecnología y cada vez son más los usuarios que aprovechan los beneficios de estos servicios. Las fotografías y los mensajes con geo etiquetas podrían generar un mapa ilustrando de nuestras actividades diarias, los lugares de convivencia con nuestra familia y amigos, así como la ubicación de nuestras pertenencias, esta información en manos de personas mal intencionadas podrían usarla para cometer actos criminales, como un secuestro o extorsión.

El proceso para tener acceso a esta información es muy sencillo. La información se puede extraer de algunos metadatos asignados a diferentes tipos de archivos, como formatos de audio, imagen o video, que tienen como fin brindar más información acerca del archivo en cuestión: como la información de fecha y hora, la configuración de la cámara, descripción e información sobre copyright, e incluso, información sobre localización, la cual podría provenir de un GPS conectado a la cámara o bien del GPS integrado a nuestros dispositivos móviles. Muchos de los dispositivos actuales tienen la opción de la geo etiqueta activada de manera predeterminada, con ella se graban en los archivos generados por nuestros dispositivos los datos necesarios para la ubicación de nuestros archivos, como la longitud y la latitud en donde fueron creados. Con la ayuda de algunos programas de libre acceso en la red, como la página http://exifdata.com/ o incluso algunos *plug-in* como Exif Viewer por Alan Raskin para el navegador web Firefox, y de manera muy sencilla, se pueden analizar los metadatos de las imágenes, conocidos como datos EXIF (*Exchangeable image file format*), e incluso obtener la ubicación y la vista aproximada del lugar con las opciones integradas que tienen de Google Maps y su Street View. Bastaría con una búsqueda en la red del nombre de usuario o el nombre de la persona que haya subido la foto para averiguar más sobre su información personal, para lo cual existen algunos buscadores de personas en la red como https://pipl.com/ que facilitan la tarea para encontrar a alguien en Internet.

Un caso ocurrido a alguien conocido fue en agosto del 2010, cuando Adam Savage, conductor del programa Cazadores de Mitos (*MythBusters*), publicó en Twitter una fotografía de un automóvil estacionado fuera de su casa, la imagen contenía una geo etiqueta con información exacta del lugar en el que se tomó la foto, revelando la dirección de su casa. Además el mensaje de la imagen decía “Voy al trabajo”. Con toda esta información publicada inconscientemente, el famoso conductor proporcionó datos muy valiosos que pudieron ser aprovechados por ladrones. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2011)

Al ver cada uno de estos peligros latentes en la red, podemos llegar a preguntarnos si es seguro o no utilizar estas nuevas tecnologías, más allá de eso, debemos considerar que acciones podrían detonar que nos veamos expuestos a estas amenazas, o de qué manera podemos vernos protegidos ante estos ataques antes de que ocurran.

2.3 Marco legal en México

El Derecho es el conjunto de normas que imponen deberes y normas que confieren facultades, que establecen las bases de convivencia social y cuyo fin es dotar a todos los miembros de la sociedad de los mínimos de seguridad, certeza, igualdad, libertad y justicia. (Pereznieto y Castro & Ledesma Mondragón, 1989)

Las normas penales buscan regular la convivencia de manera pacífica, de conformidad con ciertos principios y valores como lo son la igualdad ante la ley, la búsqueda del mayor bienestar para todos los ciudadanos, el respeto a los derechos fundamentales, la participación plena del ciudadano en la vida social, etcétera.

La función de prevención de delitos radica en esa obligación estatal de tutelar el desarrollo de la personalidad del individuo y su integración social, porque las normas penales se dirigen a la colectividad en forma de mensaje de advertencia hacia todos los ciudadanos en el sentido de que deberían abstenerse de dañarse entre sí. (Vargas, 2002)

Ya se ha mencionado que el delito supone un quebrantamiento de las normas, por lo tanto es necesaria que esta conducta sea cometida por alguien, en contra de otra persona que resentirá la conducta delictiva en sus intereses o patrimonio, siendo ellos el sujeto activo y el sujeto pasivo respectivamente.

Tomando en cuenta esto, podemos definir como un sujeto activo o imputado, a toda persona que ejecuta el acto delictivo definido en las leyes, ya sea participando como autor material al ejecutar directamente la conducta ilícita por sí mismo, como coautor cuando de alguna manera directa o indirecta participa en su comisión auxiliando a otros, o como autor intelectual al participar en la comisión del hecho delictuoso estimulando al autor o ideando la ejecución del mismo para que la realice otra persona.

El sujeto pasivo, víctima u ofendido, es aquella persona a la que le resulta lesionado un interés jurídico tutelado por la ley, o en otras palabras los derechos o cosas que la norma legal protege; los cuales pueden ser intereses individuales como son la vida, la libertad, la seguridad, entre otras; como también intereses colectivos siendo el caso de la sociedad como son las buenas costumbres, la moral pública, el medio ambiente; así mismo protege al Estado y a las personas morales en su patrimonio, su seguridad y algunos otros intereses. (Hernández Santana, 2004)

La autora del libro “Delitos Electrónicos” María de la Luz Lima, define: "delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.” (Lima, 1984)

La misma autora presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías:

- Como método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

- Como medio: son conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.
- Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Debido a la constante incursión que la tecnología ha tenido en nuestro modo de vida y las relaciones con la sociedad, se ha pretendido incluir en nuestras leyes los delitos relacionados con el uso de los medios informáticos, tanto en México como en diversos países. Como parte de este trabajo será necesario tener un panorama del ámbito legal existente en nuestro país, en específico analizaremos algunas de los delitos previstos dentro del Código Penal Federal y el Código Penal Para El Estado Libre Y Soberano De Quintana Roo. Estas leyes deberían permitirnos un uso más seguro de los recursos informáticos, y también ayudarnos a conocer los límites de nuestras acciones en Internet para no convertirnos en infractores. La prevención del delito se dará también en base al conocimiento que las personas tengan con respecto a qué clase de delitos pueden cometer al verse sujetos a estas mismas leyes, pudiendo jugar el papel en muchos casos tanto de sujetos pasivos como activos. Citaremos a continuación algunas de las leyes previstas en estos códigos, así como de otras iniciativas en cuanto a la privacidad de los datos que ha tomado el país:

Código Penal Federal

Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo

Artículo 202.- Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.

La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

Artículo 202 BIS.- Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

Turismo sexual en contra de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo

Artículo 203.- Comete el delito de turismo sexual quien promueva, publicite, invite, facilite o gestione por cualquier medio a que una o más personas viajen al interior o exterior del territorio nacional con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de dieciocho años de edad, o con una o varias personas que no tienen capacidad para comprender el significado del hecho o con una o varias personas que no tienen capacidad para resistirlo.

Al autor de este delito se le impondrá una pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

Trata de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo

Artículo 205-Bis. Serán imprescriptibles las sanciones señaladas en los artículos 200, 201 y 204. Asimismo, las sanciones señaladas en dichos artículos se aumentarán al doble de la que corresponda cuando el autor tuviere para con la víctima, alguna de las siguientes relaciones:

i) Cuando el autor emplee violencia física, psicológica o moral en contra de la víctima; y

j) Quien esté ligado con la víctima por un lazo afectivo o de amistad, de gratitud, o algún otro que pueda influir en obtener la confianza de ésta.

Revelación de secretos

Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Amenazas

Artículo 282.- Se aplicará sanción de tres días a un año de prisión o de 180 a 360 días multa:

I.- Al que de cualquier modo amenace a otro con causarle un mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado con algún vínculo, y

II.- Al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho a hacer.

De los delitos en materia de derechos de autor

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 426.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Fraude y Extorsión

Los artículos 386 y 390 del Código Penal Federal no establecen penas por actos relacionados con equipos electrónicos, ya sea como medio o como fin, sin embargo valdría la pena revisar la legislación en estos y en otros artículos ya citados para agregar dentro de las particularidades el uso de los medios electrónicos en la comisión del delito. Aun así, estos artículos pueden ser utilizados como referencia en delitos relacionados y nos dan una idea de las adecuaciones que se tienen que hacer para establecer una mejor legislación en cuanto a materia de delitos informáticos en el país.

Código Penal Para El Estado Libre Y Soberano De Quintana Roo
Revelación de secreto

Artículo 126.- Al que sin consentimiento del que tenga derecho a otorgarlo revele un secreto que por cualquier forma haya conocido o se le haya confiado, o lo emplee en provecho propio o ajeno, se le impondrá prisión de seis meses a dos años y hasta cincuenta días multa y suspensión de sus funciones de dos meses a un año, si de la revelación o empleo pudiera resultar un perjuicio para alguien.

