UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

BUENAS PRÁCTICAS PARA MINIMIZAR LA PRINCIPAL AMENAZA EN SEGURIDAD INFORMÁTICA: EL USUARIO

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERA EN COMPUTACIÓN

PRESENTA:

MARÍA FERNANDA BRISEÑO DÍAZ

ASESORA: M.C CINTIA QUEZADA REYES

Ciudad Universitaria, 2012

Agradecimientos

A mi padre, que siempre ha sido muestra de fortaleza y mi ejemplo a seguir. Le agradezco inmensamente todo el amor, cariño, confianza y apoyo brindado a lo largo de mi carrera y sobre todo a lo largo de mi vida. Gracias a él soy la persona que ahora soy.

A mi madre, que se ha convertido en mi mejor amiga y confidente. Agradezco su fortaleza, su amor, sus consejos, apoyo incondicional y estar presente siempre que la necesito.

A Emilio Briseño, por sus cuidados, apoyos, consejos y ser una persona que siempre me valora como nadie y quiere lo mejor para mí.

A Jimena Briseño, por estar conmigo en las buenas y en las malas.

A Gloria Castillo y Leticia Briseño, por la confianza depositada en mí, y por todo su apoyo para cumplir mi sueño de ser profesionista.

A Omar Reyes, por lo difícil que es encontrar a alguien como él. Por aceptarme como soy y por todos los momentos compartidos. Él me demostró que sí existen las relaciones basadas en la confianza. Le agradezco su amistad y no dejar que esto termine.

A Emmanuel Cuevas, Angélica Cervantes, Daniel Díaz y Jonathan Banfi, por convertirse en mi familia a lo largo de la carrera. Por todos los momentos compartidos, por haber creado el lazo tan fuerte que ahora tenemos.

A Norma Vázquez, Isabel Méndez, y Thalía Ocampo, por su amistad incondicional, por todo su apoyo y estar ahí siempre que las necesito.

A Mayra Briseño, por ser mi compañera de batalla a lo largo de la carrera.

A Patricia Cayetano, por enseñarme que las amistades no terminan al finalizar una carrera. Gracias por todo tu apoyo y cariño.

A Cintia Quezada, por su asesoría en la elaboración de este trabajo, por todo su apoyo y consejos. Sin ella no hubiera sido posible este trabajo. Gracias por su tiempo.

A toda mi familia por su apoyo y confianza.

A todos mis maestros, los cuales contribuyeron en mi formación profesional.

ÍNDICE

Introducción

Como es sabido, el avance de la tecnología hoy en día se encuentra en crecimiento constante. Debido a la necesidad del hombre de facilitar su trabajo y de automatizar sus actividades, y gracias a dicho avance tecnológico, se ha dado a la tarea de hacer uso de los equipos de cómputo en la realización de sus actividades, con la finalidad de poderlas realizar con mayor rapidez. Por esta razón es que actualmente los sistemas informáticos están presentes en prácticamente todos los ámbitos de la vida del ser humano, desde el ámbito educativo y el hogar, hasta el laboral y de investigación.

Cuando una persona comienza a hacer uso de este tipo de equipos, en automático se convierte en un usuario del sistema. Es muy común que cuando un usuario utiliza un sistema, se enfoque únicamente en conocer el funcionamiento del mismo, y a saber cómo debe usar el equipo para poder realizar las labores requeridas. Sin embargo lo que la mayoría no conoce, es que dichos equipos requieren de un mantenimiento y de una serie de protecciones para lograr su buen funcionamiento. El conjunto de las protecciones más importantes que requieren las computadoras se relacionan con la seguridad informática.

Al ser un sistema, una herramienta útil para una persona u organización, es un bien que posee cierta importancia y por lo tanto es necesario resguardarlo de todo aquello que pueda causarle algún daño. La seguridad informática se encarga de brindar todas esa protecciones que requieren los sistemas para permanecer en estado óptimo, al mismo tiempo que mantiene la información segura y confidencial, limitando el acceso a la misma, únicamente a quienes posean los permisos necesarios para acceder a ella.

Normalmente cuando se habla de seguridad informática, se piensa inmediatamente en proteger a los equipos y sistemas de agentes externos que puedan dañarlos. Sin embargo se ha dejado de lado, que quienes tienen mayor contacto con dichos equipos y por lo tanto tienen mayor oportunidad de dañarlos, son los propios usuarios, convirtiéndose así en la principal amenaza para sus equipos.

El tema de esta tesis, Buenas prácticas para minimizar la principal amenaza en seguridad informática: El usuario, aborda las razones por las cuales es necesario que los usuarios comiencen a verse a sí mismos como una amenaza ante sus equipos y realicen lo necesario para que esto no sea un problema para los sistemas. En el siguiente trabajo se realiza una investigación mediante la cual se respalda la hipótesis del mismo, a la vez que se brinda una posible solución a dicho problema con la finalidad de que los equipos de cómputo posean menores riesgos y puedan tener mejor funcionamiento y rendimiento.

A la par de la realización de este trabajo, se implementó una aplicación web mediante la cual los usuarios podrán obtener la información básica para mantener protegidos sus equipos, aprendiendo de ésta qué es lo que puede dañar a sus bienes y cuáles son las formas de protegerse de dichos daños.

En este trabajo se presenta una serie de conceptos e información considerada como básica para tener una idea de lo que significa la seguridad informática, lo que ésta involucra, así como su importancia en cualquier equipo de cómputo, ya sea una computadora personal o un conjunto de servidores o equipos mayores, ya que como se verá en las próximas páginas, no importa que tan grande o pequeño sea el equipo que se posea, finalmente debe tener un mantenimiento y una seguridad adecuada.

De este modo, en el capítulo 1 se tratarán los aspectos básicos de la seguridad informática y conceptos indispensables para el entendimiento de la misma. Esto permitirá que quien lea este trabajo se pueda familiarizar con el tema de la tesis, y pueda darse una idea de todo lo que la seguridad involucra.

En el capítulo 2 se realizará una introducción a las políticas de seguridad, ya que el tema principal de esta tesis tiene que ver con buenas prácticas, y éstas a su vez van directamente relacionadas con lo que son las políticas. Así, cuando el lector llegue al capítulo final y a la vez objetivo de este trabajo, ya sabrá de qué se habla en el mismo.

Posteriormente en el capítulo 3 se abordarán los principales problemas informáticos actuales, esto es con el objetivo de visualizar la problemática involucrada con la seguridad de la información, ya que muchas veces se habla del tema pero no se posee una visión de cuáles son exactamente los riesgos que corre un equipo de cómputo, o de qué manera puede ser dañado un sistema. Por lo tanto al aterrizar un poco el tema en casos reales, actuales y más comunes, el lector visualizará de mejor manera el concepto de seguridad y la importancia de la misma.

Continuando con este trabajo, en el capítulo 4 se tratará el tema de esta tesis: Usuarios, principal amenaza en seguridad informática, en el cual se plasmarán las razones por las cuales se está considerando dicha hipótesis, en base a lo estudiado en los capítulos anteriores y a la investigación realizada.

Finalmente en base a lo obtenido en el capítulo anterior, en la parte final de este trabajo se realizará una serie de buenas prácticas para el uso adecuado de los equipos de computo, de este modo el usuario sabrá de qué manera puede proteger adecuadamente sus equipos y así podrá mantenerlos en un estado ideal y óptimo.

Adicionalmente en el capítulo 5 se incluye a grandes rasgos el contenido del sitio web elaborado, haciendo referencia a éste, como un medio por el cual se promueve una cultura en seguridad informática, brindando a través de éste la difusión del tema. La información contenida en dicho sitio está basada en el trabajo presentado en esta tesis.

Capítulo 1: Seguridad Informática

1.1 Seguridad

La seguridad en un ámbito global, se refiere a todos aquellos mecanismos y medidas que permiten resguardar un bien.
Cualquier objeto que posea un valor para una persona u organización, se convierte en un bien ya que es importante para alguien y por lo tanto desea protegerlo de todo aquello que pueda dañarlo.

En el ámbito informático, el concepto es similar, únicamente se traslada a lo que son las tecnologías de la información. De este modo, la seguridad informática se encarga de brindar las protecciones necesarias para resguardar los bienes informáticos. Esto es, la información, el hardware, software y comunicaciones o redes.

La seguridad informática se refiere a todas aquellas medidas que se toman para impedir que se lleven a cabo actividades no autorizadas en un dispositivo o sistema informático, y que puedan causar algún daño en la información o en los equipos. Con la implementación de dicha seguridad, se busca impedir que se comprometa la confidencialidad, integridad o autenticidad de la información, y evitar que disminuya el rendimiento de los equipos.

El objetivo principal de la seguridad informática es preservar la confidencialidad, integridad y disponibilidad de los bienes informáticos, de no lograrse esto, se puede incluso llegar a afectar la vida privada de las personas. Es por ello que se debe crear conciencia de la importancia que tiene la seguridad informática, ya que básicamente la seguridad logra reducir las amenazas y vulnerabilidades de los bienes.

Cuando se habla de seguridad informática, lo primero que se debe hacer es preguntarse ¿qué se quiere proteger?, ¿de qué se quiere proteger?, y ¿cómo

se va a proteger? Estas tres preguntas deben hacerse en este orden para obtener el resultado esperado, ya que no se puede primero resolver la segunda o tercer pregunta sin saber primero qué es lo que se desea proteger.

a) ¿Qué se quiere proteger?

Se inicia con la primera pregunta, la cual básicamente sirve para identificar cuáles son los bienes que cada persona u organización posee, y que por lo tanto desea proteger, a estos recursos se les llama entorno de seguridad. En esta parte se visualiza en concreto qué es lo que tiene valor para alguien, o qué desean resguardar. Puede ser un equipo de cómputo, refiriéndose a únicamente la PC; el software, sistema operativo, todo un cuarto de telecomunicaciones, o un edificio completo. Dicho análisis se debe llevar a cabo no solo por una persona sino por un conjunto de personas, para tener una visión más amplia de los activos que se poseen y que en caso de estar en riesgo puedan provocar daños a alguien.

a) ¿De qué se quiere proteger?

Una vez que se tiene identificado lo que se va a proteger, se debe definir de qué se quiere proteger, para saber posteriormente cuáles serán las medidas y mecanismos necesarios para lograr el objetivo inicial. Aquí se hace un análisis acerca de qué es lo que puede dañar los bienes, si son agentes externos o internos, software malicioso, personas no autorizadas, y todo aquello que en un momento dado, podría ser dañino para los bienes. Esto es, se debe identificar todas las amenazas y vulnerabilidades de los activos, así como los riesgos que éstos poseen, y a lo que esté expuesto el entorno de seguridad.
En esta parte se define si solo se desea que personal autorizado tenga acceso a un edificio o área de la organización, o inclusive a un equipo, si es necesario tener disponible la información siempre que alguien la requiera,

etcétera. La protección de los bienes es responsabilidad de los dueños, responsables o encargados de los mismos, ya que son quienes valoran los activos y por lo tanto pueden definir la protección que le quieren dar. Estas personas pueden, con ayuda de un especialista en seguridad informática, analizar todo lo que sea capaz de aprovecharse de dichos bienes y por lo tanto los afecte de alguna manera. Con este análisis ya se puede partir para determinar cuáles serán las medidas que se tomarán para contrarrestar todos los riesgos.

a) ¿Cómo se va a proteger?

Ya que se tienen definidos los dos puntos anteriores, se pueden determinar en base en ello, las políticas de seguridad que se implementarán al entorno analizado, ya que éstas estarán orientadas a combatir los riesgos detectados y ayudarán a proteger todos los activos.

Este punto permite definir cuáles serán los mecanismos que se implementarán para lograr el objetivo deseado, que es resguardar bienes, de amenazas, vulnerabilidades y riesgos específicos, logrando así, minimizarlos y en lo posible eliminarlos, haciendo que los activos se conviertan en bienes seguros.

1.2 Amenazas

Como se puede observar, al hablar de seguridad informática se habla también de varios conceptos involucrados, uno de éstos son las amenazas.
Una amenaza es todo aquello que puede causarle algún daño a un activo, es algo que está latente y que tiene alguna oportunidad de manifestarse; es todo aquello que puede, intenta o pretende destruir o dañar un bien. Una amenaza puede o no presentarse.

Una amenaza se representa por medio de una persona, evento, circunstancia o idea maliciosa, que pueda provocar un daño en caso de que se viole la seguridad, y pueden provenir de diferentes fuentes. Con base en esto, existen 5 tipos de amenazas:

a) De humanos

Se refiere a aquellas amenazas que surgen debido al mal manejo de la información por parte de las personas, ignorancia o descuido. Abarca todo aquello que tenga que ver con acciones humanas, es decir, falta de conocimientos por parte de los usuarios para manejar los equipos, descuido de la información, daños provocados por todo tipo de atacantes, curiosos, terroristas, etcétera.

b) De hardware

Son todas aquellas fallas físicas que puedan sufrir los equipos y dispositivos. Problemas en el suministro de energía, variación de voltaje, bajo rendimiento, deterioro de los equipos o desperfectos en los mismos, sobrecalentamientos, defectos de fábrica, son solo algunos de las amenazas que están en esta clasificación.

c) De red

Son aquellas amenazas que tienen que ver con la red y que podrían presentarse, por ejemplo congestionamiento o tráfico en la red, falla en la disponibilidad de la red, desconexión del canal; monitorización, virus por correo electrónico, denegación de servicios, etcétera, son algunas de las más comunes.

d) De software

Son las amenazas que tienen que ver con problemas lógicos en los sistemas, es decir que el software falle o no funciones correctamente, que exista código malicioso en los equipos, intrusión de virus o gusanos, etcétera.

e) Desastres naturales

Son las amenazas que menos se puede combatir debido a que no se sabe cuándo sucederán ni de qué manera podrían suceder, sin embargo se deben siempre de considerar para estar prevenidos. Incendios, sismos, inundaciones, etcétera, son solo algunos de los desastres que podrían suceder.

Otra clasificación que se le puede dar a las amenazas es si son externas o internas. Como su nombre lo dice, las externas son todas aquellas que provienen de agentes foráneos a la organización o lugar donde se encuentran los activos. Así mismo las internas son aquellas producidas en el interior de la organización. Ejemplos de amenazas externas son los virus y gusanos que provienen de la red; como ejemplo de amenazas internas están los propios usuarios de los equipos que por algún descuido provoquen un daño en los activos.

1.3 Vulnerabilidades

Otro concepto muy utilizado en seguridad informática son las vulnerabilidades.

Una vulnerabilidad es todo aquello que no ha sido considerado en la protección de los activos, son las debilidades que tienen los bienes y que pueden ser explotadas por una amenaza. Es un punto débil y que puede ser atacado o puede provocar daños en la seguridad de los bienes. Es todo lo que no se ha implementado y que puede causarle algún daño a los activos al ser aprovechado por una amenaza.

Una amenaza puede explotar una o varias vulnerabilidades, así mismo una vulnerabilidad puede ser explotada por una o varias amenazas. Las vulnerabilidades son muy variadas e igualmente pueden clasificarse de acuerdo con su origen en:

a) Física

Se refiere a las debilidades que pueda tener el entorno físico en el que se encuentran los activos, por ejemplo el control de acceso físico al sistema. Básicamente se relaciona con la posibilidad de acceder al lugar para causar algún daño en el mismo.

b) Natural

Son las vulnerabilidades que tienen que ver con que el sistema pueda ser dañado en caso de que ocurra algún desastre natural o ambiental. Ejemplos de estas vulnerabilidades son que no se cuente con salidas de emergencia, no tener techos o paredes impermeables, que el centro de cómputo no esté ubicado en una zona climatológicamente adecuada, etcétera.

c) De hardware

Al igual que las amenazas, las vulnerabilidades de hardware tienen que ver son los dispositivos y equipos. En este caso son consideraciones no tomadas en cuenta para el buen funcionamiento de los mismos, por ejemplo no darle mantenimiento constante al hardware, no verificar que el equipo que se compra cuente con los requerimientos necesarios, entre otros.

d) De software

Las fallas en los sistemas o debilidades en los programas instalados son ejemplos de este tipo de vulnerabilidades. Como su nombre lo dice, se refiere a aquellas relacionadas con el software como errores de programación, o que los protocolos de comunicación carezcan de seguridad.

e) De red

Son todas aquellas vulnerabilidades existentes en la conexión de equipos, por ejemplo si no existe un control que permita limitar el acceso, se puede penetrar al sistema por medio de la red. También abarca las fallas en la estructura del cableado y el no seguir los estándares recomendados para realizarlo.

f) Humana

Del mismo modo que las amenazas humanas, las vulnerabilidades tienen que ver con las acciones de las personas, por ejemplo ser vulnerable a la ingeniería social, no capacitar al personal como se debe, colocar contraseñas en lugares visibles, no contar con guardias de seguridad, no

tener detectores de metales, no eliminar cuentas de acceso de ex empleados, etcétera.

Como puede apreciarse, es muy importante la identificación de las amenazas, logrando así que no estén presentes en lo posible; sin embargo también es de suma importancia identificar las vulnerabilidades, ya que aunque se identifiquen muchas amenazas, siempre queda alguna vulnerabilidad que de ser explotada provoque un ataque en los sistemas. De este modo puede visualizarse que las amenazas van de la mano con las vulnerabilidades, ya que cuando una amenaza se aprovecha de una vulnerabilidad dan como resultado un ataque.

1.4 Ataques

Como ya se mencionó, la existencia de amenazas y vulnerabilidades pueden ocasionar un ataque. Un ataque es el primer aspecto que se considera en la seguridad. Es la culminación de una amenaza, esto ocurre cuando dicha amenaza se aprovecha de una o varias vulnerabilidades que existan en un sistema. En otras palabras, un ataque es cuando ocurre la acción que causa algún daño a los activos.