Cuando el secreto se revele o se use en beneficio propio o ajeno por persona que preste servicios profesionales o técnicos, o por servidor público, o si el secreto fuere de carácter científico o industrial, la pena se aumentará hasta una mitad más.

Extorsión

Artículo 156.- A quien con ánimo de lucro para sí o para otro, obligare a otra persona, con violencia moral o intimidación, a realizar, omitir, o tolerar un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero, se le impondrá de doce a dieciocho años de prisión y de ochocientos a mil días multa.

Cuando en la comisión del delito se utilice la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica, la pena será de veintidós a veintiocho años de prisión y la multa de mil doscientos a mil quinientos días multa.

Falsificación de documentos

Artículo 189.- Se impondrá prisión de seis meses a tres años y de quince a noventa días multa, al que para obtener un beneficio o para causar un daño, falsifique o altere un documento público o privado.

Artículo 189 Bis.- Se impondrá hasta una mitad más de las penas previstas en el artículo anterior al que:

IV.- Accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Pornografía infantil

Artículo 192-BIS.- Comete el delito de pornografía infantil quien, a persona menor de dieciocho años:

III.- Promueva, invite, facilite o gestione por cualquier medio, la realización de actividades en las que se ofrezca la posibilidad de observar actos de exhibicionismo corporal o de pornografía, que estén siendo llevadas a cabo por persona menor de dieciocho años de edad. Comete también el delito de pornografía infantil el que siendo mayor de edad, participe como activo o pasivo en los actos de exhibicionismo corporal o de pornografía realizados por persona menor de edad.

Se entiende por actos de exhibicionismo corporal a toda representación del cuerpo humano, con fin lascivo sexual.

Se considera acto de pornografía a toda representación realizada por cualquier medio, de actividades lascivas sexuales explícitas, reales o simuladas.

Artículo 192-TER.- También se entenderá como pornografía infantil, aplicándose la misma pena establecida en el artículo anterior, al que:

I.- Con o sin fines de lucro, fije, imprime o exponga de cualquier manera, los actos de exhibicionismo corporal o de pornografía realizados por persona menor de dieciocho años de edad;

II.- Con o sin fines de lucro, elabore, reproduzca, distribuya, venda, arriende, posea, almacene, adquiera, publicite o transmita material que contenga actos de exhibicionismo corporal o de pornografía realizados por persona menor de dieciocho años de edad;

Turismo sexual

Artículo 192-QUÁTER.- Comete el delito de turismo sexual quien financie, promueva, publicite, invite, facilite o gestione por cualquier medio para que una persona viaje al interior o exterior del territorio del Estado de Quintana Roo con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de dieciocho años de edad o que no tengan la capacidad de comprender el significado del hecho. Al autor de este delito se le impondrá una pena de siete a quince años de prisión y de trescientos a quinientos días de multa.

Violación de la intimidad

Artículo 194-BIS.- Se sancionará con prisión de seis meses a cuatro años y de cien a trescientos días multa, a quien sin consentimiento de otro, o sin autorización judicial y con el fin de conocer asuntos relacionados con la intimidad personal o familiar de aquél, utilizando cualquier medio:

I.- Se apodere de documentos u objetos de cualquier clase;

II.- Reproduzca los documentos u objetos que contengan información relacionada; o

III.- Escuche, observe, o grabe una imagen fija o en movimiento, el sonido, o ambos.

Para efectos de lo dispuesto en el presente Capítulo, deberá entenderse por derecho a la intimidad, la manifestación concreta de la separación entre el ámbito privado y el público. Se asocia con la existencia de un ámbito privado que se encuentra reservado frente a la acción y conocimiento de los demás y tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sea simples, particulares o bien los poderes del Estado.

Artículo 194-TER.- Se sancionará con prisión de uno a cinco años y de doscientos a trescientos días multa a quien revele, distribuya, transmita o lucre con la intimidad personal o familiar prevista en el artículo que antecede.

Usurpación de identidad

Artículo 195-Sexties. El delito de usurpación se define como al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro la identidad de una persona otorgue consentimiento para llegar a cabo la usurpación o suplantación de su identidad, se le impondrá una pena de seis meses a seis años de prisión y de cuatrocientos a seiscientos días de multa.

Artículo 195-Septies. Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el artículo 195-Sexties a quienes:

II. Utilicen datos personales sin consentimiento al que deba otorgarlo;

IV. Al que por algún uso del medio informático, telemático o electrónico, o use la red de Internet montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecta la confiabilidad y variación de la navegación de la red para obtener lucro indebido.

En el supuesto que el activo tenga licenciatura, ingeniería o cualquier grado académico reconocido en los rubros antes mencionados, la pena se aumentara hasta en una mitad más.

Ley federal de protección de datos personales en posesión de particulares

La protección de datos personales se remonta a 1948, cuando la Asamblea General de las Naciones Unidas adopta el documento conocido como Declaración Universal de Derechos Humanos, en este documento se expresan los derechos humanos conocidos como básicos. En el artículo 12 se señala lo siguiente: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

En varios países del mundo hay esfuerzos por crear legislaciones que establezcan los límites, permisos y castigos entorno al manejo adecuado de los datos contenidos en los sistemas de información, sobre todo de aquellos definidos como datos personales.

Uniéndose a estos esfuerzos por legislar y proteger la seguridad de la información y privacidad de las personas, México promulgó la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), la cual fue publicada el 5 de julio de 2010 en el Diario Oficial de la Federación y entró en vigor el 6 de julio de 2010.

Esta ley pretende salvaguardar el respeto a la privacidad, dignidad e información de las personas. En ella se establecen cuatro derechos fundamentales que tienen los individuos sobre su información en posesión de cualquier persona física o empresa particular (aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades, etc.), son los denominados derechos ARCO: Acceso, Rectificación, Corrección y Oposición. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2012)

La ley define a los datos personales como cualquier información que haga a una persona identificada o identificable, y a su vez menciona que, son datos personales sensibles aquellos datos que afecten a la esfera más íntima de su titular, como podrían ser estado de salud, preferencias religiosas o sexuales.

Otro de los puntos a los cuales hace referencia esta ley es sobre el Aviso de Privacidad, el cual es un texto en donde se define al titular de los datos el tratamiento que se le dará a la información obtenida por el particular, documento que puede ofrecerse de manera impresa o electrónica, como por ejemplo a través de un enlace en una página web. La ley y su reglamento mencionan en varios de sus artículos la forma que tendrá este aviso de privacidad.

Capítulo 3

3.1 Culturizar para la prevención de delitos

Existen muchos factores que pueden influir en nuestra seguridad en línea, algunos de ellos son errores técnicos, otros son causados por personas externas mal intencionadas, pero en su mayoría, los delitos informáticos y los incidentes relacionados con nuestra seguridad y privacidad, son causados por el usuario mismo, por su falta de interés o su falta de preparación para usar correctamente los medios informáticos de comunicación.

La falta de cultura de la prevención no es algo nuevo, más bien es una cuestión de cultura infundada en cada usuario por nuestra sociedad. Se puede observar, por ejemplo, con una simple pregunta: ¿Cuántos de nosotros vamos al doctor o al dentista de forma preventiva? Es muy probable que muchos de nosotros solo acudamos a esos servicios únicamente en caso de que se presente alguna situación y nos veamos obligados a hacerlo. Ocurre lo mismo en las cuestiones informáticas relacionadas con seguridad en una organización, ¿Cuántos de nosotros nos acercamos al departamento encargado de incidentes informáticos solo de manera preventiva?, ¿Cuántos usuarios llegan a preguntar acerca de su sistema o su antivirus que envía mensajes de error y actualización sin saber qué hacer? Lamentablemente, la falta de cultura de la prevención es un reflejo de la sociedad en que vivimos.

Hoy en día, cada vez más administradores de tecnologías de la información en diversas empresas se ven más interesados por las cuestiones de seguridad y privacidad de la información, y cada vez más directivos empiezan a comprender la importancia de estos temas para el correcto funcionamiento de su organización, empiezan a realizarse inversiones de tiempo, dinero y esfuerzo en las cuestiones de seguridad, con sistemas de respuesta a incidentes robustos, utilizando los mejores servicios al alcance, y estableciendo políticas que harán que la información y la seguridad organizacional se mantenga estable. Sin embargo, todos aquellos que saben sobre estas medidas de seguridad y han intentado aplicarlas conocen una de las dificultades más grandes para su desarrollo, que es la resistencia al cambio organizacional por parte de los usuarios, y precisamente uno de estos cambios es crear la cultura de la prevención. Pero, ¿qué podemos hacer cada uno de nosotros para crear conciencia de los riesgos de seguridad de la información?

Según los reportes que se han dado por parte de la empresa Verizon (Data Breach Investigations Report, 2014), de los 100,000 ataques analizados de los últimos 10 años, el 92% de los ataques pueden resumirse en 9 patrones básicos de conducta, por lo que es evidente que los esfuerzos en cuanto a la prevención de incidentes no han sido suficientes. El ayudar en esta creación de conciencia y esforzarnos por hacerlo una costumbre será algo que beneficiara a todos. Robo y fuga de información, mala configuración y uso de los servicios dejando brechas de seguridad, y la ingeniería social, han sido algunos de los medios que los atacantes han utilizado y que se podrían reducir al generar y promover medidas de prevención y seguridad para los usuarios a través de campañas de concientización que aborden la importancia de estos temas y las medidas simples que ellos pueden tomar.

Las autoridades gubernamentales han mencionado un gran número de impedimentos para reducir el delito cibernético y aumentar la seguridad cibernética en México. Uno de ellos es la constante falta de legislación

que permita a las entidades policiales actuar en forma inmediata para enfrentar las amenazas a la seguridad cibernética y los incidentes de delito cibernético. La capacidad limitada de las entidades policiales para actuar en muchas instancias debilita las investigaciones, perpetúa la sensación de impunidad entre los grupos criminales organizados y les permite implementar las últimas tecnologías y técnicas para cometer delitos. El otro gran impedimento identificado es la constante falta de conciencia entre la población general sobre seguridad cibernética, incluidos riesgos y prácticas recomendadas. (Organizacion de los Estados Americanos, 2014)

La protección de los datos personales y financieros es una actividad fundamental que se debe realizar con absoluta responsabilidad y conciencia. (Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2012)

Para crear una cultura de la prevención efectiva en las organizaciones y más particularmente entre los usuarios, se debe acelerar la disponibilidad de la información y de los recursos educativos, a través de programas de seguridad que incluyan diferentes campañas de concientización, y con la ayuda de ellas proporcionar las herramientas adecuadas para los usuarios.

Viendo la necesidad de fomentar una adecuada cultura de la prevención de riesgos informáticos entre los usuarios de la red universitaria, tomaremos como base algunos de los recursos que se encuentran en el documento de la *National Institute of Standards and Technology NIST 800-50 "Building an Information Technology Security Awareness and Training Program"* (Cómo construir una campaña de concientización y entrenamiento para la cultura de seguridad) para poder definir la estructura básica que deben seguir estas campañas. Se espera con esto establecer una base de trabajo para esta necesidad tan imperante en la universidad.

3.2 Estructura de una Campaña de Concientización

Los esfuerzos de una campaña de concientización de seguridad están orientados en cambiar el comportamiento o reforzar las buenas prácticas de seguridad en una organización. Una campaña de concientización no es igual a un programa de capacitación. El propósito de la campaña de concientización es simplemente enfocar la atención en la seguridad, se pretende que estas campañas permitan a los individuos reconocer las principales preocupaciones relacionadas con las tecnologías de la información y responder adecuadamente ante ellas. En las campañas de concientización, la audiencia es aquella que únicamente recibe la información y aprende, mientras que en un programa de capacitación el receptor tiene un papel más activo.

Una campaña de concientización pretende llegar a una audiencia más amplia con un paquete de técnicas de seguridad atractivas en su aplicación, mientras que un programa de capacitación es un tanto más formal, con el objetivo de tener una base firme de conocimiento y desarrollar habilidades técnicas que facilitaran el trabajo diario. Para que cumpla su objetivo, cada una de las actividades y medidas que se propongan en esta campaña de concientización, deberán estar dirigidas a un sector específico y contar con una serie de recomendaciones para su aplicación, de ser posible, relacionadas con las tareas cotidianas de los usuarios; si los esfuerzos no están bien dirigidos y la comunicación de la información no

es clara, los resultados obtenidos distarían mucho de nuestro objetivo, y podría ser incluso un tema más para evitar y sin utilidad por parte de los usuarios.

Una buena campaña de concientización debe estar diseñada con el propósito de la organización en mente, ya que su objetivo es ayudar a los usuarios a utilizar de mejor manera los recursos de la red a fin de cumplir con los objetivos organizacionales. Las campañas de concientización más exitosas son aquellas en donde los hechos y las problemáticas presentadas tienen un carácter relevante y útil para el usuario. Es por este motivo que, tanto los administradores de sistema como los usuarios, necesitan tomar conciencia sobre las medidas de seguridad en la organización, los riesgos a los que se exponen durante las operaciones diarias, y el impacto que esto puede llegar a tener dentro de la organización.

Para determinar el tipo de necesidades que deben cubrir las campañas de concientización en una organización, se pueden utilizar diferentes fuentes y se puede recolectar de diversas maneras. En nuestro caso en particular podemos hacer uso de algunas de las siguientes:

- Entrevistas con todas las organizaciones y los grupos clave previamente identificados.
- Encuestas a las diferentes organizaciones y grupos clave.
- Revisión a los programas y medidas de concientización y capacitación existentes en la organización.
- Revisión del sistema general para identificar las aplicaciones utilizadas y quienes son lo que hacen mayor uso de ellas, así como las políticas de seguridad que se aplican en él.
- Revisión de las medidas de seguridad sugeridas por organizaciones externas calificadas en la materia.
- Conversaciones y entrevistas con los encargados de los departamentos, administradores, técnicos que tengan roles dentro de la operación del sistema y soporte.
- Análisis de eventos: resultados previos de ataques de denegación de servicios, intrusiones a la plataforma web, modificaciones de terceros no autorizados en el sistema, ataques de virus y amenazas en la red, problemas técnicos más comunes en la organización, etc.
- Un estudio sobre las amenazas más comunes dentro del campo de servicio de la organización que informan diversas fuentes especializadas, podría proveer una idea de los puntos en los que se tienen que hacer conciencia antes de que llegue a ser un problema para la organización.

El análisis de la información obtenida por estos medios debe dar respuesta a las siguientes preguntas clave:

- ¿Que se está haciendo actualmente en la organización para solucionar estas necesidades?
- ¿Cuál es la situación actual con respecto a cómo se están tratando estas necesidades?
- ¿Dónde están las brechas entre las necesidades y lo que se está haciendo?
- ¿Cuál de las necesidades es la más crítica?

Después de contestar estas preguntas debemos elaborar un plan de acción para las campañas a implementar, en donde se establecerá la estrategia para llevarlas a cabo. El plan para las campañas de concientización puede contener los siguientes puntos:

- Políticas locales y nacionales existentes por parte de las entidades pertinentes que requieren conocimiento y capacitación para poder ser realizados
- Alcance de las campañas de concientización y capacitación
- Roles y responsabilidades del personal designado que diseñara, desarrollara, implementara y mantendrá las campañas de concientización y capacitación, y quien debe asegurarse de que los usuarios adecuados asistan.
- Objetivos que deben cumplirse para cada aspecto de las campañas (por ejemplo, la sensibilización, la formación, la educación, el desarrollo profesional [certificación]);
- A quien está dirigido cada aspecto de las campañas;
- Objetivos de aprendizaje para cada aspecto de las campañas;
- Los temas a tratar en cada sesión o curso;
- Métodos de implementación que se utilizarán para cada aspecto de las campañas;
- Documentación, información y evidencia de aprendizaje para cada aspecto de las campañas;
- Evaluación y actualización del material para cada aspecto de las campañas; y
- Frecuencia que cada audiencia debe estar expuesto al material del curso.

Una vez que el plan de capacitación se ha finalizado, debe ser establecido un calendario de implementación. Si esto tiene que ocurrir en fases (por ejemplo, debido a las restricciones presupuestarias y la disponibilidad de recursos), es importante identificar los factores que se utilizarán en la determinación de cual iniciativa programar primero y en qué secuencia. Los factores clave a tener en cuenta son:

- **Disponibilidad del material y de los recursos:** Si los materiales y los recursos para las campañas pueden prepararse con prontitud, entonces las campañas podrán implementarse de manera ágil. Sin embargo si los materiales aún tiene que ser preparados y los instructores necesitan ser identificados y programados, este es un punto que debe tomarse en cuenta para la calendarización de las campañas.
- **Impacto organizacional:** Es muy común asignar la prioridad en base al sector organizacional que más lo requiere y el impacto que este tendrá en el desarrollo de las labores de la organización, comúnmente los sectores relacionados con las tecnologías de la información y los administradores y responsables de los sistemas poseen mayor prioridad por el impacto que estos tendrán al aplicar la información recibida durante las capacitaciones.