Los ataques a los centros de cómputo o sistemas informáticos constan de 3 etapas que son: preparación, activación y ejecución.

a) Preparación o planteamiento

En la primera etapa lo que se hace es preparar el ataque, se planea la forma en que se llevará a cabo. Se adquiere información, se observan las posibles vulnerabilidades, los horarios viables para llevarse a cabo, se

elige una estrategia, se plantean los objetivos, se calculan tiempos etcétera.

b) Activación

Posteriormente en la etapa de activación, el ataque se activa o dispara[1]. Esto es, se llevan a cabo las acciones necesarias para que pueda realizarse el ataque.

c) Ejecución

Finalmente en la ejecución se logra el objetivo principal, que es provocar algún daño a cierto activo de cierta manera, es decir son las consecuencias del ataque.

1.4.1 Clasificación de los ataques

Los ataques pueden clasificarse con base en el lugar de su realización, es decir, pueden ser internos o externos. Al igual que las amenazas, un ataque externo es aquel que tiene su origen en algún lugar fuera de la organización, provienen de agentes externos; así mismo el interno es aquél que se origina dentro de la propia organización, por lo que regularmente son ocasionados por el propio personal o los mismos usuarios.

[1] María Jaquelina López Barrientos, Fundamentos de seguridad Informática, 1ª. Edición, UNAM Facultad de Ingeniería, México D.F, 2006, p.107.

Por otra parte existe otra clasificación de los ataques, la cual se basa en el tipo de daño que se causa a los bienes. Bajo esta naturaleza, los ataques pueden ser activos o pasivos. Los pasivos son aquellos que no provocan una modificación, alteración o daño físico a los bienes, sino que únicamente se dedican a observar, escuchar o monitorear los lugares donde se encuentran los bienes o los mismos bienes. Debido a esto es muy común que los propietarios de dichos activos no se percaten de que han sufrido un ataque.

Contrariamente, un ataque activo es aquél que sí provoca una alteración o daño físico a los dispositivos, equipos, información o lugares en donde se encuentran los bienes, por lo tanto los dueños o encargados de ellos, pueden darse cuenta de que han sido víctimas de un ataque.

De acuerdo con el objetivo que se busca al llevar a cabo el ataque, se pueden clasificar en:

a) Intercepción

Ocurre cuando una entidad no autorizada logra acceder a un equipo, información o cualquier bien, por lo que se atenta contra la confidencialidad (Figura 1.1).

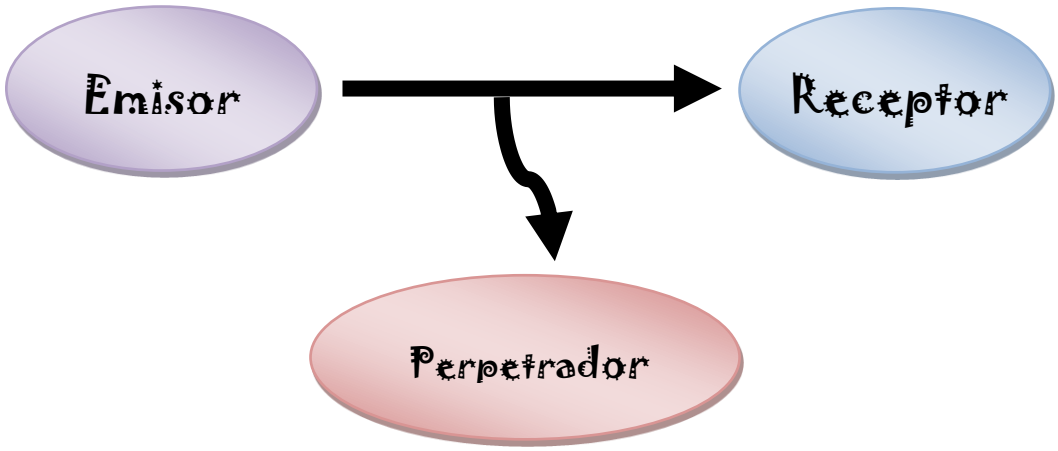


Figura 1.1 Ataque de intercepción

b) Modificación

Son aquellos ataques en los que se logra eliminar o ingresar información, cambiar configuraciones de los equipos, o realizar cualquier acción que cambie el estado inicial de los activos. Se atenta contra la integridad (Figura 1.2).

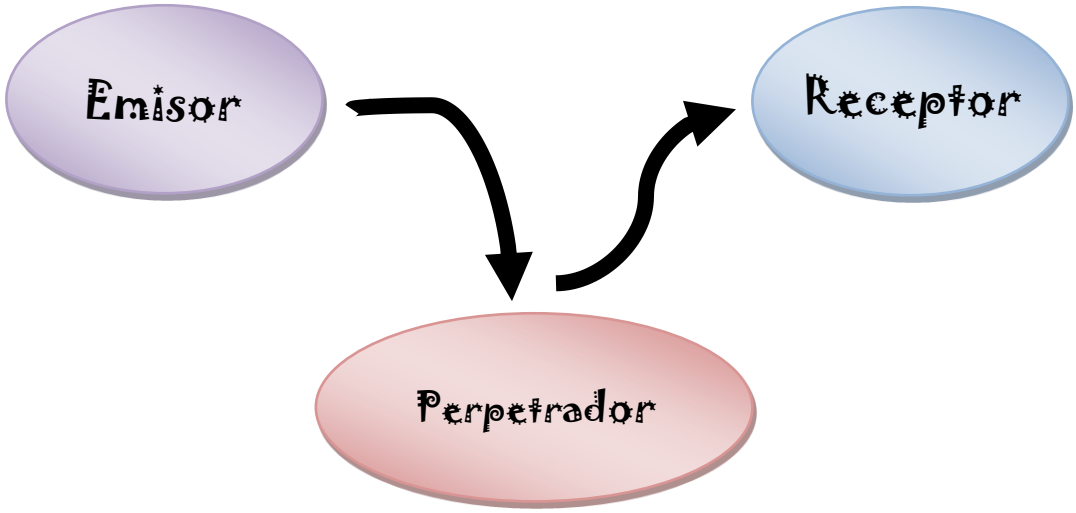


Figura 1.2 Ataque de modificación

c) Interrupción

Se refiere a cuando se logra una denegación de un servicio o sistema, por lo que atenta contra la disponibilidad del bien (Figura 1.3).

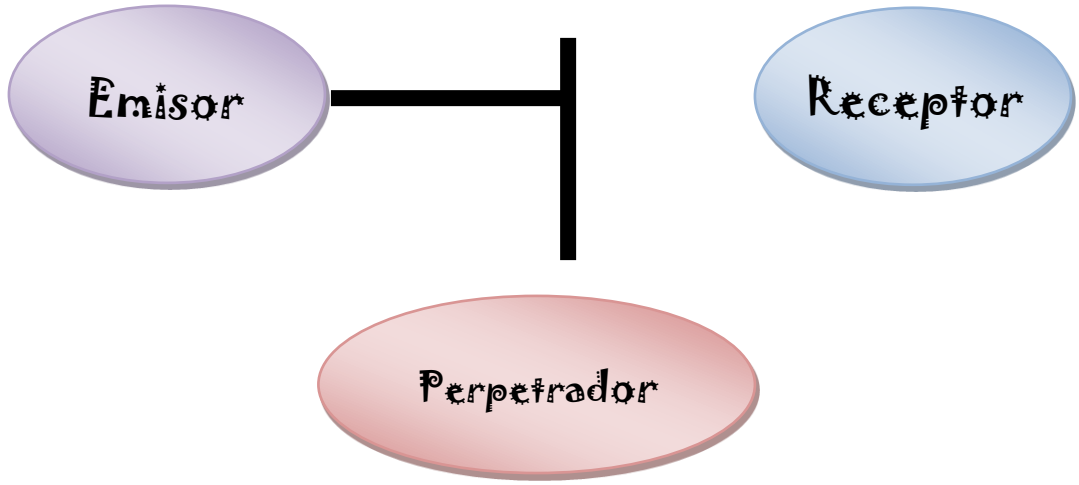


Figura 1.3 Ataque de interrupción

d) Suplantación o falsificación

Son todos aquellos ataques en los cuales se logra usurpar la identidad de una persona u objeto, es decir no sólo se refiere a que alguien pueda acceder al bien bajo el nombre de alguien más, sino también al hecho de ingresar objetos falsificados. Se atenta en contra de la autenticidad de los activos (Figura 1.4).

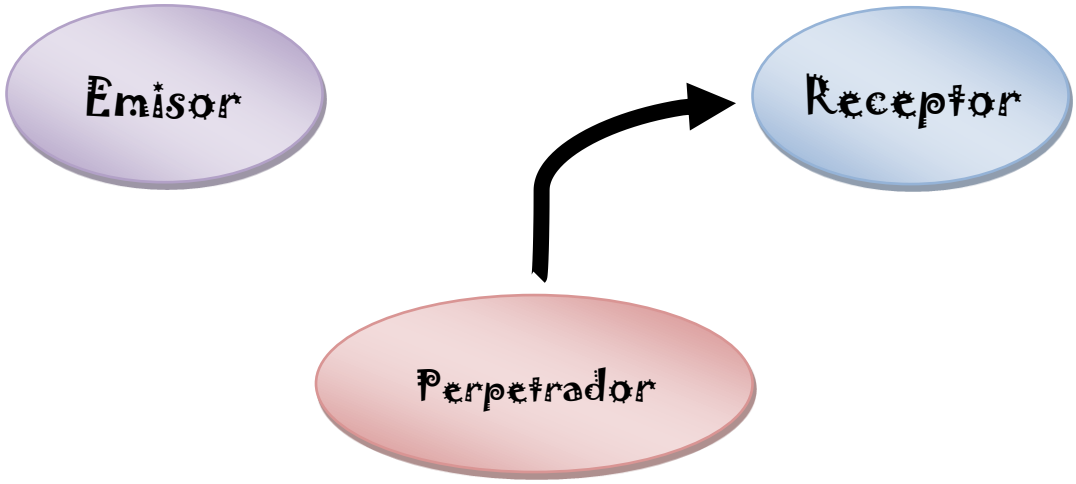


Figura 1.4 Ataque de suplantación

Finalmente aquellas personas o procesos que se encargan de llevar a cabo cualquier tipo de ataque, son los llamados atacantes o perpetradores. Dichas entidades tienen el objetivo de dañar de alguna forma a los activos, y estos atacantes pueden ser internos (insiders) o externos (outsiders). Del mismo modo que los ataques, los atacantes son internos o externos de acuerdo con el origen que tenga su ataque, ya sea dentro de la organización o fuera de la misma.

1.5 Servicios de seguridad

El segundo aspecto que se considera en la seguridad son los servicios de seguridad, que son aquellos que tienen como finalidad mejorar la seguridad de un equipo o sistema informático, así como el flujo de la información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio[2].

Los servicios de seguridad se clasifican en seis, los cuales son:

1. Autenticación

   Consiste en verificar la identidad de algo o alguien, probando que se es quien se dice ser. Este servicio de seguridad lo que busca es que la comunicación sea auténtica y no exista usurpación o suplantación por parte de alguna entidad. De este modo se asegura que información valiosa o un bien en general no sea interferido por un perpetrador, evitando así, transmisiones y usos no autorizados de los activos.

[2] María Jaquelina López Barrientos, Fundamentos de seguridad Informática, 1ª. Edición, UNAM Facultad de Ingeniería, México D.F, 2006, p.117.

Para poder llevarse a cabo la autenticación de una manera correcta, se realiza por medio de:

- Algo que se sabe. Puede ser una contraseña o algún número de identificación, el cual al ingresarlo al sistema, éste puede corroborar que es auténtico.

- Algo que se tiene. Algún objeto que se posee y que sirve para probar que se es quién se dice ser, por ejemplo la credencial de elector.

- Algo que se es. Se refiere a algún aspecto que forma parte de la entidad del ser humano, que lo hace irrepetible, por ejemplo la huella digital o la retina del ojo.

2. Confidencialidad

Se trata de lograr que personas no autorizadas no tengan acceso a los bienes e información, es decir que éstos únicamente puedan ser vistos por aquellas personas que tengan permisos, para poder evitar que dicha información sea utilizada con fines diferentes y peor aún con fines malignos para los dueños o encargados de dichos activos. Regularmente para poder lograr esto, se recurre a resguardar los bienes bajo llave o algún control de acceso.

El objetivo primordial de la confidencialidad es poseer privacidad, y el control de dicha confidencialidad depende de qué tan importantes es el activo y qué tanto se quiere proteger.

La autenticación y la autorización son una manera de preservar la confidencialidad, ya que siempre existirán perpetradores que deseen acceder a algún bien y sin la autorización y autenticación indicada, les será muy difícil poder acceder a dichos bienes.

Este servicio de seguridad, brinda protección a los recursos y en cierto modo evita que los atacantes puedan acceder, modificar y descubrir información a la que no tienen autorización, así mismo se busca que las comunicaciones no sean interceptadas por terceras personas.

Los 2 aspectos importantes de la confidencialidad son:

- Servicios de confidencialidad de contenido. Se refiere a proveer de confidencialidad a la información o recurso mediante algún tipo de cifrado que evite que entidades no autorizadas descubran el contenido del recurso.

- Servicios de confidencialidad de flujo de mensaje. Se provee confidencialidad acerca del emisor y receptor del mensaje, igualmente se implementa mediante algún tipo de cifrado.

3. Control de acceso

En este servicio se brinda seguridad acerca de quiénes pueden acceder a los bienes que se desean proteger. Este acceso se puede controlar mediante dispositivos como son los controles biométricos o dispositivos más simples como las cámaras de seguridad; así mismo se pueden usar mecanismos más comunes como un ID o contraseña, de tal forma que se valide la identidad de quien desea acceder a los activos. Es por ello que el

control de acceso va muy de la mano con la autenticación. De este modo, para que alguien pueda acceder a cualquier activo, primero tendrá que validar su identidad y su permiso para tal acceso, esto logra que los bienes estén protegidos de intrusiones.

Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Estos últimos describen los privilegios de la entidad o los permisos con base en qué condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red.[3]

Es conveniente que los permisos que se brindan a una persona o usuarios de cierto sistema sean actualizados de manera constante, para evitar que entidades que en algún momento tuvieron autorización para manejar los bienes, logren acceder a los mismos cuando ya no son considerados usuarios con permisos. También es conveniente que existan niveles de seguridad, de tal modo que entre mayor importancia posea un activo, mayor sea la dificultad para acceder a él.

Para la protección de los recursos individuales se puede hacer uso de una lista de control de acceso (LCA), que es una lista de permisos asignados a las personas y a los recursos, es decir, en ella se plasma quién puede acceder a qué recurso, así como lo que puede realizar con el mismo.

[3] María Jaquelina López Barrientos, Fundamentos de seguridad Informática, 1ª. Edición, UNAM Facultad de Ingeniería, México D.F, 2006, p.117.

4. Disponibilidad

Trata de la seguridad de que los bienes estén disponibles en el momento y circunstancia que se desee, las veces que se requiera. El administrador del activo es quien decide en qué momento estará disponible, para quién lo estará y cuántas veces podrá acceder a él.

La disponibilidad es independiente de la integridad, es decir únicamente se encarga de que el activo esté disponible sin importar las condiciones en que se encuentre.

En este servicio de seguridad se tratan las posibles causas por las que un bien no esté disponible y se deben prevenir o reparar cuanto antes los errores que provoquen la indisponibilidad no prevista, contando con opciones alternativas que logren una restauración del sistema en caso de que se requiera.

5. Integridad

La integridad se refiere a que un sistema, información o cualquier bien que se está protegiendo permanezca en óptimas condiciones y como se requiere. Esto es, si se tiene un activo en cierto estado, y es el estado deseado, se hará lo necesario para que se mantenga de ese modo y no sea modificado. Para lograr esto, primeramente se verifica que los activos se encuentren en el estado que se requiere, de no ser así, se toman las medidas necesarias para lograrlo, y una vez que ya se tiene dicho estado, se protegen de cualquier agente que pueda cambiarlo o modificarlo. Esto implica resguardo no solo en un lugar establecido, sino que si es una

información o un dispositivo que será enviado de un lugar a otro, se debe verificar que llegue de manera adecuada.

Es muy común que se recurra a mecanismos que validen que el estado del activo es el correcto, por ejemplo algún sello de garantía.

Cuando no se cuenta con este servicio de seguridad, puede que entidades no autorizadas hagan algún tipo de modificación en los bienes según sea su conveniencia, como inserción o modificación de información. Es por ello que el principal objetivo de la integridad, es mantener el estado inicial de los activos evitando con ello, cualquier tipo de alteración o en el peor de los casos, la denegación de algún servicio.

Existen 2 tipos de servicios:

- Servicios de integridad del contenido. Tiene que ver con las pruebas que se realizan para verificar que el contenido se encuentra en el estado ideal y no ha sido alterado.

- Servicios de integridad de la secuencia del mensaje. Se refiere a la verificación de que la secuencia de un mensaje es la correcta y no ha sido modificada, evitando así, la réplica y mal ordenamiento de un mensaje.

6. No repudio

Es la prevención de que algún emisor o receptor niegue ser el autor de un envío o una recepción según sea el caso. Lo que se busca con este servicio de seguridad es que el receptor pueda comprobar quién fue quien le envió

un mensaje. Así mismo el emisor debe poder comprobar quién recibió dicho mensaje. Con esto se logra una protección de un usuario frente a otro, por medio de evidencias que comprueben lo que se está afirmando.

Los servicios que pueden ser proporcionados son:

- No repudio de origen. Se proporcionan pruebas del origen de los datos, protegiendo al receptor de que el emisor niegue un envío.

- No repudio de envío. Se brindan pruebas de recepción de datos, protegiendo al emisor de que el receptor niegue haber recibido algo.

- No repudio de presentación. Se prueba que la presentación de un bien fue como se indica, protegiendo de negar que la información fue presentada para su envío.

- No repudio de transporte. Protege de cualquier intento de negar que los datos han sido transportados de un lugar a otro.

- No repudio de recepción. Similar a la primera, se protege de cualquier negación de haber recibido los datos.

Con estos servicios de seguridad se pretende, que los bienes se encuentren protegidos lo mejor que se pueda. Es por ello, que no solo se debe considerar un servicio sino que deben ser considerados todos y cada uno de ellos, ya que de no ser así, se da la posibilidad a los perpetradores de realizar sus ataques y dañar los activos que se poseen.