- **Cumplimiento actual de las normas:** Este punto hace referencia en identificar los puntos con más deficiencia dentro de los problemas a corregir, y ubicar las áreas involucradas para solucionarlo con mayor prontitud.
- **Dependencias críticas para el desarrollo de un proyecto:** Si existen áreas que necesitan ser capacitadas para impulsar algún proyecto de acuerdo con su tiempo establecido, se deberá tomar en consideración la capacitación para esa área con el fin de optimizar su desarrollo.

Otro aspecto importante a considerar es el nivel de complejidad para el material que se desarrollará. La complejidad debe de ser adecuada con el rol que las personas desempeñen dentro de la organización, el material debe ser desarrollado de acuerdo a la posición que ocupa la audiencia de la campaña y las habilidades necesarias para la seguridad que necesitan aplicar en su rol. Generalmente el propósito de una campaña de concientización es simplemente ayudar a enfocarse y poner atención a las buenas prácticas de seguridad, el mensaje que deben transmitir debe ser corto y simple. El mensaje puede contener uno o más temas en los que la audiencia debe tomar precauciones. Lo ideal es que la audiencia de las campañas de concientización incluya a todos los usuarios de la organización. El mensaje que se transmitirá en ellas debe de ayudar a cada individuo a ser consciente de las responsabilidades de seguridad de la información que comparten con los demás.

El análisis previo nos permitirá determinar las necesidades a cubrir, se pueden mencionar y discutir brevemente un número significativo de temas en estas campañas de concientización. Los temas pueden incluir:

- Uso y administración de contraseñas ;
- Protección de virus, malware, troyanos y otros códigos maliciosos;
- Implicaciones de no cumplir con las políticas organizacionales;
- Uso adecuado de Internet, correo electrónico y redes sociales;
- Copias de respaldo de datos;
- Ingeniería Social;
- Respuesta a incidentes;
- *Shoulder Surfing*;
- Seguridad en dispositivos móviles;
- Uso de encriptación para la transmisión de datos confidenciales a través de Internet;
- Aplicación adecuada de parches y actualizaciones…

Hay toda una variedad de fuentes para los materiales relacionados con la concientización de seguridad que pueden ser incorporados a las campañas de concientización. Los materiales pueden referirse a una

problemática en particular, o en algunos casos, pueden incluir diversos temas a fin de llevar a cabo todo un programa de concientización y seguridad más completo. Algunas de las fuentes que se pueden utilizar para el desarrollo de estas campañas de concientización son:

- Boletines por industrias, grupos, cuerpos académicos o el departamento encargado de las Tecnologías de la Información de la organización;
- Organizaciones y proveedores profesionales de Tecnologías de la Información;
- Conferencias, seminarios y cursos;
- Noticias en línea de sitios relacionados con Tecnologías de la Información.

El material de concientización puede ser desarrollado tomando en cuenta un solo tema a la vez o se puede crear combinando un cierto número de temas en una sola sesión. Independientemente de la manera en cómo se presente, la cantidad de información no debe de abrumar a la audiencia. Una breve reseña de las políticas, los problemas que se buscan remediar, y las acciones a tomar son en su mayor parte la manera en cómo abordar a la audiencia en una sesión de estas campañas.

Existen diversas técnicas para que el mensaje de las campañas de concientización de seguridad pueda ser esparcido por toda la organización, estas técnicas dependerán de los recursos y de la complejidad del mensaje. Algunas de las técnicas o medios que se pueden incluir para difusión, son:

- Materiales con mensajes de prevención (plumas, botones, calcomanías, post-it, marcadores, unidades de memoria con mensajes, llaveros, entre otros)
- Posters, recordatorios impresos de listas de verificación y prácticas seguras e inseguras.
- Protectores y fondos de pantalla, mensajes, y banners de advertencia.
- Boletines informativos
- Recordatorios y consejos a través de correo electrónico
- Videos
- Sesiones de teleconferencias
- Días de seguridad o programas similares

Algunos de esto recursos permiten la transmisión de breves mensajes de un solo tema, como los materiales impresos como plumas, botones, calcomanías, posters, y otros; sin embargo algunos pueden contener también una variedad de temas más extensos en un solo medio como lo son los boletines, videos y teleconferencias. Las técnicas que pueden ser implementadas sin altos costos de producción pueden ser los posters y los banners, en este caso con la ayuda de los departamentos encargados de publicidad e imagen de la organización, recordatorios por correo electrónico, y periódicamente algunos boletines

electrónicos. La presentación de videos, teleconferencias, y los días de seguridad o programas similares, pueden llegar a requerir mayor cantidad de recursos y planeación.

Además de hacer el material para prevención interesante y con temas de actualidad, el repetir el mismo mensaje de prevención y el usar diversas maneras de representar el mensaje, puede incrementar la retención de los consejos y problemáticas en los usuarios. La mejora continua debe ser siempre el lema para todas las iniciativas de concientización y seguridad, debido a que en estas áreas nunca se puede hacer suficiente.

Otra parte importante en el desarrollo de estas campañas de concientización es la implementación de mecanismos de evaluación y retroalimentación, ya que estos son críticos para la mejora continua, y esta no podría darse sin una buena información de cómo el programa actual está funcionando. Adicionalmente, el mecanismo de retroalimentación debe ser diseñado para poder medir los objetivos establecidos al inicio del desarrollo de las campañas.

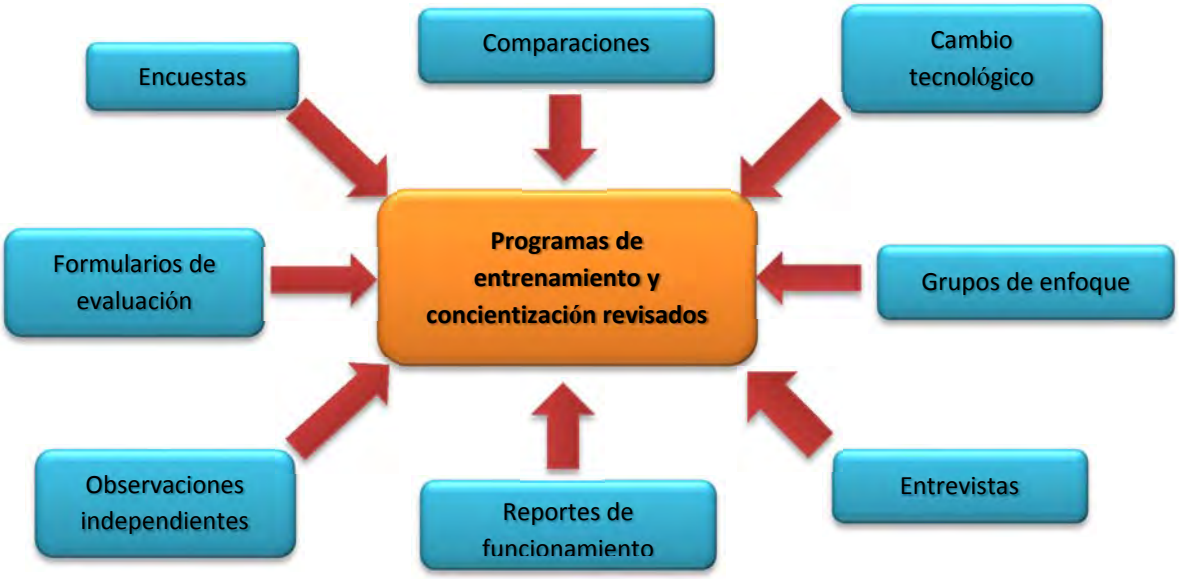


DIAGRAMA 1. TÉCNICAS DE EVALUACIÓN Y RETROALIMENTACIÓN

La administración y actualización de cambios debe ser el componente de las campañas diseñado para asegurarse que estos programas no se estanquen y se vuelvan irrelevantes ante las nuevas amenazas emergentes que pueda enfrentar nuestra organización; así como también el dirigir los cambios en los procedimientos y las políticas de seguridad. De la misma manera en como establecimos un nivel para definir la complejidad de los materiales, será necesario ajustar las expectativas a medida que se concientiza y se aplican las nuevas políticas para mejorar el entorno de seguridad de la organización.

Los directores de tecnologías de la información, encargados de programas, y los administradores del programa de seguridad de tecnologías de la información deben estar principalmente enfocados en un mejoramiento continuo, una manera es por medio de brindar soporte a estas campañas de concientización dentro de la organización. Es importante que cada uno de ellos pueda ser capaz de llevar sus responsabilidades de acuerdo a su rol de seguridad en la organización.

Cuando hablamos de seguridad, la frase “tan fuerte como el eslabón más débil” es verdad, asegurar la información y la infraestructura de una organización es un esfuerzo de equipo.

3.3 Ejemplo de una sesión de la campaña de concientización y cultura informática para la Universidad de Quintana Roo

Como parte de la preparación de estas sesiones para la campaña de concientización, se realizaron entrevistas con Luis Fernando Mis Ramírez, coordinador del área de Redes y Soporte de la Dirección de Informática, en las que pudimos observar algunas necesidades que la Universidad tiene y que pueden verse fortalecidas a través de estas campañas:

- La mayoría de los problemas en la red universitaria están relacionados con el correo electrónico, como lo es el envío excesivo de correo no deseado o *spam*, la administración de contraseñas, y un uso eficiente de las nuevas tecnologías aplicadas; problemas de acceso a los portales del sistema de administración escolar, en su mayoría relacionados con la disponibilidad del servicio; y problemas relacionados con la navegación en Internet en general, mencionando principalmente el impacto en la velocidad del servicio. Otro problema recurrente son los códigos maliciosos que se distribuyen a través de medios de almacenamiento y por equipos infectados en la red.

- Hasta el momento, la Dirección de Informática no ha tenido reportes de ataques o incidentes relacionados con delitos informáticos generados dentro del mismo campus, sin embargo se han reportado casos en los que los usuarios se han visto amenazados por estos peligros por usuarios fuera de las instalaciones de la universidad y se han tomado las medidas necesarias.

- Se están llevando a cabo pláticas breves para mejorar la seguridad en el uso del correo electrónico y de los portales del sistema de administración escolar para los alumnos de nuevo ingreso, así como tutoriales en línea en la página de cómputo e informática de la Universidad relacionados con temas básicos de seguridad. Es necesario actualizar este último punto con las problemáticas más comunes y retomar su difusión a través de boletines informativos por medio del correo electrónico.

- No se cuenta con una infraestructura de seguridad que mitigue los riesgos, o asegure las comunicaciones de manera interna. Los dispositivos y políticas que se tienen en el Departamento de Informática, son para proteger la información y los servicios de atacantes externos. Tampoco se cuenta con políticas firmes en cuanto a la privacidad de los datos personales manejados en la universidad, se mencionó que es una de las cosas que se busca desarrollar para futuras certificaciones de seguridad. Por estas razones, es necesario incrementar la conciencia informática en los usuarios, debido a que la responsabilidad de aplicar las diferentes medidas preventivas recae principalmente en ellos, a fin de mantener sus comunicaciones y su información a salvo de atacantes y programas maliciosos dentro de la red informática universitaria.

UNIVERSIDAD DE QUINTANA ROO

PROGRAMA DE CONCIENTIZACIÓN Y CULTURA INFORMÁTICA: PELIGROS Y AMENAZAS EN REDES SOCIALES

Siendo la Universidad de Quintana Roo un centro de educación superior, su principal fin es el formar profesionistas sólidamente preparados, comprometidos con el progreso del ser humano, fuertemente vinculados con la sociedad, capaces de contribuir al fortalecimiento de la cultura y al desarrollo social y económico de Quintana Roo y México.

Las nuevas tecnologías de la información, así como los usos y los riesgos que ello conlleva, son ahora parte de la sociedad global creciente, por lo cual la adecuada preparación de los profesionistas egresados de esta institución con respecto al uso y la interacción con estos nuevos medios, deberá reflejar el espíritu del quehacer de la Universidad.

Como parte de los esfuerzos de la Universidad de Quintana Roo en su programa de capacitación y concientización a los usuarios de la red, se impartirán conferencias en donde participaran usuarios de toda la red universitaria en el Campus Chetumal, tanto alumnos así como docentes y personal administrativo, y se difundirá a través de los diferentes medios electrónicos e impresos con que cuenta la universidad. Se pretende que estas acciones permitan a los participantes reconocer las principales preocupaciones relacionadas con las tecnologías de la información, el uso adecuado de las redes sociales y las amenazas que existen en ellas, así como consejos y prácticas básicas que les permitirán un manejo más seguro de estos medios de comunicación. Se pretende realizar un acercamiento a las redes sociales con mayor impacto entre los usuarios de la red universitaria, se desarrollaran las pláticas adaptándolas a la plataforma a analizar. Estas sesiones pueden realizarse como parte de un curso de inducción a la universidad, como sesiones de capacitación aisladas, o en el marco de eventos tecnológicos realizados por la universidad.

Debido a que el programa está dirigido a toda la comunidad universitaria, con diferentes niveles de conocimiento en cuanto al tema, se desarrollarán materiales con definiciones de los riesgos y consejos muy básicos, adecuados para que cualquiera pueda comprender y aplicar las recomendaciones brindadas.

La difusión de esta sesión se hará por medio del correo electrónico e invitaciones por parte de Bienestar Estudiantil.

Peligros Y Amenazas En Redes Sociales: Facebook

Análisis de la plataforma

- Funcionamiento y características: Explica las diferentes características de la plataforma, a manera de interactuar con los demás usuarios, y las principales actividades que se realizan en ella.
- Estadísticas breves: Proporciona información sobre el uso de la plataforma en el entorno a estudiar así como las formas de uso más comunes entre los usuarios de la red.

Análisis de riesgos

- Definiciones de riesgos: Se explicaran las amenazas con mayor incidencia a las que se enfrentan los jóvenes al hacer uso de las redes sociales.
- Metodología de los ataques: Se expondrán los diferentes medios por los cuales los atacantes sacan provecho de estas vulnerabilidades para cumplir con sus propósitos.
- Impacto en la seguridad: Se pretende sensibilizar a la audiencia sobre las diferentes repercusiones que estas amenazas pueden tener en su seguridad y su integridad, tanto en la red, como en su reputación y su integridad física.
- Casos de estudio: Se pretende analizar algunos casos en los que se han realizado ciertas acciones delictivas a través de las redes sociales, y exponer algunas recomendaciones básicas para prevenir en lo futuro este tipo de amenazas.

Análisis de medidas preventivas

- Medidas de privacidad y seguridad a tomar en cuenta para una navegación segura en Internet y las redes sociales: Se analizaran algunos medios impresos con recomendaciones básicas que se proveerán a la audiencia para su información de consejos básicos para el uso adecuado de esta plataforma.
- Se entregaran trípticos con consejos básicos y se realizara una campaña con posters en lugares estratégicos, medios que podrían ser diseñados por la universidad o utilizar los ya publicados por organismos especializados en la materia.

Retroalimentación.

- Análisis del impacto en la audiencia: Se aplicará una pequeña encuesta informativa para determinar hasta qué grado la audiencia tenía conocimiento de estas amenazas y la manera en que la información proporcionada ha cambiado su perspectiva sobre el uso de las redes sociales

MEDIOS IMPRESOS

UNIVERSIDAD DE QUINTANA ROO

PROGRAMA DE CONCIENTIZACIÓN Y CULTURA INFORMÁTICA:

PELIGROS Y AMENAZAS EN REDES SOCIALES

Edad: Sexo: Carrera:

1.- A continuación te mostramos una serie de enunciados. Selecciona el que refleja mejor cómo te sientes al utilizar Internet:

- ☐ "Internet me permite comunicarme, estar en contacto con mis amigos y ampliar mi círculo social"
- ☐ "Internet me ofrece posibilidades inmensas de conocimiento e información"
- ☐ "Internet me vigila. Cada una de mis acciones, por ejemplo los contenidos que visito, deja rastro"

2.- ¿Cómo calificarías tu nivel de preocupación con respecto a la privacidad en Internet?

- ☐ Muy preocupado
- ☐ Moderadamente preocupado
- ☐ Poco preocupado
- ☐ Nada preocupado

3.- Selecciona las redes sociales que utilizas habitualmente:

- ☐ Facebook
- ☐ Twitter
- ☐ Youtube
- ☐ Instagram
- ☐ Google+
- ☐ Pinterest
- ☐ Foursquare
- ☐ Whatsapp
- ☐ Vine

4.- ¿Sabes qué información de tu cuenta o perfil es la que los demás usuarios ven sobre ti?

- ☐ Si
- ☐ No

5.- ¿Qué grado de facilidad o dificultad encuentras en configurar la privacidad de tu perfil?

- ☐ Me resulta sencillo, he conseguido hacerlo
- ☐ Me resulta complicado, pero he conseguido hacerlo
- ☐ Me resulta complicado, no he sido capaz de hacerlo
- ☐ No utilizo la configuración de privacidad en mi perfil

6.- ¿Podrías indicarnos si alguna vez has hecho alguna de las siguientes actividades en la red social?