1.6 Mecanismos de seguridad

Como se mencionó, es muy importante implementar todos los servicios de seguridad existentes. Para poder lograrlo es necesario hacer uso de herramientas y medidas que permitan resguardar los activos de manera adecuada. De ahí la existencia de los mecanismos de seguridad.
Los mecanismos de seguridad son también llamadas herramientas de seguridad y son todos aquellos que permiten la protección de los bienes y servicios informáticos. Con estos mecanismos es con lo que se contesta la última pregunta de la metodología de la seguridad informática: ¿Cómo se van a proteger los bienes?

Estos mecanismos pueden ser algún dispositivo o algo físico que permita resguardar un bien, un software o sistema que de igual manera ayude de algún modo a proteger un activo y que no precisamente es algo tangible, o una medida de seguridad que se implemente, por ejemplo las políticas de seguridad.

Un mecanismo de seguridad puede servir para implementar uno o varios servicios de seguridad, al igual que un servicio de seguridad puede ser implementado mediante varios mecanismos.

Básicamente, al hacer uso de los mecanismos de seguridad lo que se busca es, detectar, prevenir y recuperarse de algún ataque que se efectúe en contra del activo a proteger.

Los mecanismos también reciben el nombre de controles ya que dentro de sus funciones se encuentran el indicar la manera en que se deben ejecutar las acciones que permitan resguardar la seguridad y se eviten vulnerabilidades en la misma.

Hoy en día no existe un mecanismo que logre implementar todos los servicios de seguridad, es por ello que se debe hacer un análisis de lo que se quiere proteger y de qué se quiere proteger para saber qué mecanismos se utilizarán para poder lograr el objetivo deseado, y elegir los que resulten más convenientes para la persona u organización que desea la protección.
De acuerdo con la función que desempeñan, los mecanismos de seguridad pueden clasificarse en mecanismos específicos o mecanismos generalizados.

1. Mecanismos específicos. Son aquellos que se encargan de cumplir un aspecto de seguridad, es decir tienen un solo objetivo definido. Como ejemplo se puede tomar un antivirus, cuya finalidad al hacer uso de él, es impedir que un sistema sea atacado por algún virus o gusano.

2. Mecanismos generalizados. Son aquellos que logran cubrir varios aspectos de seguridad informática. Por ejemplo un control biométrico, logra asegurar un data center en varios aspectos, ya que evita que se roben algún dispositivo que se encuentre en el interior, cubre también la autenticación y la confidencialidad, al no permitir el acceso al bien, y permite preservar la integridad.

Por otra parte los mecanismos de seguridad pueden clasificarse de acuerdo con la importancia que poseen, de este modo, pueden ser mecanismos requeridos o mecanismos discrecionales.

1. Mecanismos requeridos. Son los controles mínimos que se requieren para implementar un servicio de seguridad.

2. Mecanismos discrecionales. También llamados específicos, son los controles que se implementan de acuerdo con la experiencia de alguien, es decir ya son conocidos por una persona y de acuerdo con los

resultados obtenidos con la implementación de ellos, es que se utilizan o no.

Como puede observarse, existe una gran cantidad de mecanismos de seguridad para alcanzar el nivel de protección que se desea, al saber cuáles son los activos que se quieren proteger y de qué se quiere proteger, se pueden elegir los mecanismos adecuados para lograr esa seguridad, ya sea uno o varios, según sea necesario.

Finalmente los mecanismos pueden clasificarse de acuerdo con el objetivo principal de los mismos en:

1. Mecanismos preventivos. Como su nombre lo dice, son aquellos cuya finalidad consiste en prevenir la ocurrencia de un ataque informático. Básicamente se concentran en el monitoreo de la información y de los bienes, registro de las actividades que se realizan en la organización y control de todos los activos y de quienes acceden a ellos.

2. Mecanismos detectores. Son aquellos que tienen como objetivo detectar todo aquello que pueda ser una amenaza para los bienes. Ejemplos de éstos son las personas y equipos de monitoreo, quienes pueden detectar cualquier intruso u anomalía en la organización.

3. Mecanismos correctivos. Los mecanismos correctivos se encargan de reparar los errores cometidos o daños causados una vez que se ha cometido un ataque, o en otras palabras, modifican el estado del sistema de modo que vuelva a su estado original y adecuado.

4. Mecanismos disuasivos. Se encargan de desalentar a los perpetradores de que cometan su ataque para minimizar los daños que puedan tener los bienes.

1.7 Estándares o normas de seguridad

Con lo visto en las páginas anteriores, puede visualizarse que la seguridad informática hoy en día es de suma importancia en la vida cotidiana, aunque no todos los usuarios posean los conocimientos necesarios de la misma. Es por ello que existe una normatividad acerca de la manera en que debe ser implementada la seguridad de cualquier organización.

Para la adecuada administración de la seguridad de la información, es necesario enfrentarla de forma teórica y documentada, de tal forma que se base en una evaluación de los riesgos a los que se está expuesto.

Un estándar es algo que está establecido, sirve como referencia para realizar algo, es un patrón en el cual se pueden basar las personas para llevar a cabo una acción, pero que no es obligatorio, simplemente ayuda a la realización de las cosas sin tener que hacerse exactamente como está planteado.

En la seguridad informática existen varios estándares que permiten la implementación de la protección a los activos, de una mejor manera. Con estos estándares se pretende que los usuarios y organizaciones logren la seguridad de sus bienes basándose en medidas conocidas que faciliten la labor de los encargados de la protección de dichos activos.

Algunos de estos estándares con los conocidos Criterios Comunes y la serie 27000.

1. Criterios Comunes

Los Criterios Comunes o Common Criteria es un estándar mundial de seguridad que permite medir la fiabilidad de los productos de tecnologías

de la información. Se encarga principalmente de establecer niveles definidos de evaluación y aplica el objetivo del concepto de evaluación y el documento de seguridad de destino.

Los CC son útiles como guía para el desarrollo, evaluación o adquisición de productos de tecnología de la información (TI) que incluyan alguna función de seguridad ya que permiten comparar los resultados entre evaluaciones de productos independientes. Para ello, se proporciona un conjunto común de requisitos funcionales para los productos de tecnologías de la información. El proceso de evaluación establece un nivel de confianza en el grado en el que el producto TI satisface la funcionalidad de seguridad de estos productos y ha superado las medidas de evaluación aplicadas.

Con el fin de poder certificar un producto según los criterios comunes se deben comprobar, por parte de uno de los laboratorios independientes aprobados, numerosos parámetros de seguridad que han sido consensuados y aceptados por 22 países de todo el mundo. El proceso de evaluación incluye la certificación de que un producto específico cumple con los siguientes aspectos:

a) Los requisitos del producto están definidos correctamente.
b) Los requisitos están implementados correctamente.
c) El proceso de desarrollo y documentación del producto cumple con ciertos requisitos previamente establecidos.

Los Criterios Comunes definen las funciones de seguridad de los productos y sistemas de Tecnologías de la Información y de los criterios para evaluar su seguridad. El proceso de evaluación, garantiza que las funciones de seguridad de tales productos y sistemas reúnen los requisitos declarados. Así, los clientes pueden especificar la funcionalidad

de seguridad de un producto en términos de perfiles de protección estándares y de forma independiente seleccionar el nivel de confianza que posee dicho sistema.

2. Serie 27000

La serie 27000 es un conjunto de estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Dicha serie contiene un conjunto de buenas prácticas recomendadas para desarrollar, implementar y mantener especificaciones que permitan preservar el buen funcionamiento de los sistemas de gestión de la seguridad de la Información (SGSI). Actualmente la mayoría de estas normas aún están en desarrollo.

Esta serie brinda un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
Los rangos de numeración reservados por ISO para la serie 27000 van de 27000 a 27019 y de 27030 a 27044.

Los más importantes de esta serie son las normas ISO 27001, ISO 27002, ISO 27006 e ISO 27799.

a) ISO/IEC 27001

Es un estándar internacional que fue publicado en 2005, el cual se aplica a cualquier organización y de cualquier sector, en donde se tenga información crítica y tecnología de información. Dicho estándar define

cuáles son los requisitos que se necesitan para establecer un sistema de gestión de la seguridad de la información, SGSI. También es muy utilizado en las organizaciones que se encargan de gestionar información para terceros, ya que con ello brindan a los clientes una garantía de que su información está protegida, por ejemplo las empresas de subcontratación de TI.

Para poder realizar la implementación de ISO/IEC 27001, se requiere de entre 6 y 12 meses, según sea el grado de seguridad que se tenga en la información y el ámbito en el cual será sometido el SGSI. Además de contar con equipo en el que estén miembros de todas las áreas de la organización que vayan a ser afectadas por el sistema; este equipo debe ser liderado por consultores especializados en seguridad informática, protección de datos y SGSI.

b) ISO/IEC 27002

Se trata de otro estándar que describe los objetivos de control y medidas recomendables en cuanto a seguridad de la información. El ISO/IEC 27001, contiene un anexo en el cual se resumen los controles de este 27002. Este documento está dividido en 15 capítulos, en los cuales se plasman sus objetivos y utilidades. Básicamente trata de minimizar lo más posible, los daños que pueda tener la información de una organización; trata de identificar y ordenar por prioridades, los riesgos de seguridad que puedan ocurrir. Busca dar un tratamiento adecuado a dichos riesgos, mediante el uso de prevenciones, para evitar en lo posible que los daños ocurran. Proporciona dirección y soporte para la seguridad de la información. Para esto es necesario que cada organización redacte un "documento de la política de seguridad de la información", el cual debe ser aprobado por la gerencia de la empresa y posteriormente se le debe

informar a los empleados de la misma, sobre la existencia de él. El documento debe contener la definición de seguridad de la información, sus objetivos e importancia, gestión de riesgos, y en general una explicación de lo que se pretende, sin incluir información confidencial.

c) ISO/IEC 27006

Fue publicada el 13 de febrero de 2007. En esta norma se hacen especificación acerca de los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

Brinda ayuda para interpretar los criterios de acreditación, pero no es una norma de acreditación por sí misma.

d) ISO/IEC 27799

Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario. Esta norma, define directrices para apoyar la interpretación y aplicación en la salud informática; también especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria para garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud.

Estas normas no son de libre difusión, por lo que si desea acceder a las normas completas, deben ser adquiridas.

Capítulo 2: Políticas de seguridad

2.1 Definición y objetivos

Cuando se habla de seguridad informática, se habla de activos y el deseo de protegerlos de todo aquello que quiera dañarlos; por lo mismo se determinan acciones que los usuarios y personas externas pueden o no pueden hacer con los sistemas informáticos, para lograr esa seguridad. Es aquí donde entra el concepto de políticas de seguridad.

Las políticas de seguridad son un conjunto de reglas o normas con base en las cuales se busca obtener la seguridad deseada. Es decir, es la definición de lo que se puede y lo que no se puede realizar dentro de una organización, lugar, asignación de tareas a los usuarios, permisos y restricciones de todo aquello que tenga acceso a los bienes. Son todas aquellas normas que permiten llevar a cabo los procedimientos necesarios para lograr el nivel de seguridad que se desea en una organización, edificio, equipo, o cualquier activo.

La RFC 1244 define política de seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."[4]

Estas políticas se definen en un documento en el cual se afirman las prohibiciones o permisos que se pueden tener en algún lugar o con respecto a algún objeto.

La finalidad de plasmar las políticas de seguridad en un documento es respaldar las condiciones establecidas para el uso de los equipos o de la información, por si se presenta el caso en el que alguien realice algún uso

[4] RFC 1244: Site Security Handbook. J. Reynolds –P. Holbrook. Julio 1991

indebido de éstos, se le pueda sancionar de acuerdo con lo ya establecido; este respaldo de las políticas se logra con la documentación.

Se puede establecer la cantidad de políticas de seguridad que se desee de acuerdo con lo que se busca proteger y de qué se va a proteger. De hecho, para cada cuestión a tratar lo más adecuado es redactar las políticas de seguridad necesarias para cada una de manera independiente, para lograr el objetivo deseado sin omitir ningún aspecto y haciendo una correcta determinación de las políticas. Esto es, si se desea especificar quién puede o no acceder a algún sitio y quién puede usar y de qué manera los equipos, lo ideal sería hacer unas políticas de control de acceso y otras de usos de equipos, para poder establecer adecuadamente la seguridad que se desea tener; de lo contrario, si se define todo en un solo documento puede que se omita algún aspecto por visualizar las restricciones de manera más general y no tan específica como sería de hacerlas de manera independiente.

El principal objetivo de las políticas de seguridad es garantizar que se está cumpliendo con los objetivos determinados inicialmente, permite que se efectúe un correcto uso y manipulación de los recursos. De este modo, las políticas de seguridad especifican las medidas de seguridad que se requieren para lograr la protección de los recursos, especificando las acciones que cada miembro de la organización o persona que haga uso de los bienes, puede o no hacer, así mismo determinan las propiedades y responsabilidades de los sistemas o activos.

Con la implementación de las políticas de seguridad se logra un mejor control de quienes hacen uso de los bienes y la manera en que los utilizan. Se determinan jerarquías que asignen diversos permisos a quienes tienen acceso a los activos, de manera que se logra un mayor nivel de seguridad en la

organización, y se establecen reglas que al respetarse garanticen la seguridad de los activos.

Existe una gran cantidad de tipos de políticas de seguridad, ya que de acuerdo con el objetivo que se busque, o lo que se desee proteger, es como se pueden clasificar. Algunos ejemplos de esto son las políticas de seguridad en cómputo, políticas de seguridad para la confidencialidad, políticas de seguridad de respaldo, de correo electrónico, de autenticación, de sanciones, de contraseñas, de higiene, de convivencia, de comportamiento, etcétera. Como se puede ver, todo depende de lo que se desea proteger y es sobre lo que tratarán las políticas de seguridad.

Es importante que a la hora de implementar un conjunto de políticas de seguridad, primeramente se consideren la determinación de políticas para la protección de la información y los recursos; sin embargo, posteriormente se deben considerar todos los aspectos que involucren una necesidad de seguridad sin minimizar los riesgos que pueda tener cada uno de los activos.

Las políticas de seguridad deben ser redactadas o por lo menos autorizadas por los responsables de los sistemas, ya que son éstos quienes teóricamente poseen mayor conocimiento acerca de los requerimientos de los activos y lo que es mejor para la organización.

En las políticas de seguridad se deben reflejar claramente las normas, reglamentos y protocolos que se desea que se sigan. En dichas políticas es preciso que se definan las medidas a tomar para proteger la seguridad del sistema o del activo del cual se busca la seguridad pero siempre se debe considerar que una política de seguridad es una manera de comunicarse con los usuarios o con toda aquella persona que tenga acceso al bien en cuestión, por lo cual es importante considerar una serie de reglas que nunca deben

olvidarse a la hora de la redacción de las políticas y que facilitarán la comprensión de las mismas y el cumplimiento de los objetivos.

Cuando se desea determinar un conjunto de políticas de seguridad, se consideran los elementos claves de seguridad, que son los ya mencionados servicios de seguridad: Integridad, Disponibilidad, Control de Acceso, Autenticación, No Repudio y Confidencialidad.

Sin embargo, es indispensable reconocer que no se trata de una descripción técnica de los mecanismos de seguridad, sino únicamente de una descripción de lo que se desea proteger y la manera en que se busca lograr esto.

Es de suma importancia que en la elaboración de las políticas de seguridad, se consideren todos los aspectos posibles, esto es, el físico, lógico, de humanos, logístico. Es conveniente que se considere la experiencia de las personas para lograr una mayor cobertura en la seguridad, pues muchas veces se piensa que no es importante abordar algún aspecto y resulta que es justo en ese punto el que dio origen a algún ataque o amenaza. También la persona responsable de la redacción de las políticas debe estar abierta a recomendaciones de su equipo de trabajo o de alguien que pueda aportar ideas buenas, pues entre mayor sea la colaboración del equipo, serán considerados más aspectos de seguridad y la probabilidad de sufrir un ataque disminuye.

Un concepto muy importante en las políticas de seguridad son los modelos de seguridad. Un modelo de seguridad es la presentación formal de dichas políticas. En este modelo se definen todas las tareas y reglas que estén establecidas para el manejo de los sistemas informáticos y de la información que éstos administran.

Los modelos de seguridad pueden ser:

a) Modelo abstracto. Se ocupa de las entidades abstractas como sujetos y objetos.[5]

b) Modelo concreto. Traduce las entidades abstractas a entidades de un sistema real como procesos y archivos.[6]

Así mismo, los objetivos[7] de los modelos son:

1. Proveer un sistema que ayude a comprender los diferentes conceptos.

2. Proveer una representación de una política general de seguridad formal y clara.

3. Expresar la política exigida por un sistema de cómputo específico.

2.2 Principios fundamentales

Los principios fundamentales son las bases en una política de seguridad. En otras palabras, son los objetivos que se buscan al implementar las políticas de seguridad.
Es de suma importancia que se tenga bien definido qué es lo que se quiere lograr al implementar una política de seguridad, para ello quienes realicen estos documentos pueden basarse en los principios fundamentales y delimitar los objetivos de las políticas.

[5] María Jaquelina López Barrientos, Fundamentos de seguridad Informática, 1ª. Edición, UNAM Facultad de Ingeniería, México D.F, 2006, p.134.
[6] Ídem
[7] Ídem

Los principios que se aplican en las políticas de seguridad en general son:

- Autorización. Son las normas que asignan quién y de qué manera puede realizarse una acción.

- Responsabilidad individual. Cuando una persona tiene autorización para llevar a cabo ciertas actividades, debe saber que con dicho privilegio lleva una responsabilidad, ya que se registrarán las actividades que realice y los problemas que surjan en el tiempo en que dicha entidad hace uso de la autorización brindada, caerán sobre la persona que está ejecutando las actividades.

- Separación de actividades. Esto se realiza con la finalidad de separar responsabilidades y tener un mejor control de las acciones que se llevan a cabo dentro de una organización, con ello se logra que una persona no haga actividades no autorizadas sin que pueda ser detectada.

  La separación de actividades también ayuda a que se tengan una mayor cantidad de opciones para encontrar una solución a los problemas que se presenten.

- Mínimo privilegio. Se refiere a que únicamente se le brinde a cada persona la autorización necesaria para la correcta elaboración de su trabajo. Esto es, que no se le dé a nadie la posibilidad de acceder a un bien que no es necesario, logrando así un acceso mínimo a los bienes que se desean proteger, limitando la cantidad de agentes que puedan acceder a dicho bien. Para realizar esto se establecen jerarquías tanto en el personal como en el acceso a los bienes.

- Auditoría. Llevar a cabo un control constante de las actividades que se están realizando, ayudan de manera importante a saber con tiempo cuándo existen irregularidades con el manejo de los activos. Se deben monitorear las acciones y resultados que se están obteniendo para controlar las acciones de cada persona.

- Redundancia. Es importante que se realicen copias de seguridad de la información de manera constante y resguardarlas en distintos lugares, para que en caso de que exista un daño en el sistema se cuente con respaldos y no se pierda dicha información, logrando así que no se afecte el trabajo que se está llevando a cabo. Sin embargo, es de suma importancia que los respaldos sean correctos y actualizados, de modo que se evite tener un gran número de copias no actualizadas y que no se sepa cuál es la correcta.

- Reducción de riesgos. Como su nombre lo dice, se busca reducir al máximo los riesgos que se tengan, de manera que sea proporcional el costo de la aplicación al riesgo.

Cuando se realizan políticas de seguridad se deben tomar en cuenta varios roles de las personas involucradas con las mismas. Estos roles son:

- Autor. Es quien redacta las políticas de seguridad. Regularmente dicha personas es la encargada de la organización.

- Autorizador. Es quien controla el documento y aprueba o no cada una de las políticas que se establezcan en él así como el acceso al mismo. Puede ser el mismo autor.

- Custodio. Se refiere a la persona que resguarda el documento y la encargada de autorizar si alguien puede acceder a él.

- Usuario. Es quien lee el documento.

Si se consideran todos estos puntos al realizar un documento de políticas de seguridad, es más probable que se logren los objetivos planteados y se logre el nivel de seguridad que se requiere.

Como ya se mencionó, unas de las principales propiedades más importantes de la seguridad informática son la confidencialidad, integridad y disponibilidad; las 2 primeras reflejan las propiedades del mundo real.[8]

Es por ello que las políticas de seguridad que más comúnmente se pueden encontrar tienen que ver con estos aspectos. Con respecto a la confidencialidad, normalmente se redactan políticas que permitan resguardar la información de toda aquella persona que no tenga autorización para verla o que pueda usarla con fines diferentes a los establecidos, debido a esto es que en algunos casos se clasifica la información de acuerdo con su nivel de confidencialidad y las políticas pueden definirse como una relación entre el nivel de acceso que posea la persona, por ejemplo, de acuerdo con su cargo, y el nivel de confidencialidad que tenga el documento.

Con respecto a la integridad, lo que se busca es lograr protección contra perpetradores que puedan modificar la información o dañarla. Las políticas de integridad más comunes son:

[8] María Jaquelina López Barrientos, Fundamentos de seguridad Informática, 1ª. Edición, UNAM Facultad de Ingeniería, México D.F, 2006, p.132.

- Establecimiento de las acciones que pueden o no pueden hacer las personas con respecto a los bienes.

- Supervisar y aprobar las acciones que se realizan.

- Rotación de obligaciones. Se refiere a que no siempre sean realizadas las mismas acciones por las mismas personas, sino que se cambien las tareas constantemente.

- Cooperación de varias personas para la elaboración de una tarea. No permitir que una sola persona se haga cargo de las actividades.

- Verificar que la información es válida.

- Realizar cambios en la información de manera escrita. Se deben respetar ciertos procedimientos para poder modificar la información, sin embargo, se permite que existan esos cambios siguiendo lo establecido inicialmente.

- Definir el orden de las actividades, es decir, que las tareas sean realizadas única y específicamente como fueron definidas.

Finalmente las políticas de seguridad de la computación, se definen de acuerdo con lo que ocurre día con día en la realidad. No tiene caso que se establezcan medidas para acciones que sean improbables que sucedan, pero nunca se deben minimizar las probabilidades de que ocurran ciertos ataques que tienen una sola posibilidad de presentarse.

De acuerdo con todo lo anteriormente mencionado, se puede observar que el hecho de idear la realización de una política de seguridad requiere un gran compromiso con la organización, ya que se debe tener una clara visión acerca de las amenazas y vulnerabilidades que se tienen en los activos y estar seguros que con las realización de un conjunto de políticas se podrán minimizar dichas amenazas y vulnerabilidades, así como los riesgos que éstas conllevan.

2.3 Redacción de políticas de seguridad

En la redacción de políticas de seguridad es de suma importancia que como primer punto se identifique a todos y cada uno de los miembros de la empresa que tiene intervención para la redacción de las políticas. Estos actores son los siguientes:

- Administradores del sistema
- Persona con autoridad
- Representante jurídico
- Editor/Redactor
- Psicólogos
- Usuario típico

Primeramente los administradores del sistema y la o las personas con autoridad en la empresa como los directivos de la empresa u organización son los personajes principales que se deben encargar de la redacción de las políticas de seguridad. Ellos, con la colaboración de los expertos en tecnologías de la información, deben definir explícitamente los puntos a tratar acerca de la seguridad que se desea implementar mediante el uso de

las políticas de seguridad. Deben ser claros y precisos al plasmar los objetivos deseados con la redacción de dichas políticas.

Las principales razones por las que estas personas son quiénes deben encargarse de la redacción de las políticas son las funciones y roles que tienen dentro de la organización ya que tienen la capacidad, responsabilidad y conocimientos para que por una parte los directivos se encarguen de preservar:

- El desarrollo y mantenimiento de todas y cada una de las políticas.
- La garantía de las políticas, apoyándose en la documentación pertinente, así como las instrucciones de procedimiento.
- La garantía de que la documentación será pertinente y se mantendrá al día.
- La garantía de cada una de las políticas y sus sucesivas actualizaciones se comunicarán a los departamentos y personal correspondiente.

Y por otra parte los expertos en tecnologías de la información o encargados del sistema verificarán que:

- Se están tomando en cuenta todos y cada uno de los recursos que se desean proteger, así como el valor de los mismos.
- Se han analizado todas las vulnerabilidades y amenazas del sistema, probabilidad de ocurrencia y costo.
- Se han tomado las medidas necesarias para contrarrestar los efectos que pueda provocar el incumplimiento de las políticas, de acuerdo a lo que se desea proteger y de lo que se desea proteger, siendo dichas medidas, proporcionales a los puntos anteriores.

Continuando con los diferentes roles de las personas que intervienen en la redacción de las políticas de seguridad, sigue el representante jurídico. Esta persona es importante que conozca y aporte sus ideas acerca de la redacción de dichas políticas, ya que en caso de que se falte a una o varias políticas será quien, dependiendo del daño que se cause al violar la política, tomará las medidas acerca de la sanción que debe recibir el individuo que haya cometido dicha falta. En su defecto, el representante jurídico también es quien debe verificar que en la redacción de las políticas no se viole los derechos o se falte a alguna persona.

Otra persona que debe intervenir en la redacción es el editor o redactor, que debe ser alguien que sepa del tema y con base en lo que los personajes anteriores desean plasmar en el documento, se encargará de hacer la redacción de dicho documento, asegurando así, que se expresará lo que realmente se desea, ya que de lo contrario, muchas veces se tiene en claro cuál es el objetivo de las políticas, pero debido a la mala redacción en ellas, no se logran los objetivos.

El psicólogo también debe aportar sus conocimientos para la redacción de las políticas, debido a que es un especialista en el comportamiento de las personas y aportará demasiado acerca de la forma en que se debe redactar el documento para que las personas involucradas memoricen mejor o aprendan de una manera más rápida qué es lo que deben y no deben realizar. También aportará ideas acerca de cuál es la mejor manera de redactar y que las personas entiendan sin que alguien se sienta ofendido.

Finalmente no se debe olvidar de considerar al usuario típico, que si bien no interviene directamente en la redacción de las políticas, nunca se debe dejar de lado su importancia en las políticas, pues es a quien va dirigido el mensaje.

Para la redacción de las políticas de seguridad es muy importante que se tomen en cuenta varios aspectos básicos que permitirán un correcto entendimiento de las mismas y de este modo se logren cumplir los objetivos buscados. Esto se debe a que si una política no es redactada de manera adecuada, puede que los usuarios o a quienes van dirigidas, no entiendan qué es lo que se está pidiendo, lo que ocasionará que no se lleven a cabo y de nada servirá que se hayan implementado.

Lo primero que se hace cuando se piensa hacer la implementación de unas políticas de seguridad, es realizar un análisis de lo que se busca o cuál es el objetivo principal de establecer dichas políticas de seguridad. En esta parte se hace el análisis de seguridad informática, es decir, identificar qué es lo que se quiere proteger y de qué se quiere proteger. Una vez que ya se sabe esto, se puede continuar con la redacción de las políticas, pues ya se tiene el conocimiento de lo que se requiere y ahora sí se puede seleccionar la mejor opción para redactarlas, buscando expresar adecuadamente lo que se quiere o no se quiere en un edificio, aula, equipo o cualquier bien que se desee proteger; incluso si lo que se desea proteger es la seguridad de los propios usuarios o el personal.

Cuando ya se conocen los objetivos de las políticas se prosigue con la redacción. Para realizar dicha redacción de manera adecuada, como primer punto se selecciona una filosofía. Dicha filosofía se refiere a la manera en que serán redactadas las políticas.

Existen 2 filosofías que pueden ser utilizadas para la redacción de las políticas de seguridad que son la prohibitiva y la permisiva.

- Prohibitiva. Se refiere a que todo está prohibido a excepción de lo que se permite en las políticas.

- Permisiva. En esta filosofía todo está permitido menos lo que se prohíbe en las políticas.

Como ejemplo de dichas filosofías, en las políticas de seguridad prohibitivas es común encontrarse con enunciados como:

"El acceso al edificio será de 8:00 am a 10:00 pm", o "Se permite la entrada a la sala de cómputo a toda persona que presente tarjeta de acceso".

En estos enunciados puede verse claramente la filosofía prohibitiva, ya que lo único que se permite es el acceso al edificio en el horario establecido, por lo que se entiende claramente que si alguien desea acceder fuera del horario, no podrá hacerlo. Del mismo modo se entiende que para ingresar a la sala de cómputo se requiere de una tarjeta de acceso, por lo que cualquier persona no autorizada no podrá acceder.

Por otra parte, en las políticas de seguridad permisivas, el tipo de enunciados que se pueden ver normalmente son prohibiciones como por ejemplo: "Se prohíbe ingerir alimentos" o "Prohibido usar el elevador en caso de sismo". En este tipo de políticas se puede entender claramente que todo está permitido a excepción de lo que está explícitamente prohibido en el documento. En estos casos queda claro que no se puede comer, pero se puede fumar; también queda claro que si bien no se puede hacer uso de los elevadores en caso de sismo, se pueden usar las escaleras.

Para hacer una correcta selección de la filosofía, es necesario saber el nivel de seguridad que se desea y qué filosofía es más conveniente para los fines deseados. Es decir, si se busca un nivel de seguridad alto, en el cual sean demasiadas cosas las que se prohíban, lo adecuado es usar la filosofía prohibitiva, de lo contrario se tendrían que redactar demasiadas políticas y

sería más complicado. Además de que es muy importante que se tome en cuenta a las personas a quienes van dirigidas las políticas, pues resultaría conflictivo usar una filosofía permisiva cuando son demasiadas las cosas que desean prohibir, pues hay casos en los que las personas se sienten ofendidas o afectadas cuando este tipo de documentos no son redactados de manera adecuada y por ejemplo, si ven una larga lista de prohibiciones, muchas veces se sienten atacados.

Por el contrario, si el nivel de seguridad es bajo, o son muy pocas las cuestiones que se desean prohibir, lo ideal es usar la filosofía permisiva, con lo cual se le permite al personal todo y únicamente se redacta aquello que no puede realizar. De este modo es más práctico y se cumple con el objetivo deseado.

Una vez que se ha seleccionado la filosofía que se utilizará para la redacción de las políticas de seguridad, se prosigue con la elaboración de las mismas. Para ello, se deben considerar otros aspectos importantes y de los cuales depende que se cumpla con los objetivos y que las personas hagan caso a lo que se está pidiendo.

Los puntos que se consideran para la redacción de las políticas son:

1. Se deben redactar en presente, ya que de este modo se entiende que es en el momento cuando se puede o no se puede realizar una acción. Está permitido redactarlas en futuro siempre y cuando se indique en el documento a partir de cuándo entran en rigor dichas políticas.

2. Se deben redactar de manera clara para evitar cualquier tipo de confusión entre el personal y para que se puedan cumplir sin ningún problema.

3. Deben establecerse jerarquías y responsabilidades, pues no siempre van dirigidas a todo el personal sino solo a una parte del mismo.

4. Se debe tomar en cuenta qué tan capacitadas están las personas a quiénes van dirigidas las políticas, para tener la seguridad de que lo expresado en el documento podrá ser entendido por las personas que lo leen.

5. Se debe considerar un lenguaje adecuado en el cual no se utilicen términos técnicos que no todas las personas puedan entender, pero tampoco se usen palabras vulgares, simplemente un vocabulario coloquial pero adecuado para los fines que se pretenden.

6. Evitar realizar hostigamiento a las personas.

7. Evitar hacer uso de la negación (la palabra NO), y siempre redactarlas de manera positiva, ya que muchas veces las personas omiten esa palabra y terminan realizando lo contrario a lo que se pide.

8. Se debe realizar una constante actualización de las políticas para asegurarse de que se está cumpliendo con lo requerido.

9. Se deben dar a conocer de manera adecuada y verificar que se están cumpliendo, de este modo se garantiza que se obtuvo el objetivo. Éste último punto es muy importante ya que si no se dan a conocer de manera correcta, de nada servirá que se realice adecuadamente todo lo demás, pues no se cumplirá el objetivo principal que es el hecho de que se cumplan las políticas. Debido a esto es de suma importancia que se considere a quién va dirigido el documento y se informe de manera correcta a dichas personas, para que ellas puedan cumplirlas. De este

modo, si las políticas van dirigidas a una sola persona, puede entregarse una copia del documento a quien debe cumplir con lo establecido; si las políticas son para un aula o sala en específico, dicho documento puede pegarse en una parte visible del lugar para quienes tengan acceso a él puedan visualizarlas y respetarlas. Si por lo contrario, las políticas de seguridad van dirigidas a un grupo grande de personas como los alumnos de una escuela o un edificio completo, se debe buscar la manera correcta de darle difusión a las políticas, esto se puede lograr haciendo uso de folletos, carteles o trípticos.

Es de suma importancia que se cuente con el apoyo de un experto en tecnologías de la información para la realización de las políticas de seguridad, esto se debe a que aunque tal vez se presente el caso en el cual el administrador del sistema conozca el funcionamiento de los dispositivos, puede que no sea tan minucioso a la hora de identificar las amenazas y vulnerabilidades de los activos, como podría serlo un experto en seguridad informática.

El responsable de la seguridad informática debe ser muy riguroso con la redacción de las políticas, pues debe cubrir todos los aspectos relacionados con la seguridad y debe visualizar todo aquello que represente un problema para alguno de los activos, sin pensar que algo sea irrelevante. Esto se debe a que de no tomarse en cuenta algún aspecto, puede que el resultado sea el incumplimiento de los objetivos iniciales debido a que se minimizó alguna cuestión y esto puede dar como resultado una vulnerabilidad en los sistemas. Por ejemplo, no tiene sentido proteger el acceso con una puerta blindada si a ésta no se la ha cerrado con llave.

También es muy importante que esta persona (responsable de la seguridad informática) se adecúe a las necesidades y recursos; primeramente se

definen los objetivos y después se implementan las soluciones. No tiene sentido adquirir un antivirus si lo que se desea es controlar el acceso físico.

Se debe ser atemporal. Esto quiere decir que el tiempo en el que se aplica no debe influir en su eficacia y eficiencia.

Finalmente se deben definir estrategias y criterios generales con los cuales se pretende resolver los problemas que se tienen.

Es muy importante que a la hora de redactar las políticas, se considere el hardware, software, entorno físico, los usuarios y a las interacciones de todos estos.

Cuando se tiene un modelo de seguridad asumiendo que las políticas de seguridad son adecuadas, se deben seguir ciertos criterios para poder considerarse que se trata de un buen modelo.

Los puntos básicos de un modelo de seguridad son:

- Hacer una clara representación de las políticas de seguridad, es decir, en el modelo se debe definir la forma en que el modelo corresponde a la política.
- Explicar las políticas de seguridad mediante expresiones exactas.
- Soportar decisiones sobre seguridad y un análisis en el cual se pueda determinar si en cierto estado del modelo, hay una propiedad de seguridad determinada que no se mantenga.
- Permitir un modelado de los sistemas por partes. Cuando se trata con sistemas muy complejos, se debe poder manejarlos poco a poco y posteriormente unir todas las partes para una correcta verificación.

- Soportar la creación y verificación del sistema.[9]

2.4 Definición y objetivos de las buenas prácticas

Como ya se vio, las políticas de seguridad son normas que se establecen con la finalidad de que se cumplan y con ello se obtenga un resultado. Sin embargo, en seguridad informática existe otro tipo de enunciados que como tales no son reglas sino únicamente consejos. Estos enunciados son los conocidos como "buenas prácticas".

Las buenas prácticas son únicamente una serie de recomendaciones que se brindan a las personas u organizaciones con la finalidad de mejorar la seguridad de sus bienes. Estas prácticas, si se llevan a cabo de manera constante, llega un momento en el que se convierten en costumbres para quienes las ejecutan.