- [ ] Eliminación de contactos de la lista de amigos
- [ ] Bloqueo de contactos
- [ ] Geo-etiquetado automático
- [ ] Des-etiquetado de fotografías publicadas por otros
- [ ] Etiquetado de otros usuarios sin su permiso
- [ ] Eliminación de contenido publicado por el mismo usuario
- [ ] Eliminación de comentarios del perfil del usuario publicados por terceros
- [ ] Denuncia a un usuario por insultos, amenazas, acoso, etc.

7.- ¿Habías escuchado sobre los riesgos y amenazas de las redes sociales?

- [ ] No
- [ ] Solo sobre algunos
- [ ] Si

8.- La información proporcionada, ¿cambio en algo la perspectiva que tenías sobre los riesgos y amenazas en las redes sociales?

- [ ] Si
- [ ] No

9.- ¿Crees que podemos vernos expuestos a estas amenazas en donde vivimos?

- [ ] Si
- [ ] Probablemente
- [ ] No

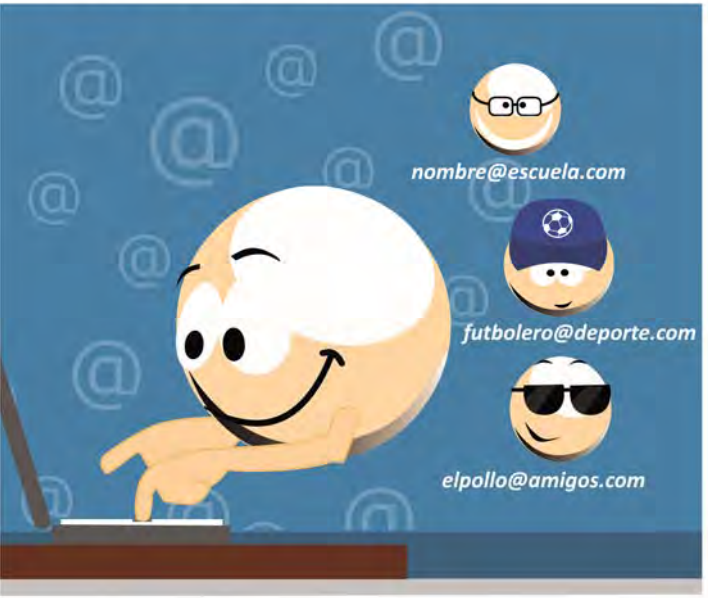
10.- ¿Crees importante que los usuarios de Internet conozcan sobre estas amenazas y las maneras de contrarrestarlas?

- [ ] Si, a todos los usuarios de la red
- [ ] Si, a niños y jóvenes que están aprendiendo el uso de Internet
- [ ] No, la información está al alcance de todos los que estén interesados
- [ ] No, los riesgos no alcanzan a afectarnos si sólo utilizamos internet por diversión

Asegura y cuida tus cuentas

Decide qué información es conveniente publicar y compartir en las redes sociales, así como quiénes pueden acceder a ellas.

Crea varios e-mails



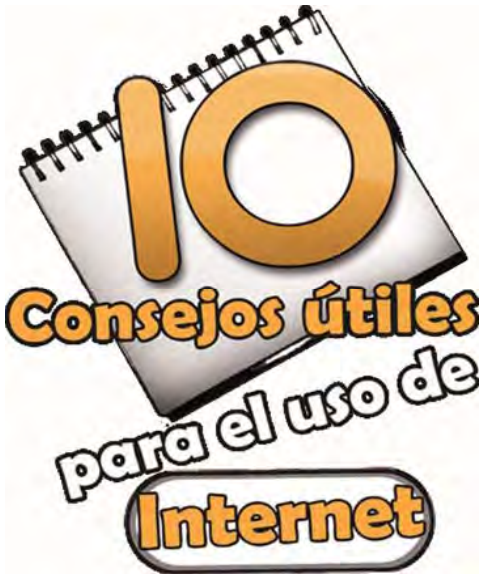
Puedes tener uno para los amigos, otro para juegos y redes sociales, etc.

¡Protege tus datos!

SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

ifai

www.ifai.gob.mx
www.sep.gob.mx
www.datospersonales.sep.gob.mx

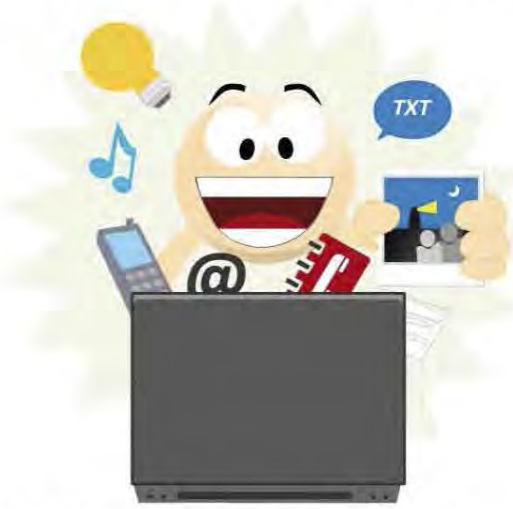


SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

ifai

Vivir Mejor

Piensa antes de publicar



Todo lo que escribas en la red puede permanecer al alcance de otros, aun cuando lo borres: datos, información, ideas, fotografías.

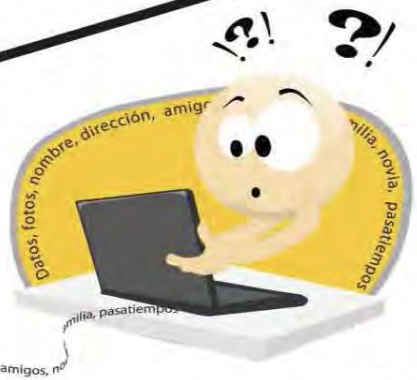
Cuida tu imagen y la de los demás

No subas fotos tuyas o de otros de las que después te puedas arrepentir. Una vez en Internet su difusión es incontrolable. Su publicación puede dañar a alguien.

Respeta a los demás

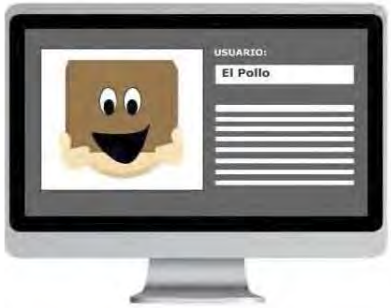
Tú eres responsable de lo que publicas. Cuida las palabras que pones en los foros y redes sociales.

Verifica qué saben de ti



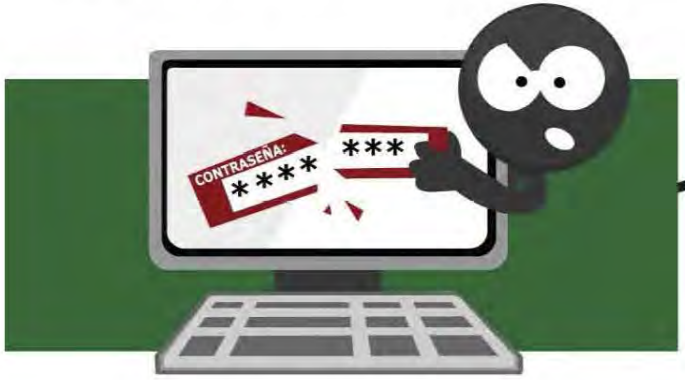
Así te proteges y sólo tus amigos y familiares sabrán que eres tú.

Usa un apodo o alias



Así te proteges y sólo tus amigos y familiares sabrán que eres tú.

Mantén secreta tu contraseña

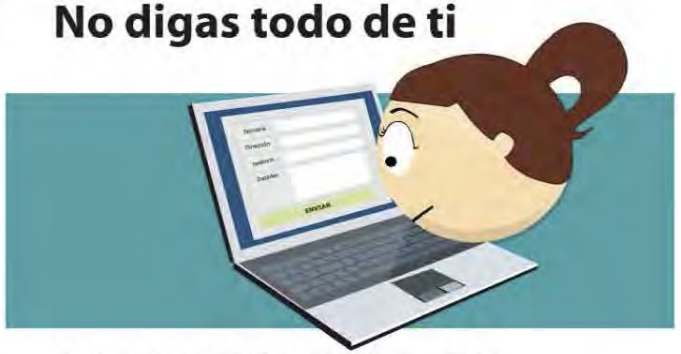


No se la digas a nadie. Inventa una que sea difícil de adivinar, pero fácil de recordar. No utilices tu nombre ni tu fecha de nacimiento.