Conforme transcurre la vida de las personas, éstas experimentan día con día nuevas cosas, obtienen vivencias y son parte de ciertos acontecimientos de los cuales aprenden o se quedan con algo de esos sucesos. Es a esto a lo que se refieren las buenas prácticas. Todo lo que ocurre y todos los avances que se obtienen constantemente durante el transcurso del tiempo, con respecto a la seguridad informática, sirve como ejemplo y como experiencia para ejecutar o implementar cosas nuevas que ayuden a preservar la seguridad de los activos de una mejor manera y minimicen las amenazas, vulnerabilidades o riesgos que éstos poseen.

[9] María Jaquelina López Barrientos, Fundamentos de seguridad Informática, 1ª. Edición, UNAM Facultad de Ingeniería, México D.F, 2006, p.135

Diariamente ocurren hechos que pueden servir como experiencia en seguridad informática. Los avances tecnológicos traen consigo mayores facilidades para la realización de las labores de cualquier ámbito, sin embargo, no solo mejoran los equipos, también aumenta el nivel de los ataques, nacen nuevas vulnerabilidades y nuevos agentes amenazantes.

Si únicamente se limitaran las organizaciones a lo teórico y a lo reglamentado, no se conseguirían los avances en seguridad informática que se poseen y no se lograría implementar una buena seguridad informática. Sin embargo, al experimentar cosas diferentes cada persona o cada organización se logra conocer más acerca del tema, conociendo todo lo que puede ser causa de una amenaza, vulnerabilidad o ataque.

Las buenas prácticas tienen que ver con todo esto, ya que una persona que tal vez trabajó en un lugar diferente al que se encuentre laborando en la actualidad, puede saber mediante su experiencia lo que es más conveniente para los equipos con los que trabaja actualmente, sin siquiera haber experimentado previamente con ellos, se puede dar una idea de los diferentes peligros que éstos pueden tener o de las consecuencias de que ocurra cierto ataque, sin que haya ocurrido ya. Es por ello que se recomienda que al momento que se desea implementar alguna serie de mecanismos para la protección de los bienes, se consulte con un experto en seguridad informática, pues estas personas poseen mayor conocimiento del tema, han laborado en distintos lugares, han lidiado con diferentes ataques o atacantes, saben acerca de lo teórico y lo práctico del área y por lo tanto verán mas allá de lo que una persona que no sea experta en el tema pueda ver.

Con las buenas prácticas lo que se busca es hacer uso de ideas alternativas para el manejo de la seguridad informática, es decir, emplear soluciones viables según sea el objetivo deseado, buscar mejores protecciones, mejores

métodos o simplemente recurrir a procedimientos más adecuados o recomendaciones. Esto obviamente se hace basándose en conocimientos previos, personas que saben lo que hacen y que han tenido experiencias que ayuden a la mejora de la seguridad.

También es importante considerar que las buenas prácticas no solo hacen referencia a experiencias malas que ayuden a la implementación de una mejor seguridad, sino también a las experiencias buenas. Por ejemplo, si se desea proteger algo determinado de un perpetrador definido, y en ese caso con base en la experiencia, ya se conoce un conjunto coherente de acciones que han funcionado para el tratamiento del objetivo determinado, pues es muy normal que con base en esas buenas prácticas se quiera establecer lo mismo, con la finalidad de obtener resultados similares a los obtenidos con anterioridad en un contexto igual o parecido.

En términos generales, las buenas prácticas son un 'plus' para la seguridad informática, ayudan a abarcar mayores aspectos, a controlar de mejor manera la seguridad y a visualizar más ampliamente los riesgos que se tiene y la manera de contrarrestarlos. Por ejemplo, si se desea controlar el acceso de un edificio con un control biométrico, pero a la vez se sabe que con un guardia de seguridad se ha obtenido un buen control en ese lugar, se puede recomendar seguir teniendo al guardia en lo que se valora el funcionamiento del control biométrico.

Las buenas prácticas siempre van a depender del avance tecnológico que se tenga, las modas y de quiénes se encargan de la seguridad del lugar, porque finalmente solo se trata de recomendaciones y son los administradores de la seguridad quienes se encargarán de definir si se siguen o no, si se llevan a cabo o si prefieren optar por soluciones alternas.

Finalmente, las buenas prácticas únicamente brindan posibles soluciones a determinados problemas, siempre se basan en conocimientos previos y soluciones determinadas. Sin embargo, aunque muchas veces los avances tecnológicos las van dejando poco a poco de lado, siempre se puede y se debe contar con ellas como una opción en caso de que algo falle o de que una nueva tecnología se esté probando. Esto es porque las buenas prácticas ya tienen un resultado, ya se sabe lo que pasará si se llevan a cabo, a diferencia de los nuevos mecanismos que se desean implementar. Nunca estará de sobra contar con opciones conocidas que brinden la correcta solución a problemas ya conocidos.

La utilización y manejo de las buenas prácticas, siempre va a depender de la elección que se tenga acerca de la manera en que se piensan atacar los determinados problemas de entre las posibles soluciones, de la estrategia que se tenga para la implementación de la seguridad informática, de las políticas que se tengan, las metas y el control con que se cuenta.

Finalmente es importante mencionar que todo el personal es responsable de que se cumplan las políticas de seguridad, y para informar de cualquier falta o incidentes relacionados con las mismas.

Capítulo 3: Principales problemas informáticos en la actualidad

Como se ha mencionado, conforme la tecnología avanza, el nivel de los problemas informáticos también lo hace, esto es porque se desarrollan nuevos métodos de ataque, se usan las nuevas tecnologías para dañar los bienes informáticos y en cuanto se pretende lanzar una nueva tecnología, los perpetradores ya están trabajando para encontrar vulnerabilidades en las mismas.

De ahí proviene la importancia del estudio de la seguridad informática y conocer las diversas formas en que cada persona puede ser víctima de un ataque informático (Figura 3.1).

Actualmente existen muchos problemas informáticos, inclusive día con día se desarrollan nuevas amenazas y nuevos ataques, y es muy grande la cantidad de dificultades a las que se enfrentan los expertos en tecnologías de la información. Sin embargo, existe un conjunto de estos problemas, los cuales son más comunes en la actualidad y a los que es más probable que cualquier usuario de un recurso informático pueda enfrentarse.

A continuación se hace una presentación de algunos de los principales problemas informáticos a los que las personas y organizaciones se enfrentan día con día, esto incluye los agentes amenazantes y perpetradoras causantes de los ataques informáticos, las vulnerabilidades más comunes a las que hacen frente la mayoría de las personas y organizaciones, así como los ataques más comunes a los que se deben de enfrentar día con día los usuarios y los expertos en seguridad informática.

Figura 3.1 Seguridad Informática

3.1 Agentes amenazantes

Hoy en día existe una gran cantidad de agentes amenazantes que logran un objetivo común: causarle algún daño a la información o a los bienes informáticos.

Estos agentes amenazantes van desde personas que tal vez no tengan intención de realmente hacer ese daño pero que finalmente lo hacen, por lo cual se deben de considerar como una amenaza, hasta quienes sí buscan hacer uso incorrecto de los bienes informáticos y obtener algún beneficio de ellos.

También se incluyen no solo personas, sino todo aquello que pueda causarle un daño a los bienes informáticos.

3.1.1 Perpetradores

Como primer punto, están los perpetradores, aquellos que tienen toda la intención de dañar algún bien informático. Éstos tienen diferentes modos de operar dependiendo del objetivo que tengan. Por ejemplo, uno de los objetivos más comunes es la obtención de información para darle un uso diferente para el que inicialmente fue definido. Esto se puede realizar mediante técnicas como la ingeniería social o usurpando la identidad de alguien más, por ejemplo, personal de un banco o empresa, mediante las cuales se pide información o hacen llenar formatos para algún trámite y así obtienen la información que se desea. Esto generalmente se realiza personalmente.

En esta clasificación entran todos los hackers, crackers, cardings, etcétera., toda aquella persona que causa algún daño a los equipos de los usuarios.

Las actividades que realizan estos individuos es muy variada, no sólo se concentran en la obtención de la información, sino en dañarla, derribar los sistemas y ocasionar problemas de denegación de servicios. Ejemplos del daño que pueden causar es la infección de los equipos mediante virus, gusanos o malware, el cual lo realizan mediante contenidos, noticias o información que comúnmente le interesa a las personas y quienes acceden a sitios inseguros mediante los cuales los atacantes dañan los sistemas de los usuarios.

Algunos perpetradores son:

a) Spammers

Un grupo de estos perpetradores son los conocidos como spammers y vale la pena hablar un poco de ellos ya que actualmente son un dolor de cabeza para muchos usuarios. Estas personas se encargan de saturar las bandejas de correo de los usuarios mediante correos "basura" y esto lo realizan mediante diversas técnicas con las cuales obtienen las direcciones de correo de miles de usuarios y es así como logran enviar todo lo que desean a sus víctimas. Su modo de operar es muy diverso, por ejemplo, mediante el uso de cadenas, chistes y demás correos que los usuarios acostumbran reenviar, pueden obtener gran cantidad de direcciones de correo electrónico ya que usualmente las personas simplemente le dan reenviar y colocan las direcciones de sus conocidos y llega un momento en el cual el mensaje ya contiene un sinfín de direcciones. También es común que los usuarios se suscriban a diversas páginas, foros o blogs o simplemente al realizar una descarga o estar consultando algún sitio, brinden como dato su dirección de correo electrónico.

Otro ataque menos común, pero que sucede, es la entrada de los perpetradores a los servidores y una vez realizando esto, pueden tener

acceso a la información contenida en los equipos, incluyendo las direcciones de correo que se encuentren en las bases de datos.

Como puede verse, es muy difícil estar exento de estos atacantes, sin embargo, con ciertas medidas los usuarios pueden minimizar la posibilidad de ser víctimas de estos individuos.

b) Hacktivistas

Se les conoce con este nombre a quiénes hacen uso de las tecnologías de la información para expresar sus inconformidades en ciertos asuntos sociales como la política, religión, etcétera. (Figura 3.2) Frecuentemente lo que realizan estas personas es la escritura de código con el que pretenden promover una ideología política, como la libertad de expresión, derechos humanos y la ética de la información. Básicamente lo que realizan es similar a las actividades de los activistas, sólo que hacen uso de medios informáticos y afectan de algún modo los bienes de ciertas personas u organizaciones.

Figura 3.2 Hacktivistas

Este tipo de actos tienen la finalidad de que al realizarlos se provoquen efectos en la sociedad como símbolo de protesta ante alguna situación.

La razón por la cual se consideran una amenaza para la seguridad informática no es por las razones o motivos que mueven a estas personas, sino por las consecuencias que sus actos provocan, ya que comúnmente hacen uso de herramientas y código con el que provocan desconfiguraciones de sitios web, ataques de denegación de servicio, robo de información, sustituciones virtuales, sabotajes virtuales y desarrollo de software maligno.

Ejemplo de este tipo de amenazas es un grupo de activistas en línea de nombre Anonymous, quienes han realizado una gran cantidad de protestas en línea y diversos ataques por medio de internet. Este grupo recientemente realizó un ataque a una empresa de seguridad informática en EU de nombre HBGary Federal, después de que ésta afirmara que conocía la identidad de sus líderes. En diciembre de 2010 lanzaron una campaña en apoyo a WikiLeaks que causó una interrupción en los servicios de MasterCard, Visa y otras empresas. Así mismo irrumpieron en el sitio de la empresa y la cuenta de Twitter del director de la empresa, realizando una serie de comentarios racistas y sexuales, además de datos personales como el teléfono celular o el número de seguridad social de la víctima. El grupo también informó que habían tomado el control de todo el correo electrónico de la compañía, borrado sus archivos, dando de baja su sistema telefónico y publicando copias de documentos internos en línea. Esta agrupación afirma que está tratando de "defender la libertad y apertura de internet".[10]

c) Ciberdelincuentes

Por otra parte están los llamados "Ciberdelincuentes", que no son otra cosa más que personas que hacen uso del internet para obtener la información que quieren, creando sitios falsos, mediante los cuales las personas ingresan su información o realizan alguna transacción o compra en línea y es así como cumplen su objetivo estos perpetradores, que puede ir desde obtener información confidencial o privada hasta fraudes.

Estas personas también hacen uso de virus y todo tipo de malware para dañar a sus víctimas de uno u otro modo.

[10] http://www.noticiasmvs.com/noticias/capital/los-hacktivistas-de-anonymous-atacan-una-firma-de-seguridad--606.html

Entre las formas de ataque más comunes de estos individuos están las llamadas telefónicas, mediante las cuales realizan el robo de información y el robo de identidad.

Dentro del apartado de nuevas amenazas, los ciberdelincuentes siguen apostando por la creación de los clásicos troyanos bancarios como principal arma para sus ataques. Este tipo de troyanos lo que hacen es intentar captar las contraseñas y datos bancarios de sus víctimas y representa el 56% de las nuevas amenazas, seguido por virus y gusanos.[11]

Recientemente el Barómetro de Pérdida de Datos de KPMG dio a conocer que la piratería informática continúa siendo el mayor riesgo para la pérdida de datos en las empresas.[12]

En dicho reporte se afirma que el espionaje corporativo y el terrorismo son las principales causas de ataques informáticos hoy en día y dicho ataque proviene de los llamados piratas informáticos.

El Barómetro también reveló que el sector de servicios financieros continúa siendo el más afectado, captando 33% de los 249 millones de ataques registrados desde 2007. En segundo sitio se encontró la industria de ventas minoristas con 31%, siendo las tarjetas de crédito y de tiendas departamentales los mayores riesgos a la seguridad. [13]

[11] http://www.theinquirer.es/2011/01/03/la-tercera-parte-de-todos-los-virus-de-la-historia-se-han-generado-en-2010.html

[12] http://www.bsecure.com.mx/ultimosarticulos/espionaje-corporativo-y-terrorismo-son-principales-causas-de-perdida-de-datos/

[13] Ídem

3.1.2 Virus, gusanos y malware

Es importante considerar como agentes amenazantes no sólo a quienes se encargan de diseñar o ejecutar los ataques, sino también a todas aquellas herramientas y medios lógicos mediante los cuales se logra la correcta ejecución de los ataques.

Como es sabido, hoy en día toda persona y organización que hace uso de un equipo de cómputo ha tenido en algún momento problemas con alguna de estas herramientas lógicas como son los virus, gusanos y malware.

La razón por la cual este tipo de amenazas es tan importante se debe a la gran variedad y cantidad que existen. Cada día se generan nuevos virus y nuevas formas de propagación de los mismos, por lo que resulta prácticamente imposible estar protegido de todos estos atacantes lógicos y es muy común que cualquier usuario sea víctima de alguno de ellos.

Por esta misma razón es que se han convertido en una amenaza muy delicada para cualquier ordenador, ya que cada uno de estos programas son diferentes, dañan de manera diferente y si bien es cierto que algunos son relativamente inofensivos, existen otros que pueden provocar un verdadero caos en los equipos, anteriormente sólo se dañaba a los archivos, actualmente esto ya no se limita a eso, sino que existen virus y gusanos que son capaces de dañar el BIOS del ordenador.

Finalmente uno de los principales problemas relacionados con este tema es que avanzan y se multiplican de manera más rápida de la que se contrarrestan, es decir, mientras se está en estos momentos buscando una solución para los "bichos", que salieron ayer, mañana saldrá uno nuevo. (Figura 3.3)

Ejemplo de esto es la reciente amenaza que entra dentro de esta clasificación y es conocida como los antivirus falsos, los cuales poseen una gran incidencia en la actualidad y que se están convirtiendo en una forma de

ataque muy común ante cualquier usuario y que representa el 11.6% de las nuevas amenazas.[14]

Otro ejemplo muy conocido de este tipo de amenazas fue el virus conocido como Zeus. Este virus básicamente lo que hacía era robar información bancaria, y la forma en que se ejecutaba era mediante las descargas y el phishing. Fue identificado por primera vez en el 2007 y en el 2009 se tuvo un registro de más de 74 000 cuentas comprometidas en los sitios web de empresas como el Banco de América , la NASA , Monstruo , ABC , Oracle, Cisco , Amazon , y BusinessWeek, por lo que puede apreciarse el nivel de seguridad en el que se estaba entrometiendo dicho virus. Sin embargo, aunque a finales de 2010 el desarrollador de Zeus donara su código malicioso al creador del troyano SpyEye y las firmas de seguridad dieran por muerto a uno de los códigos maliciosos más peligroso de los últimos años, poco después varios expertos en seguridad notificaron sobre nuevas versiones de Zeus en la red.[15]

Lo peor de estos asuntos es que el desarrollo de este tipo de programas es cada vez mayor y el problema no radica en que exista, sino en la creación de nuevas versiones que dificultan a los expertos en seguridad informática a contrarrestarlo. Por ejemplo, actualmente se han registrado 2 nuevas versiones de dicho virus, las cuales ya logran ocultar la procedencia del mismo, y no puede ser identificado por los expertos en seguridad.

Figura 3.3 Virus y gusanos

Por otra parte Dmitry Tarakanov, experto de seguridad de Kaspersky Lab, señala que las nuevas versiones que se han detectado de Zeus cuentan con un candado de doble cifrado, mientras que las anteriores contaban sólo con una.

[14] http://www.theinquirer.es/2011/01/03/la-tercera-parte-de-todos-los-virus-de-la-historia-se-han-generado-en-2010.html

[15] http://www.bsecure.com.mx/featured/zeus-aun-no-ha-muerto-el-virus-resurge-tras-unirse-al-troyano-spyeye/

Así mismo, un reporte a cargo de Panda Security reveló que durante los tres primeros meses de 2011, los troyanos se convirtieron en el ataque predilecto de los ciberdelincuentes, estando presentes en 70% de las amenazas registradas a lo largo de este periodo.[16]

Del mismo modo existe una gran cantidad de casos de este tipo, una gran variedad de virus, gusanos y todo tipo de malware; así como una enorme cantidad de maneras de ser víctimas de un ataque de este tipo y al parecer no se ve para cuándo se pueda erradicar este tipo de problemas informáticos.

3.2 Vulnerabilidades más comunes

Existen diferentes vulnerabilidades a las que las organizaciones y personas se enfrentan. Éstas normalmente se presentan debido a que no se le da la importancia requerida a ciertos aspectos de seguridad o porque simplemente minimizan la posibilidad de que pueda ser causa de un ataque informático.

3.2.1 Falta de protección de la información

Una de las más comunes vulnerabilidades tiene que ver con la fuga de información; y aquí entra toda la falta de medidas para la protección de la misma. Esto es, no cerciorarse de que la información está debidamente protegida. Ejemplo de estas vulnerabilidades, es no corroborar que los sitios a los que ingresa el personal son seguros y corresponde a quien se dice ser, así como realizar intercambio de información mediante conexiones no seguras como establecimientos públicos.

[16] http://www.bsecure.com.mx/featured/troyanos-arma-favorita-de-ciberdelincuentes-en-2011/

En este aspecto también es una vulnerabilidad el hecho de no tener cuidado con quien los observa cuando realizan alguna actividad en los equipos, que tenga que ver con información importante, ya que los atacantes pueden capturar lo que están realizando, y en caso de que alguien transmita la información, el sistema podría quedar totalmente vulnerado y a disposición del ladrón o de quien pueda hacer daño alguno al sistema. Esto es conocido como un error de capa 8 y se refiere a que la falla en el sistema es originada entre el usuario y el teclado.

3.2.2 Falta de protección de contraseñas

Uno de los principales problemas de descuido de muchos usuarios es la falta de protección o descuido ante sus contraseñas y aunque en ocasiones no es más que una palabra secreta de acceso, muchas veces es la clave para poder ejecutar muchos ataques informáticos que desencadenan una gran cantidad de problemas graves.

Los usuarios minimizan muchas veces la importancia de cuidar sus contraseñas, la mayoría de las veces porque desconocen las consecuencias que una simple palabra puede provocar. Frecuentemente las dejan en lugares poco seguros, como es el escritorio donde laboran o en un "post it" junto al monitor. Esto no lo hacen con intención de perjudicar al sistema sino más bien porque no pueden memorizarlos y desconocen el daño que están haciendo.

Symantec realizó un estudio en el que encontró que 54% de las compañías que utilizan un sistema de seguridad basado en contraseñas experimentó brechas de seguridad durante el último año.[17]

[17] http://www.bsecure.com.mx/ultimosarticulos/el-uso-de-contrasenas-reduce-productividad-y-no-ofrece-seguridad/

La importancia de una contraseña radica en que actualmente la mayoría de los usuarios y organizaciones basan su seguridad en una contraseña; esto va desde las cuentas de correo electrónico, redes sociales, hasta el acceso a un equipo u edificio.

3.2.3 Vulnerabilidades en Cloud Computing

Debido al avance de las tecnologías de la información, se han generado distintas maneras de resguardar la información y de tenerla al alcance de los usuarios cuando es necesario. Una de estas tecnologías es la conocida como el Cloud Computing o cómputo en la nube. Esta tecnología permite ofrecer una gran cantidad de servicios en internet a los cuales los usuarios pueden acceder sin complicación alguna.

Esta tecnología está siendo cada vez más utilizada por una gran cantidad de negocios debido a los beneficios que ofrece, como por ejemplo la movilidad, sin embargo, debido a que aún se encuentra en desarrollo, actualmente posee diversas vulnerabilidades en cuanto a seguridad.

La principal vulnerabilidad es que no todos los usuarios del Cloud Computing, cuidan la información que suben a dicha red y se debe considerar que la información crítica no debe estar en esos centros de información.

Los expertos en seguridad afirman que llevar la información al cloud tiene un alto riesgo debido a que se tiene una cobertura trasfronteriza.[18]

[18] http://www.bsecure.com.mx/featured/expertos-en-seguridad-ti-debaten-sobre-diversas-tecnologias/

En esta parte también es importante mencionar que la llegada de la web 2.0 ha cambiado mucho la forma en que está diseñado internet, ya que ahora se tiene una red mucho más abierta que antes y personalizada, por lo que es muy difícil tener un control sobre lo que cada usuario realiza en la misma.

Entre las aplicaciones más usadas dentro de la Web 2.0 están los blogs, el Software Como Servicio (SaaS), los sitios wikis y las redes sociales.

3.2.4 Vulnerabilidades en redes sociales

Como es sabido, en la actualidad existen diversas redes sociales que permiten tener comunicación con todo el mundo (Figura 3.4). Hoy en día se han convertido en toda una moda y la cantidad de personas que hacen uso de por lo menos una de éstas redes es muy grande. Los empresarios y las organizaciones usan las redes sociales para tener contacto con sus clientes, así mismo todos los usuarios ven a estas redes como una manera de mantener a la gente informada al mismo tiempo que ellos se informan de todo lo que ocurre en el exterior.

Debido a la gran afluencia que tienen estas redes, es que los perpetradores actualmente las visualizan como el medio para la ejecución de una gran cantidad de ataques, aprovechándose de las vulnerabilidades que poseen y creando nuevas, para así poder cumplir sus objetivos.

La principal vulnerabilidad que poseen estas redes es la confianza que tienen los usuarios de las mismas, puesto que piensan que al tratarse de una red social, deben compartir cierta información que no deberían y de la cual se aprovechan los atacantes. Hoy en día es muy común el robo de información en redes sociales, en los cuales las criminales incurren a engaños con los que obtienen información directamente del usuario.

De acuerdo con el estudio Cisco 2010 Annual Security Report, los cibercriminales han comenzado a desarrollar modelos delictivos alrededor de redes sociales, teléfonos inteligentes y sistemas de control de infraestructura. "Los criminales web de la segunda década del siglo cuentan con una poderosa arma a su disposición: la capacidad de vulnerar la confianza. De una u otra forma han aprendido a convencer a los usuarios a confiar en ellos, a que los vean como sus amigos, a que den clic en cualquier liga, a que descarguen software sin cuestionarlo o incluso a que el mismo internauta sea el que les entregue su cuenta y clave de acceso", cita el reporte de Cisco. [19]

Las redes sociales son aplicaciones muy populares para los perpetradores debido a la gran afluencia que poseen. Facebook es la red social más utilizada a nivel mundial con más de 600 millones de usuarios, mientras que Twitter cuenta con más de 200 millones de seguidores.[20]

Esto ha ocasionado que inclusive en las áreas de trabajo de las empresas permitan su uso, existiendo casos en los que son tomadas como parte de los procesos laborales, lo que trae como consecuencia para la empresa, baja productividad, consumo de recursos de la empresa y sobre todo el uso inadecuado de la información que desencadena que se lleven a cabo los ataques de manera exitosa.

Figura 3.4 Redes Sociales

La mayoría de dichos ataques se ejecutan

[19] http://www.bsecure.com.mx/featured/mulas-smartphones-y-redes-sociales-las-preferencias-del-cibercrimen/

[20] http://www.bsecure.com.mx/featured/empresas-deben-estar-alerta-por-uso-de-redes-sociales-de-empleados/

mediante la ingeniería social, haciendo uso de temas que llaman la atención de los usuarios[21]. Una vez que los usuarios caen en el engaño, se les pide que autoricen diversos permisos para poder mostrar el contenido supuestamente ofrecido, cosa que el usuario realiza sin darle importancia y esto genera que la información se vea comprometida.

Esto está siendo muy preocupante en la actualidad para las empresas y organizaciones debido a que cuando los empleados realizan esto en algún equipo de la empresa, se inyecta el malware en el equipo y en ocasiones el atacante puede tener acceso no sólo a información personal de la víctima sino a datos corporativos.

Éstas son algunas de las vulnerabilidades de las redes sociales en cuestión de usuarios. Sin embargo, recientes ataques han evidenciado la existencia de la inseguridad en las mismas, cuestión que no depende solamente de los usuarios sino de los creadores de ellas.

Una encuesta realizada por la firma indicaba que 82% de los 1,200 usuarios encuestados consideran que Facebook es la red social más insegura. Twitter y MySpace obtuvieron 8% de las opiniones en ese sentido.[22]

3.3 Ataques más comunes

Algunos de los ataques que se presentan con mayor frecuencia y de los cuales no están exentos ninguna organización o usuario son:

[21] http://www.bsecure.com.mx/featured/empresas-deben-estar-alerta-por-uso-de-redes-sociales-de-empleados/

[22] http://www.bsecure.com.mx/ultimosarticulos/hackean-pagina-en-facebook-del-fundador-de-facebook/

3.3.1 Robo de identidad

Uno de los ataques más comunes a los que se enfrentan las personas son el robo de identidad. Este ataque se basa en la obtención de información personal y privada para después utilizarla con fines lucrativos o de usurpación, inclusive en actividades ilegales. Con esta información se pueden ejecutar diferentes acciones que causan un gran daño a la víctima como lo es el fraude.

Los casos más cotidianos que se presentan tienen que ver con las tarjetas de crédito y los delitos relacionados con éstas. Esto es debido a que los carteristas han logrado no sólo adquirir las tarjetas de sus víctimas sino que hoy en día logran descifrar datos relevantes que les permiten hacer uso de las mismas, lo que se convierte en un robo de identidad.

Un estudio a cargo de la firma de soluciones de seguridad financiera CCP indicó que los mexicanos no toman las medidas adecuadas para evitar ser víctimas de este tipo de ataques, lo que propicia que los perpetradores logren hacer cargos irregulares y los usuarios no se percatan de que han sido víctimas de un robo de identidad.

De acuerdo con los resultados presentados por CCP, otro de los factores que interfieren mucho en este tipo de ataques es el hecho de que los mexicanos no le dan la suficiente importancia a la seguridad de su información en internet, específicamente en las redes sociales que utilizan, y esto causa un riesgo más a su estabilidad financiera, debido a que es muy común que las personas hagan públicos sus datos personales en dichas redes.

Las cifras indican que 23% de la población mexicana hace públicos sus datos personales dentro de las redes sociales. También se destaca el envío de

información confidencial a través de la red. El estudio indica que 16% de los mexicanos utiliza su correo electrónico para enviar datos sensibles[23].

Estos datos resultan demasiado preocupantes, ya que esto hace que aumente la probabilidad de que la información sea interceptada y consecuentemente está expuesta a cualquier tipo de ataque.

Todo este robo de información es explotado por los delincuentes para abrir cuentas bancarias, solicitar préstamos y financiar vehículos, además de comprar bienes y servicios o incluso establecer contratos como la renta de una vivienda, todo esto bajo la identidad de otra persona, asegura la firma.

Cifras oficiales revelan que tan sólo en 2009 la cantidad de personas que sufrieron robo de identidad en México ascendió a 330,000[24].

Por otra parte, el "Reporte del Crimen en Internet 2010" indicó que el robo de identidad fue el tercer delito cibernético más reportado del 2010 en Estados Unidos, ocupando 10% de las más de 300,000 quejas que se realizaron en el país del norte a lo largo del año. [25]

3.3.2 Fuga de información

Otro ataque que está relacionado con el anterior es el robo de información. Existen diversas formas de ejecución de este ataque. Por ejemplo, algunas formas de conseguir dicha información se basa en el llenado de formatos de tarjetas de crédito o descuentos que les ofrecen a las personas muy frecuentemente y que en ocasiones son falsas o usan la información de

[23] http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion-deficientes-estudio/

[24] http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion-deficientes-estudio/

[25] http://www.bsecure.com.mx/featured/fraudes-en-linea-generan-en-eu-mas-de-300000-quejas-al-ano/

manera incorrecta. También es común que en diversos sitios de internet las personas realicen compras en línea y proporcionen datos sin verificar que el sitio en el que se encuentran es un "sitio seguro" o en ocasiones aunque el sitio sea seguro, la conexión no lo es y no se percatan que están siendo víctimas de una intercepción por medio de la red a la que se encuentran conectados; este tipo de ataques se realizan generalmente en redes públicas como son las de los cafés, restaurantes, aeropuertos y demás lugares que ofrecen conexiones gratuitas, esto implica que no piden una autenticación para conectarse por lo que cualquier persona puede hacerlo desde su equipo y en ocasiones ahí están presentes los atacantes.

Hoy en día gracias a la tecnología, los atacantes poseen diversas formas de realizar sus ataques y es posible que también realicen este tipo de ataques mediante la captura de pantalla y el teclado de los equipos mediante video. Debido a esto se logra informarse acerca de los movimientos que realizan las personas, así como ver claves y posteriormente acceder a datos.

La obtención de información también se realiza gracias a la obtención de contraseñas y claves de acceso, que es otro ataque muy común.

Las pérdidas generadas por las brechas de información durante 2010 alcanzaron $7.2 millones de dólares, un aumento de 7% con respecto a lo registrado en 2009, reveló un estudio a cargo del Instituto Ponemon y la firma de seguridad Symantec[26].

Las pérdidas de información pueden ser provocadas por distintas causas sin embargo, aquella provocada por un ciberataque es la que más costos genera a las organizaciones, cifras presentadas por Larry Ponemon revelan que cada documento robado a partir de un ciberataque tuvo un costo de $318 dólares.

[26] http://www.bsecure.com.mx/featured/brechas-de-informacion-aumentan-7-durante-2010-generan-perdidas-por-7-2-mdd/

Tanto el cibercrimen, como el robo de información son temas que tiene un mayor impacto en países desarrollados, esto se debe a que gran parte de las transacciones se realizan en línea.

Un reporte de McAfee, señaló que el cibercrimen es una industria que le cuesta, tan sólo a Estados Unidos más de $560 millones de dólares al año en reportes o reclamos de robo de información, de identidad o fraude por internet y es un sector que se cree genera más de $1 billón de dólares alrededor del planeta[27].

Si bien es cierto que los mecanismos de seguridad cada día mejoran, para lograr una mejor protección de la información también es una realidad que no garantizan al cien dicha seguridad. Ejemplo de esto es la nueva tecnología conocida como tokens de autenticación, los cuales son un mecanismo de seguridad utilizado por empleados de gobierno, empresas privadas y la industria bancaria. Sin embargo, como todos los mecanismos, no son totalmente seguros, por lo que el robo de información de los mismos podría comprometer los sistemas de protección de dichas instituciones.

3.3.3 Obtención de contraseñas

El ataque anterior va de la mano con la obtención de contraseñas, ya que si bien por una parte se considera como información una contraseña, también es verdad que con dicha palabra logran obtener la demás información o bien la obtención de la contraseña es sólo el inicio de un ataque planeado de mayor gravedad.

Esto se puede realizar mediante distintos métodos, de acuerdo con la facilidad que proporcione el usuario; es decir, si es un usuario demasiado descuidado, será fácil obtener las claves de acceso al revisar el escritorio o

[27] Ídem

monitor donde trabaja. De lo contrario existen otros métodos para la obtención de contraseñas como puede ser un keylogger o un exploit.

Una vez que se cuenta con estas contraseñas es común que los atacantes procedan a navegar por la información y explotar aquella que sea relevante.

3.3.4 Infecciones

Es uno de los ataques más comunes y a los que todos los usuarios se enfrentan todos los días en cualquier equipo. Las infecciones por virus, troyanos, malware, gusanos, bombas lógicas, entre otros programas que están diseñados para causar algún tipo de daño en los sistemas y de los que puede un usuario ser víctima, son algo de todos los días y es muy difícil estar exentos de ellos debido a la gran variedad que existe. (Figura 3.5)

El medio más común por el cual se llevan a cabo las infecciones es mediante la descarga de archivos de internet o al abrir un correo electrónico infectado. En realidad para poder ejecutar dicho ataque basta con tan sólo hacer una búsqueda en internet, ya que en automático aparecen sitios que invitan a los usuarios a descargar canciones, instalar programas, ringtones para celulares, videos y demás atracciones para los usuarios y en realidad lo que hacen sin darse cuenta es descargar algún código malicioso.

La creación y distribución del malware aumentó de forma muy notable en el 2010. De hecho, en los 12 meses del 2010 se generó el 34% de todos los virus que los expertos en seguridad han identificado en la historia. Según los datos de PandaLabs, el 99.4% de las nuevas amenazas recibidas ha alcanzado 134

millones de ficheros diferentes, más de 60 de los cuales son malware (virus, gusanos, troyanos y otras amenazas informáticas).[28]

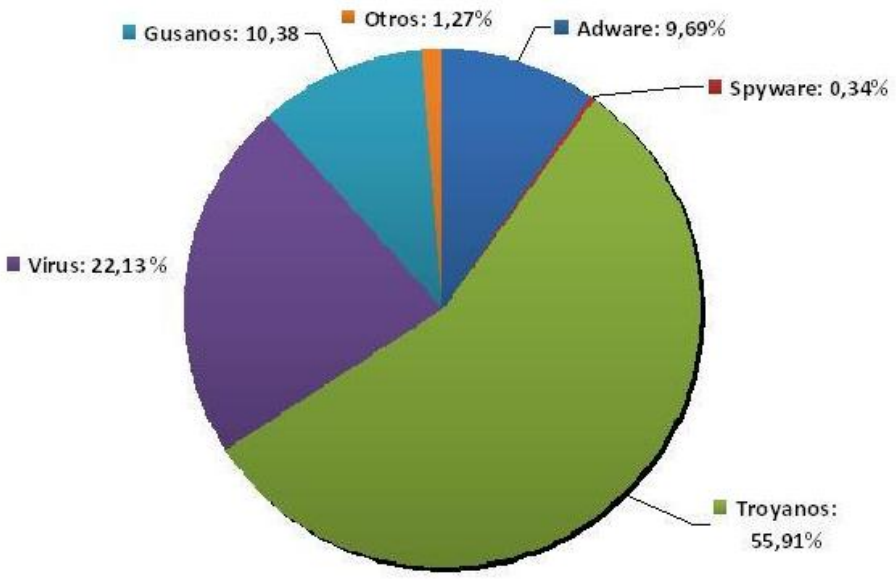


Figura 3.5[29] Amenazas Informáticas

Un ataque que actualmente ha crecido de manera muy rápida es el conocido como rogueware o scareware.