Cierra tu sesión

Si te conectas en una computadora que no sea la tuya, siempre cierra tu cuenta para que otros no tengan acceso a tu información o se hagan pasar por ti.

No digas todo de ti



Da la mínima información posible.
No te expongas, ni expongas a los tuyos.

RESULTADOS DE LA CAMPAÑA DE CONCIENTIZACIÓN

Las sesiones de esta campaña de concientización se llevaron a cabo con una audiencia de 60 alumnos de diferentes carreras dentro de la universidad, esta sesión estuvo dirigida a alumnos de nuevo ingreso de diferentes carreras que no tuvieran una relación directa con las tecnologías de la información para medir el impacto en aquellos que no están tan familiarizados con la temática de Internet y sus amenazas. En ellas se ilustraron algunos ejemplos y se les proporcionó material adecuado con consejos básicos sobre seguridad y privacidad en Internet, con el fin de medir el impacto y la efectividad de la campaña para la difusión de los problemas y amenazas existentes al hacer un mal uso de las redes sociales. Al final de la sesión, aplicamos el cuestionario ejemplificado en el programa a cada uno de los 60 participantes, obteniendo los siguientes resultados a resaltar:

- El 95 por ciento de los participantes tenían una cuenta de Facebook.
- Solo un 5 por ciento no había escuchado sobre las amenazas en la red.
- Solo el 10 por ciento mencionó que no había sido capaz de configurar la privacidad en sus perfiles en la red y el 25 por ciento de los participantes manifestaron dificultades al tratar de configurar correctamente las medidas de privacidad.
- El 85 por ciento de las personas que asistieron a la conferencia obtuvieron una perspectiva diferente sobre los riesgos y amenazas de Internet después de la plática.

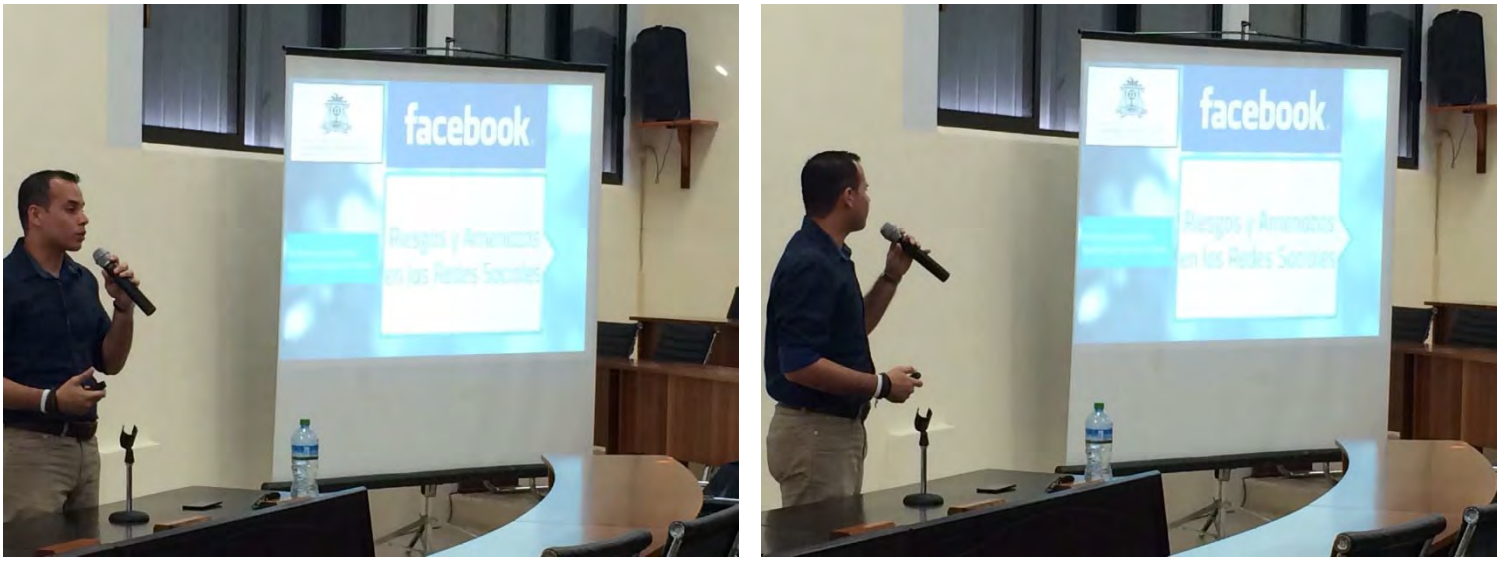


ILUSTRACIÓN 3 SESIONES DE CONCIENTIZACIÓN

Los resultados que obtuvimos fue que los riesgos y amenazas empiezan a ser de conocimiento de los usuarios de Internet, sin embargo, al no conocer el alcance que estos pueden tener, muchos no toman las precauciones necesarias para mantenerse protegido de estas amenazas. La falta de interés y prevención en cuanto al tema, demuestran la falta de la cultura de prevención que en un principio habíamos fijado como parte del aumento de incidentes relacionados con los medios informáticos. Algo positivo fue el

observar que, del total de 60 participantes en las sesiones, 85 por ciento de participantes tuvo una visión diferente de las amenazas en Internet al salir de la sesión, y el 100 por ciento de ellos ahora consideraba como un tema serio la privacidad de los datos y su seguridad en Internet. El presentar ejemplos, como casos de estudio y casos documentados de incidentes reales, ayudó a que los participantes tuvieran cierto grado de empatía con los problemas presentados, al ser tareas que ellos mismos realizan de forma cotidiana, y se observó un aumento en el interés y la percepción de los riesgos que existen.

Capítulo 4

Conclusiones y trabajo futuro

Algunas cosas a resaltar como parte de la implementación de estas sesiones de concientización, fue la facilidad y la disposición que brindó la Universidad para realizar las pláticas. Se nos facilitaron tanto el espacio como el tiempo por parte de administrativos y maestros, el Departamento de Informática también se mostró animado al ver en estas campañas de concientización una herramienta más para ayudar a mejorar la seguridad en la red informática de la universidad. Sin embargo, uno de los problemas que pudieron observarse es la dificultad de coordinación, mencionada por el Departamento de Informática, para poder llevar estos recursos hacia los administrativos y directivos. Por otro lado, también se encuentra la falta de interés y la resistencia al cambio presentados por algunos usuarios, quienes en ocasiones restan importancia a la temática de la seguridad en la red. Aun así, estas campañas de concientización nos dieron la oportunidad de captar la atención de más usuarios al presentar casos reales de problemáticas y algunas medidas de prevención que todo usuario puede aplicar.

Como parte de la investigación, se pudo observar que sí existe legislación actual para regular los riesgos y delitos informáticos en el *Código Penal Federal*, en el *Código penal para el estado libre y soberano de Quintana Roo*, y en la *Ley federal de protección de datos personales en posesión de particulares*. A pesar de esto, las problemáticas que se abordan en estas leyes no quedan del todo claras o son insuficientes, haciendo necesarias algunas reformas que permitan una mejor regulación y prevención de estos delitos. Esto llevó a algunas dificultades dentro de la investigación, sobre todo a nivel estadístico, debido a que algunos delitos informáticos, al no encontrarse aún tipificados como tal, no se lleva de ellos un control preciso en cuanto a incidencia e impacto en la sociedad. En muchos de los casos, estas acciones criminales ni si quiera son denunciadas, lo que hace aún más difícil contar con cifras exactas de la circunstancia actual en México.

También se observó que el conocimiento en cuanto a estas leyes por parte de los usuarios de la red informática universitaria es casi nulo, por lo que una buena práctica sería el difundir los aspectos legales que nos protegen ante tales situaciones, como parte fundamental de crear una correcta cultura informática en los usuarios. Estas acciones permitirán al usuario el entender la manera en como la ley le protege, y también el limitar las acciones que él mismo pueda tomar a fin de evitar la comisión de algún delito.

Existirán muchas maneras y medios que estén a nuestro alcance al desarrollar estas campañas para la capacitación y concientización de los usuarios, que es una de las mayores necesidades a solventar en la Universidad. Se propone que uno de los primeros acercamientos dentro de un programa de seguridad en la Universidad sea a través de las campañas de concientización. Se ha podido comprobar, a través de las sesiones realizadas, que es un medio eficaz para difundir las diferentes amenazas y las principales medidas de seguridad para tomar en cuenta a fin de mejorar la seguridad de los usuarios. Debido a que estas sesiones no requieren de un presupuesto elevado y son flexibles en cuanto a su contenido, se podrán desarrollar de manera ágil para su pronta implementación. No será necesario contar con expertos o especialistas en la materia, estos temas deben ser de dominio para los alumnos del programa de Ingeniería en Redes de la misma universidad, y pueden tomarse como proyectos de investigación y servicio social para el desarrollo e implementación de las campañas, o como parte de las acciones que

lleva a cabo la Dirección de Informática de la Universidad en sus esfuerzos por reforzar la seguridad y el buen funcionamiento de la red informática. Será importante no sólo proporcionar la información con respecto a los temas, sino también hacer un llamado e invitación a la acción a todo usuario de la red informática universitaria.