Rogueware

Este ataque consiste en ofrecer a los usuarios ciertas soluciones de antivirus que en realidad están diseñadas para obtener dinero, ya que se les cobra por la adquisición de dichos antivirus. Básicamente lo que los atacantes hacen es identificar ciertas "amenazas" en los equipos que en realidad no existen, y de este modo les ofrecen una solución a su "problema". Los estafadores se aprovechan del miedo de los usuarios de una posible infección, por lo que

[28] http://www.theinquirer.es/2011/01/03/la-tercera-parte-de-todos-los-virus-de-la-historia-se-han-generado-en-2010.html

[29] Ídem

creen que en realidad necesitan comprar dicho programa de Antivirus, pero en realidad se trata de un malware.

Diversas firmas de seguridad estiman que los rogueware han crecido exponencialmente en los últimos cuatro años, al pasar de menos de 25 muestras a más de 661 tipos de scareware, circulando por la web.[30]

3.3.6 Spam

Este término es utilizado para nombrar a toda aquella información y datos que no son de utilidad para los usuarios u organizaciones. Actualmente se tiene un serio problema en seguridad informática relacionado con el Spam y son las conocidas redes "botnet".

Botnet es un término referente a ciertos robots informáticos o bots, los cuales se ejecutan de manera autónoma y automática, además de que puede controlar todos los ordenadores/servidores infectados de forma remota.

Lo que se hace en la actualidad es utilizar las redes Botnet para enviar Spam a direcciones de correo electrónico y realizar ataques de tipo DDoS.

El reporte titulado "La economía subterránea del Spam" indica que en sólo un año la red botnet logró generar más de 4 millones de perfiles apócrifos desde los cuales envió más de 1.7 billones de correos electrónicos con spam.[31]

De acuerdo con dicho estudio, el 30% de los correos electrónicos enviados por redes botnet es entregado exitosamente.

[30] http://www.bsecure.com.mx/featured/musica-cine-tecnologia-y-ciberamenazas-en-el-sxsw/

[31] http://www.bsecure.com.mx/featured/cutwail-revive-la-red-botnet-responsable-de-mas-de-4-millones-de-perfiles-apocrifos/

El proveedor de seguridad de MessageLabs estima que el tamaño total de la botnet fue alrededor de 1.5 a 2 millones de ordenadores individuales, capaz de enviar 74 mil millones de mensajes spam por día o 51 millones cada minuto.[32]

Durante 2010 las víctimas de estas redes han aumentado 654% siendo el cierre del año el periodo en el que estas amenazas fueron más activas, reveló un estudio realizado por la compañía de seguridad Damballa.[33]

Lo que más preocupa a los expertos en seguridad, no son precisamente las cifras, sino que el 60% de las redes botnet incluidas en el conteo de las 10 más poderosas no existía en 2009.

	Botnet en 2010	Porcentaje de víctimas	Posición en el 2009
1	TDL Botnet A	14.8%	--
2	Rogue AV Botnet	5.7%	--
3	Zeus Botnet B	5.3%	--
4	Monkif	5.2%	5°
5	Koobface. A	4.0%	<top 10
6	Conficker. C	2.8%	< top 10
7	Hamweq	2.5%	--
8	Adware Trojan Botnet	2.2%	--
9	Sality	2.1%	< top 10
10	Spy Eye Botnet A	1.9%	--

Tabla 3.1: Ranking completo de las 10 botnet más poderosas de 2010 [34]:

[32] http://msmvps.com/blogs/harrywaldron/archive/2010/02/02/pushdo-botnet-new-ddos-attacks-on-major-web-sites.aspx

[33] http://www.bsecure.com.mx/ultimosarticulos/las-10-botnet-mas-poderosas-de-2010/

3.3.7 DDOS

Se le conoce con este término a todos aquellos ataques de denegación de servicio. Estos ataques se realizan a redes completas por lo que el servicio o recurso que proveen se vuelve inaccesible para todos aquellos usuarios del mismo. Actualmente está siendo muy popular este tipo de ataques debido al aumento del hacktivismo a nivel mundial, principalmente por la presencia de Anonymous, representante principal de este movimiento.

Durante la primera parte de 2011 el porcentaje de este tipo de ataques aumentó 22% respecto a lo registrado en el mismo periodo de 2010, reveló un estudio a cargo de la firma de seguridad Trustwave. La empresa señala que los ataques DDoS ocuparon 32% del total de los embates registrados durante la primera parte del año, seguido por la inyección de SQL con 21% y los ataques XSS con 9%.[35]

En México recientemente el sitio de la empresa de noticias MVS fue derribado por un grupo de internautas llamado Operación Tequila. El motivo del ataque fue el despido de la periodista Carmen Aristegui, conductora del programa radiofónico Primera Emisión de la empresa MVS Radio. El grupo invitó a través de su perfil de Facebook a los usuarios que desearan sumarse al ataque de manera voluntaria la información referente al horario, los sitios, las direcciones IP y el método o programa a utilizar para formar parte del ataque.[36]

En marzo del año en curso, los servidores de la plataforma de blogs WordPress fueron víctimas del mayor ataque de Denegación de Servicios (DDoS) en su historia. Esto fue anunciado por la propia empresa mediante su cuenta de Twitter.

---

[34] http://www.bsecure.com.mx/ultimosarticulos/las-10-botnet-mas-poderosas-de-2010/

[35] http://www.bsecure.com.mx/featured/ataques-ddos-crecen-22-durante-2011-estudio/

[36] http://www.bsecure.com.mx/featured/ataques-ddos-crecen-22-durante-2011-estudio/

Como es de esperarse, una amenaza o vulnerabilidad van de la mano con uno o varios ataques, así mismo los ataques en ocasiones se relacionan entre sí. Ejemplo de esto es el hacktivismo y los ataques DDOS.

3.3.8 Hacktivismo

Como es sabido por la mayoría de los usuarios de internet, el hacktivismo está muy de moda y los hacktivistas se han involucrado en una serie de ataques informáticos que han ocasionado grandes pérdidas.

Ejemplo de este tipo de ataques es el ya conocido en México contra la empresa de MVS a causa del despido injustificado de la periodista Carmen Aristegui. Como ya se mencionó, los móviles de estos atacantes son ideologías, por lo que este despido generó gran inconformidad entre el público en general, y ocasionó el movimiento de los atacantes conocido como Operación Tequila.

Esta operación consistió en un Ataque de Denegación de Servicio Distribuido a los servidores de multivisión.[37]

Luego de dicho ataque, un nuevo grupo de activistas digitales en el país, conocido como Operación México, amenazó con atacar de la misma manera el sitio web de la Presidencia de la República, el de la Secretaría de Comunicaciones y Transportes y el de la Secretaría de Hacienda y Crédito Público.

En los países del medio oriente, el hacktivismo y los movimientos en las redes sociales han logrado lo increíble, remover malos gobernantes, iniciar movimientos ciudadanos, atraer la atención del mundo a sus geografías.[38]

Actualmente quien encabeza la lista de hacktivistas es el grupo conocido como Anonymous, quien como ya se mencionó, ha sido el autor de diversos

[37] http://www.bsecure.com.mx/opinion/hackivismo-como-para-que/
[38] Ídem

ataques, además de apoyar a Wikileaks, que era un sitio que distribuía miles de cables diplomáticos de las embajadas estadounidenses. La publicación ha sido catalogada como la filtración gubernamental más grande de la historia, por lo que fue censurado y Anonymous está en contra de eso.

Anoymous también es responsable de embates contra los gobiernos de Egipto, Túnez y Zimbabwe, el grupo justificó dichos ataques al señalar que los gobiernos de dichos países no permiten el uso de internet de manera abierta.

El éxito que ha tenido Anonymous se debe a que el grupo permite que cualquier usuario se sume de manera voluntaria a su ejército en línea. La red de hacktivistas puso a disposición de los internautas una herramienta para que éstos formen parte de una red botnet, la cual es utilizada para llevar a cabo los ataques DDoS.

Un reporte indicaba que en diciembre pasado el ejército de Anonymous había superado los 50,000 usuarios en menos de una semana. [39]

3.3.9 Ataques a dispositivos móviles

Era de esperarse que con el cambio de las tecnologías existan cambios también en los medios de ataque de los perpetradores. Con el avance de la tecnología y la aparición de los Smartphones (teléfonos inteligentes) y demás dispositivos móviles, los atacantes han comenzado a dirigirse a este mercado para el robo de información. Están comenzando a mirar este nicho como un mercado de oportunidad para el robo de información. Esto se debe a que ya comienzan a dejarse atrás las computadoras de la preferencia del consumidor.

[39] http://www.bsecure.com.mx/featured/ataques-ddos-crecen-22-durante-2011-estudio/

Cisco destaca que la International Telecommunications Union (ITU) estima que el 2010 cerró con más de 5,000 millones de usuarios de telefonía móvil alrededor del mundo y cerca de 1,000 millones de éstos son usuarios de teléfonos inteligentes.[40]

Algunos de los sistemas operativos de estos dispositivos como son Andriod, iOS, Symbian y Windows Phone 7 ya han presentado vulnerabilidades en su estructura y Cisco espera que existan más.

Uno de los recientes ataques en este ámbito fue el ejecutado en contra de los usuarios de Android. Recientemente Google informó que habían sido eliminadas 50 aplicaciones maliciosas de su tienda en línea, las cuales infectaron más de 260,000 equipos en tan sólo una semana, reveló la empresa. Las aplicaciones maliciosas eliminadas por Google eran capaces de robar el IMEI e IMSI de cada celular, además de identificar el país al que pertenecía la línea telefónica, así como el idioma y el ID de los dispositivos, afirmaron medios especializados.[41]

Estas aplicaciones se basan en el requerimiento de permisos por parte de los usuarios, con los que logran controlar los mismos y generan cargos a las cuentas de las víctimas, ya que una vez que la aplicación se encuentra cargada en el dispositivo, se comienzan a enviar mensajes multimedia sin que el usuario se dé cuenta, sino que se percata de los cobros después de que el daño ya ha sido causado.

Un ejemplo del cambio de los atacantes de la PC a los móviles es la versión de Zeus hecha para correr sobre los sistemas operativos Windows OS, Windows Mobile y Symbian.

---

[40] http://www.bsecure.com.mx/featured/mulas-smartphones-y-redes-sociales-las-preferencias-del-cibercrimen/

[41] http://www.bsecure.com.mx/featured/aprovechan-actualizacion-de-seguridad-para-reinfectar-a-usuarios-de-android/

De acuerdo con Kaspersky, la versión móvil de Zeus operaba de la misma manera que Zitmo. Se les solicita ingresar el número y modelo de su teléfono inteligente, para una supuesta "verificación de certificado". Posteriormente el usuario recibe un mensaje de texto con un hipervínculo o URL, el cual contiene la descarga del certificado, que en realidad contiene la versión del código malicioso para su Smartphone.[42]

Finalmente Apple y su iOS no se encuentran libres de ataques. Recientemente fue detectada una vulnerabilidad en su sistema, la cual permite robar las contraseñas y datos del iPhone4.

Esto ha generado que las compañías fabricantes de dispositivos móviles busquen desarrollar equipos con protección propia y no estén a expensas de aplicaciones independientes y sistemas de protección externos.[43]

3.3.10 Recientes ataques a redes sociales

Como ya se mencionó, actualmente es muy común el uso de este tipo de redes, por esta razón es que los atacantes recientemente han recurrido a hacer uso de las mismas para ejecutar diversos ataques.

Actualmente existen diferentes amenazas que atentan contra las distintas redes sociales y cada día se desarrollan nuevos ataques en contra de las mismas.

Una reciente amenaza relacionada con Facebook actualmente está latente. Ésta consiste en un correo electrónico por medio del cual se les informa a los usuarios de un supuesto cambio de contraseña de su cuenta. El correo indica

[42] http://www.bsecure.com.mx/ultimosarticulos/los-bancos-podrian-ser-vulnerados-por-medio-de-ingenieria-social/

[43] http://www.bsecure.com.mx/ultimosarticulos/los-bancos-podrian-ser-vulnerados-por-medio-de-ingenieria-social/

que debido a que la contraseña del usuario es insegura, ésta tuvo que ser modificada de manera automática por los sistemas de protección de la red social.[44] En dicho correo les adjuntan la nueva contraseña y las medidas de seguridad que deben seguir y cuando descargan el archivo, el equipo del usuario se infecta con un malware llamado Mal/Zbot-AV que es muy usado en ataques de ingeniería social.

Otro ataque actual igualmente a esta red social es una invitación a los usuarios a que visiten un sitio mediante el cual podrán saber quién visita su perfil. Las indicaciones que se dan son acceder al sitio "espiaface.com" para posteriormente abrir el sitio de Facebook en una nueva ventana, tras esto se debe reemplazar en la barra de navegación la dirección de la red por cierto código. Lo que el usuario realmente no sabe es que está cargando una aplicación externa que contiene código malicioso y que hace solicitud de permisos de la cuenta del usuario con los que toma el control de la cuenta.

Lo que realiza la aplicación es enviar la invitación al evento "Averigua quién visita tu perfil" a cada uno de los contactos del usuario engañado, de esta manera la amenaza se distribuye velozmente dentro de la red social.[45]

Otro ataque muy común aunque no todos los usuarios se percatan de él, es el hackeo de las cuentas. Recientemente la página de Facebook de Mark Zuckeberg, creador de la compañía, fue hackeada por un fan que lo confrontó en cuanto a cómo opera el modelo de financiamiento de la red social. El atacante colocó un mensaje apócrifo, como si fuera el mismo Zuckerberg, retándolo a obtener financiamiento de los usuarios y no de capitales privados, de una forma social.[46] Estos ataques no son raros, y se ha hablado acerca de la inseguridad de la red social, sin embargo, Facebook ignoró dichas

[44] http://www.bsecure.com.mx/featured/facebook-infecta-usuarios-a-traves-de-correo-electronico/

[45] http://www.bsecure.com.mx/featured/averigua-quien-robo-tu-cuenta-en-facebook/

[46] http://www.bsecure.com.mx/ultimosarticulos/hackean-pagina-en-facebook-del-fundador-de-facebook/

recomendaciones diciendo que la compañía trabajaba para mantener seguros tanto a sus usuarios como a la red misma. Aunque con estos ataques queda evidenciada la inseguridad de la red.

Twitter también ha sido víctima de diversos ataques. Uno de los más recientes es la distribución de un falso antivirus. Se trata de un ataque que utilizaba el servicio de acortamiento de direcciones web de Google para ocultar el destino de los links.[47] Los enlaces enmascarados dirigen al usuario a un dominio de máximo nivel de Ucrania que, a su vez, lo redirige a una dirección IP asociada a otras estafas de software antivirus, según explica Nicolas Brulez de Kaspersky Lab en un blog corporativo.

Como conclusión se puede mencionar que de acuerdo con diversos estudios que han realizado las diferentes empresas de seguridad en tecnologías de la información, los medios elegidos para la distribución de malware en 2010 han sido las redes sociales. Igualmente concuerdan los expertos en que conforme la tecnología avanza, los perpetradores se están mudando a los dispositivos actuales, pasando de la computadora a los teléfonos y demás dispositivos móviles. Cabe destacar que este mismo año se ha dado el posicionamiento de falsas webs (llamado BlackHatSEO) y el aprovechamiento de vulnerabilidades zero-day.

También es importante señalar que en el 2010 se están viendo mayor cantidad de hechos relacionados con la ciberdelincuencia y el ciberactivismo y se espera que la tendencia continúe hasta el 2011, según los expertos.

[47] http://www.idg.es/pcworldtech/Twitter_-amenazado-por-una-estafa-de-falso-antivir/doc105175-actualidad.htm

Capítulo 4: Usuarios: Principal amenaza en seguridad informática

4.1 Nivel de conocimiento en seguridad informática por parte de los usuarios

En la actualidad, cada usuario tiene ciertos conocimientos acerca del equipo de cómputo que maneja. Estos conocimientos van desde el sistema operativo que maneja, la paquetería y equipo de hardware con el que interactúa. Sin embargo, la mayoría de las personas no tienen conocimiento acerca del mantenimiento que le deben dar a sus equipos y sobre todo no conocen las medidas necesarias que deben tener para mantenerlos protegidos ante cualquier tipo de ataque.

En las organizaciones o empresas los empleados están acostumbrados a hacer uso de sus equipos computacionales única y exclusivamente para la realización de sus actividades laborales y personales. En caso de tener algún problema con dicho equipo, llaman al personal de soporte técnico para que les resuelva su problema y se evitan cualquier complicación que pudieran tener.

En el hogar y en general en la vida cotidiana de las personas dueñas de algún equipo de cómputo, los usuarios se limitan en su mayoría, a hacer uso de sus computadoras para la realización de sus tareas y actividades, sin tomarse la molestia de aprender un poco acerca de las medidas que deben tomar para mantener sus equipos en un estado óptimo. Simplemente cuando sus equipos no funcionan, llaman al técnico, quien se encarga de solucionar sus problemas.

Hoy en día, se dice que quien no tiene conocimientos en computación es prácticamente un analfabeta, por lo que en las escuelas de educación básica y educación media, se brindan cursos de cómputo para todos los alumnos.

Sin embargo, pese a que ya es considerado como obligatorio la enseñanza de conocimientos en computación en la educación mexicana, la realidad es que actualmente aún son muy limitados los recursos para la enseñanza de la computación en las escuelas públicas de la República Mexicana, y aunque existe un reconocimiento creciente de la importancia de impulsar el aprendizaje masivo de dicha área, "hay mucho por hacer en materia de

objetivos, planes de estudio, recursos disponibles, uso de estándares comunes y disminución de la disparidad dentro del sistema educativo".

Así lo consideró el investigador Ricardo Estrada, del Centro de Investigación para el Desarrollo A.C. en su trabajo "Inglés y Computación en México: Déficit y Brecha de Habilidades". [95]

El avance más importante en materia de educación, con respecto al área de computación es la llamada Enciclomedia, la cual es calificada como el programa federal "más ambicioso" para la incorporación de tecnologías de información al proceso educativo. Actualmente, se encuentra presente en alrededor de 150 mil aulas de escuelas públicas de un total de 200 mil. [96]

Considerando que aún existe mucho déficit en cuanto a la enseñanza de la computación básica, qué decir de la seguridad informática, la cual es una rama ya más específica de la computación y de la cual no se habla en las aulas de educación de hasta el nivel medio superior.