Se pretende que esta iniciativa no esté dirigida únicamente a los alumnos, sino también se busca incluir en ella a docentes y administrativos, y anexar algunos temas a desarrollar como el uso adecuado de los servicios de Internet de la universidad, el uso adecuado del nuevo sistema de correo, y prácticas comunes de seguridad en línea para una navegación segura, así como otras necesidades que puedan detectarse con el paso del tiempo; esto con el objetivo de establecer una serie de acciones que permita tener un programa fijo de capacitación y concientización, que sea capaz de ajustarse a las necesidades de la universidad y de las demandas de las nuevas tecnologías emergentes.

El conocimiento de las diferentes amenazas y de lo que pueden implicar en nuestra vida, permite a los usuarios visualizar la gravedad del problema. El brindar las herramientas necesarias, como lo son el conocimiento sobre las diferentes prácticas de riesgo y las técnicas para evitarlas, les permitirá tomar acciones que se convertirán en algo habitual al momento de utilizar estos medios de comunicación. También, el conocimiento sobre las implicaciones legales y las acciones que pueden tomar al encontrarse ante situaciones riesgosas en Internet, brindará a los usuarios la seguridad necesaria para hacer valer la ley y proteger su integridad física y emocional. Como podemos observar, una adecuada cultura informática es parte esencial para que los usuarios de las nuevas tecnologías de la información, en especial los futuros egresados de la universidad, estén preparados para hacer frente a este nuevo mundo digital e interactuar de manera segura con las nuevas tecnologías de la información.

Este es sólo el inicio para ayudarnos a tomar conciencia del cambio que podemos llegar a generar si le damos a la seguridad de la información la importancia que se merece. Este tipo de programas e iniciativas podrán aplicarse a cualquier institución que esté interesada en mejorar la seguridad y el uso eficiente de las nuevas tecnologías de la información, ya sea empresas, instituciones educativas, o dependencias de gobierno, todos tomamos parte en la seguridad. En especial, si llevamos esto a aquellos que se encuentran en su formación y educación más temprana, lograremos cambiar la perspectiva y la cultura de la prevención que muchos tienen y lograr hacer de nuestra red un lugar más seguro.

En este tiempo donde la información está al alcance de todos, y en donde todos tenemos una identidad digital en la red, debemos tomar la iniciativa y buscar crear en nosotros mismos y en las personas que nos rodean esta cultura informática, estar conscientes que nuestras acciones en la red pueden ser tan importantes como en nuestra vida real.

Bibliografía

National Institute of Standards and Technology NIST 800-50 ‘‘Building an Information Technology Security Awareness and Training Program’’ (Cómo construir una campaña de conciencia y entrenamiento para la cultura de seguridad); http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) ‘‘Manual de Seguridad para Instituciones de Educación Superior: estrategias para la prevención y atención (2011)’’; http://www.sep.gob.mx/work/appsite/anuies/manual_de_seguridad_anuies.pdf

ANUIES. (18 de Abril de 2013). *Misión, Visión y Objetivos Estratégicos*. Obtenido de http://www.anuies.mx/content.php?varSectionID=3

Asociación Nacional de Universidades e Instituciones de Educación Superior. (15 de Enero de 2014). *ANUIES otorgó 110 mil pesos a "Universidad Segura" de la UdeG*. Obtenido de Últimas Noticias: http://www.anuies.mx/content.php?varSectionID=163&varIDNoticia=1649

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (Agosto de 2009). Fraude Electrónico. Distrito Federal, México.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (Febrero de 2009). Seguridad en los Sitios de Redes Sociales. Distrito Federal, México.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2 de Febrero de 2009). *Seguridad en los Sitios de Redes Sociales*. Obtenido de http://revista.seguridad.unam.mx/numero-0/seguridad-en-los-sitios-de-redes-sociales

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (30 de Julio de 2011). Geoetiquetación: Los riesgos de hacer pública tu ubicación. Mexico, Mexico.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (Junio de 2012). El poder de proteger tu información. Distrito Federal, México.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (05 de 06 de 2012). Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I. Mexico.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (Marzo de 2012). Riesgo tecnológico y su impacto para las organizaciones parte I. Distrito Federal, México.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (1 de Abril de 2014). *Hablando correctamente de seguridad de la información*. Obtenido de REVISTA .SEGURIDAD, DEFENSA DIGITAL: http://revista.seguridad.unam.mx/numero-20/hablando-correctamente-de-seguridad-de-la-informaci%C3%B3n

El Economista. (27 de Enero de 2014). *México, entre los 10 primeros lugares en robo de identidad*. Obtenido de El Economista: http://eleconomista.com.mx/sociedad/2014/01/27/mexico-entre-10-primeros-lugares-robo-identidad

El País. (13 de Septiembre de 2014). *Apple tropieza con la nube*. Obtenido de http://elpais.com/elpais/2014/09/06/opinion/1410020167_633827.html

El Universal. (25 de Abril de 2013). *Alerta SSPDF de virus que usa imagen de Policía Federal*. Obtenido de http://www.eluniversal.com.mx/notas/919171.html

ESET. (2014). *Glosario: We Live Security En Español*. Obtenido de http://www.welivesecurity.com/la-es/glosario/

Hernández Santana, M. A. (Noviembre de 2004). Los delitos a través del uso de la computadora. San Luis Potosí, México.

Kaspersky Lab. (2014). *¿Qué es un código malicioso?* Obtenido de http://latam.kaspersky.com/mx/internet-security-center/definitions/malicious-code

Kaspersky Lab. (2014). *¿Que es un troyano?* Obtenido de http://www.kaspersky.es/internet-security-center/threats/trojans

Lima, M. d. (1984). *Delitos Electronicos.* Mexico: Editorial Porrua.

Milenio. (12 de Agosto de 2013). *Robo de identidad, un delito sin estadísticas*. Obtenido de Milenio.com: http://www.milenio.com/monterrey/Robo-identidad-delito-estadisticas_0_133786917.html

Noticieros Televisa. (14 de Febrero de 2013). Fraudes por robo de identidad. Mexico, Mexico.

Oficina de Seguridad del Internauta. (s.f.). Privacidad. España.

PantallasAmigas. (Diciembre de 2010). *Cinco consejos básicos para un uso seguro de la webcam*. Obtenido de http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/cinco-consejos-basicos-para-un-uso-seguro-de-la-webcam.shtm

PantallasAmigas. (17 de Octubre de 2012). *Amanda Todd, caso dramático de sextorsión y ciberbullying analizado por PantallasAmigas*. Obtenido de Ciberbullying: Ciberacoso escolar entre menores: http://www.ciberbullying.com/cyberbullying/2012/10/17/el-video-con-el-que-amanda-todd-luchaba-contra-el-ciberbullying-subtitulado-al-espanol-por-pantallasamigas/

PantallasAmigas. (28 de Noviembre de 2014). *Siete jóvenes detenidos por difundir imágenes de sexting de una menor ¿Conoces los riesgos?* Obtenido de BLOG DE PANTALLASAMIGAS: http://blog.pantallasamigas.net/2014/11/siete-jovenes-detenidos-por-difundir-imagenes-de-sexting-de-una-menor-conoces-los-riesgos/

Pereznieto y Castro, L., & Ledesma Mondragón, A. (1989). *Introducción al estudio de Derecho* (Segunda edición ed.). Editorial Harla.

PGJE. (2014). TRÍPTICOS INFORMÁTIVOS: Dirección de Prevención del Delito. (P. G.-A. 2016, Ed.) Chetumal, Quintana Roo, Mexico.

UNAM - CERT. (2009). *Usuario Casero: Phishing Scam*. Obtenido de http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=166

Universidad de Quintana Roo. (2012). *Identidad Universitaria*. Obtenido de Nuestro Quehacer: http://www.uqroo.mx/nuestra-universidad/identidad-universitaria/nuestro-quehacer/

Vargas, J. L. (Abril de 2002). La configuración del Derecho Penal dentro del modelo de Estado social y democrático de Derecho. Costa Rica.

Verizon. (s.f.). Obtenido de 2014 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2014/