Por otra parte, resulta demasiado común que se brinde una gran cantidad de cursos de computación e informática, en diferentes escuelas especializadas en el tema.

Sin embargo, pese a todo esto, el tema de seguridad informática, no es un tema tan difundido como son las matemáticas, la literatura, e inclusive la computación como tal. Cuando las personas acuden a una escuela de computación para adquirir conocimientos sobre el tema, generalmente estos cursos se limitan a la enseñanza del manejo de algún sistema operativo, regularmente Windows que es el más comercial, manejo de internet, paquetería igualmente comercial como office, un poco de lenguajes de programación y ensamblado de computadoras. Ya en caso de que se necesite aprender un software específico o conocimientos más profundos, se debe recurrir a cursos especializados, los cuales generalmente quien recurre a

[95] http://www.oem.com.mx/laprensa/notas/n1085982.htm
[96] Ídem

ellos es porque sabe sobre el tema, es decir, tiene estudios en alguna carrera relacionada con la computación como lo es la informática, ingeniería en sistemas o en computación y ciencias de la computación, por lo que posee conocimientos acerca del tema y toma cursos de su interés o que le ayudarán en su nivel profesional; o también se dan los casos en los que los cursos se tomen debido a que se trate de una persona que tal vez no tenga estudios en el área, pero que su profesión se lo exija o que lo requiera en su empleo, como son aquellos casos en los que una empresa capacita a sus propios usuarios para un mejor desempeño de la misma. Por consiguiente, es muy poco común que se presenten los casos en los que un usuario común de cualquier equipo de cómputo diga: "Deseo o voy a tomar un curso de seguridad informática".

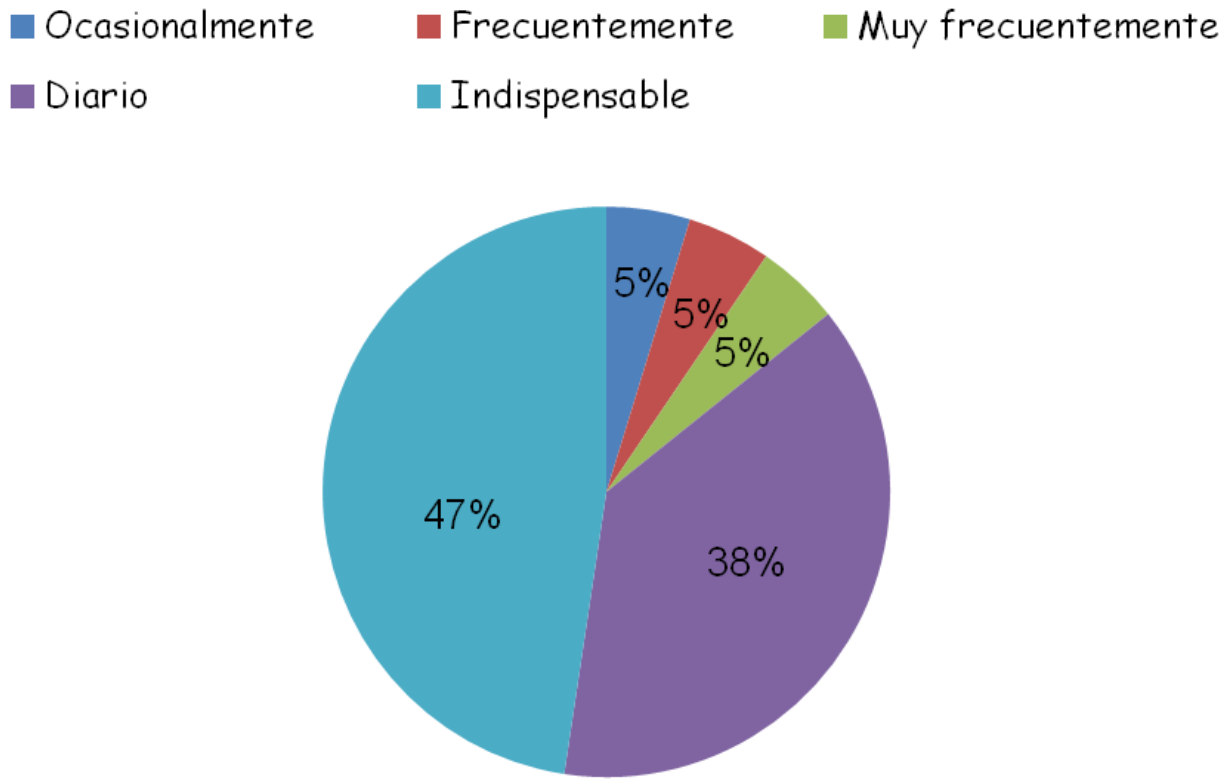
Esto se debe quizá a que las personas que no se dedican al área no tengan interés en aprender ese tipo de conocimientos, sin embargo, si se considerara que existen ciertas cuestiones que toda persona debería saber acerca de la seguridad informática, conceptos, medidas básicas de prevención y de detección, se podrían ahorrar gran cantidad de problemas que muchas veces inician como mínimos y que por descuidos o no tratarlos de inmediato, derivan en grandes fallas informáticas.

Como parte de la investigación correspondiente al tema abordado en esta tesis, se realizó una encuesta acerca del tema de seguridad informática, en la cual se cuestionaba a las persona de asuntos básicos del tema, es decir, sólo se preguntaron puntos que en teoría o a consideración de esta investigación todo usuario debería conocer y con lo cual podría mantener sus equipos en un estado relativamente protegido, al menos de las amenazas más simples a las que puede estar expuesto un bien informático.

Dicha encuesta se aplicó a una cantidad de 210 personas de una edad de entre 15 y 50 años, todas ellas son o han sido usuarios en cierto momento de un equipo de cómputo y las áreas en las que se desempeñan los encuestados son muy variados, esto se hizo con la finalidad de conocer el uso que le dan a sus bienes informáticos las personas en general y no usuarios específicos.

Con la elaboración de las encuestas[97] se obtuvieron los siguientes datos:

El 47.61% de los encuestados consideran a los equipos informáticos como algo imprescindible en su vida cotidiana, el 38.09%, si bien no es imprescindible, sí los utilizan prácticamente diario y el resto hacen uso de dichos equipos de manera menos frecuente, sin embargo, no hubo una sola persona que afirmara no hacer uso de ellos. Como puede verse, es un hecho real que hoy en día es de suma importancia el uso de este tipo de herramientas para la elaboración de las actividades diarias de las personas, por lo prácticamente todas las personas hacen uso de estos bienes. (Gráfica 4.1)



Gráfica 4.1: Uso de los equipos informáticos por parte de los usuarios

[97] Véase el cuestionario del anexo 1

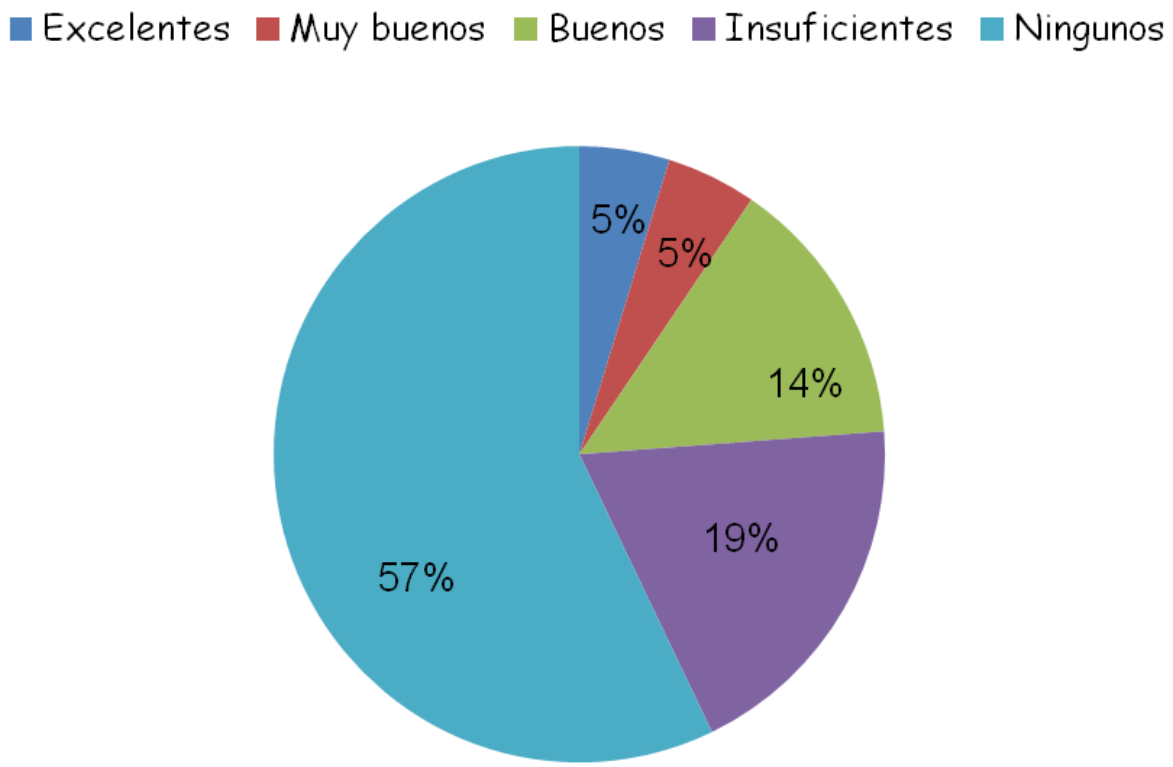
El uso que se le da a dicha tecnología es muy variado, va desde el uso para el trabajo o escuela hasta el uso personal, de comunicación y diversión. Sin embargo, sea cual sea el uso que se le dé, se deben conocer las medidas mínimas que se necesitan para la protección de estos activos y de este modo minimizar al máximo los riesgos que éstos poseen.

Para visualizar un poco el grado de importancia que tiene el hecho de educar a las personas en cuestiones de seguridad informática, se pueden mencionar algunos de los resultados que se obtuvieron al realizar las encuestas, para brindar a grandes rasgos una idea de la poca importancia que los usuarios le dan a la seguridad por la falta de conocimientos en el ámbito.

El 85.71% de los encuestados han tomado algún curso de computación ya sea a nivel curricular o externo. De estas personas, la mayoría dice tener únicamente conocimientos firmes en el manejo de Windows, Office e Internet. Otros pocos que están relacionados profesionalmente con la computación o las ingenierías tienen conocimientos en lenguajes de programación, reparación de computadoras y otros sistemas operativos y paqueterías. Sin embargo, únicamente el 9.52% afirmó tener conocimientos sólidos en seguridad informática, el 14.28 están informados sobre el tema en un nivel medio, el 19.04% sabe algo del tema pero considera que son conocimientos insuficientes, y el 57.14% no tiene conocimientos al respecto. (Gráfica 4.2)

Por obvias razones esto es importante mencionarlo, pues considerando que el total de los encuestados hacen uso de la tecnología informática, resulta alarmante que más de la mitad de ellos no sepan en lo mínimo la forma en que deberían cuidar sus bienes y si se considera que de los encuestados el 33.33% tienen estudios en alguna carrera relacionada con la computación, el resultado se agrava, pues si se suma el porcentaje de los que poseen conocimientos sólidos en seguridad informática y los que están informados a nivel medio, se obtiene el 23.8% del total de los encuestados. Esto quiere decir que ni siquiera los usuarios que se involucran directamente en la

computación poseen los conocimientos adecuados en seguridad informática, por lo que desde ahí se tiene una deficiencia notable.



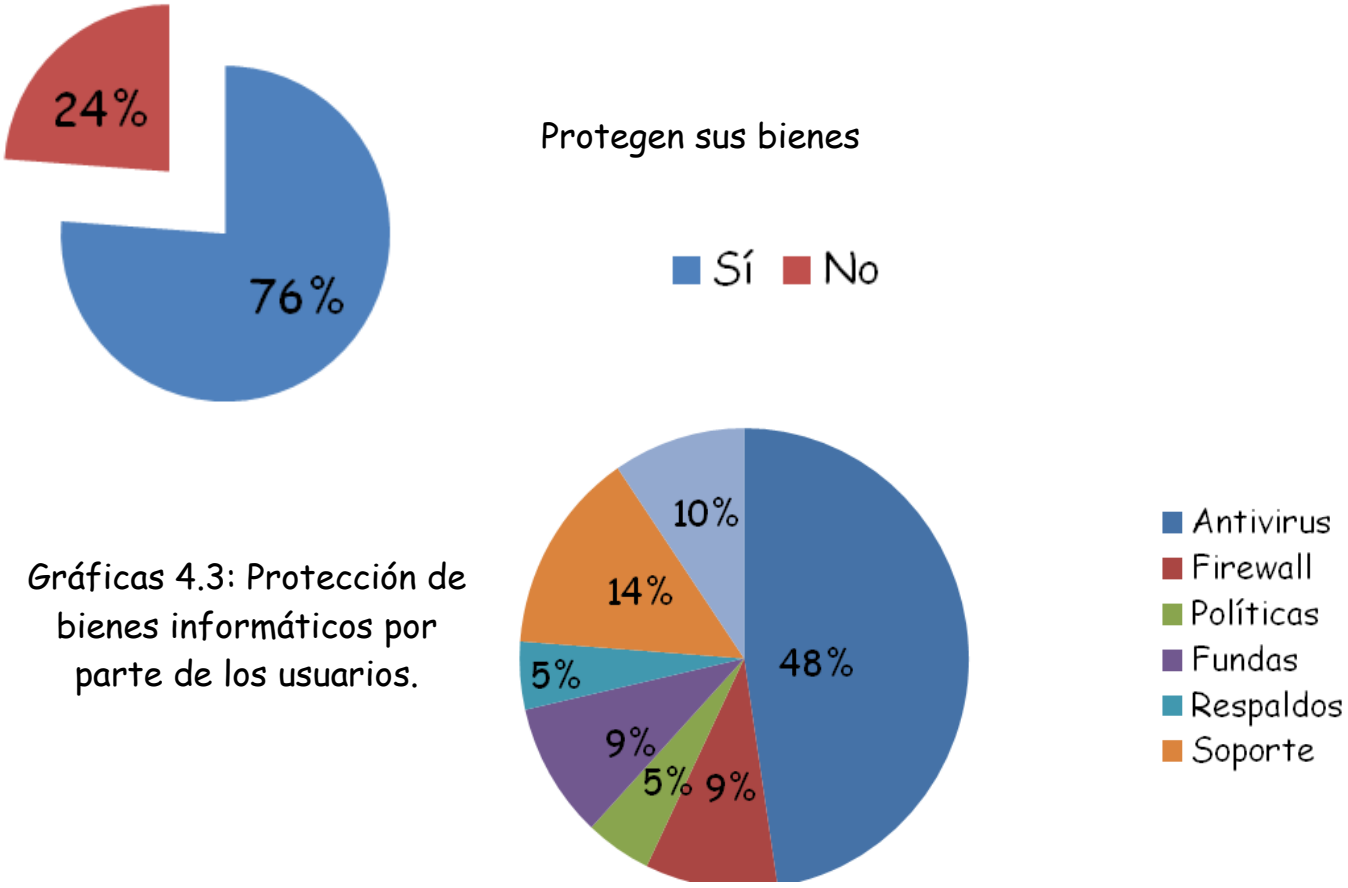
Gráfica 4.2: Conocimientos de los usuarios en seguridad informática.

Continuando con las estadísticas, se encontró que el 80.95% hacen uso de una PC o laptop, y el 95.23% hace uso del internet y el 90.47 de los teléfonos celulares. Esto es muy común y son resultados esperados, pues son las herramientas tecnológicas de mayor uso en la actualidad, sin embargo, no se debe olvidar que por lo mismo, son los medios más utilizados para la ejecución de ataques informáticos.

Por otra parte, en cuestiones de medidas de seguridad, al preguntarle a los usuarios los métodos que utilizan para la protección de sus bienes, el 47.61% de los usuarios limita el cuidado de los equipos a un antivirus, además que de este porcentaje el 10% admitió tener caducada dicha herramienta.

Salvo los usuarios que cuentan con el antivirus pero no lo tienen activado, el resto usa una medida básica de seguridad muy necesaria, pero como pudo verse en el transcurso de este trabajo, con la implementación de un antivirus sólo se logra el control de la seguridad en un aspecto y no de manera completa, por lo que es importante enseñar a los usuarios las demás medidas que deben tomar, así como las buenas prácticas que deben tener.

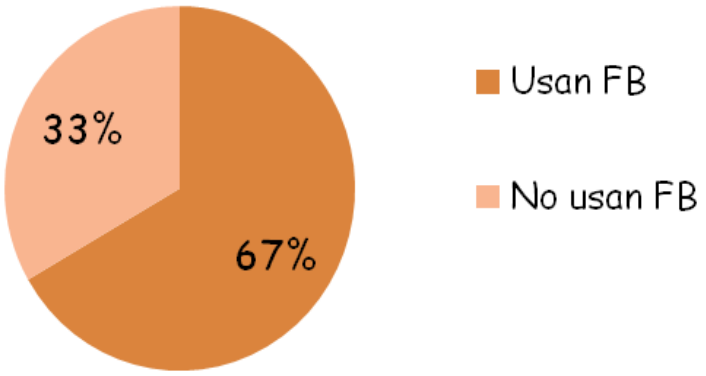
De acuerdo con la encuesta, otras herramientas que utilizan como medida de protección son: contraseñas, firewall y soporte técnico 14.28%, fundas y antispyware 9.52% y políticas de seguridad 4.76%. Estos porcentajes son bajos, considerando que son medidas consideradas igualmente básicas y a las que la mayoría de los usuarios debería recurrir. Sin embargo, también es importante mencionar que en esta parte de la encuesta, el 23.8% simplemente no hace nada para proteger sus bienes (Gráfica 4.3).

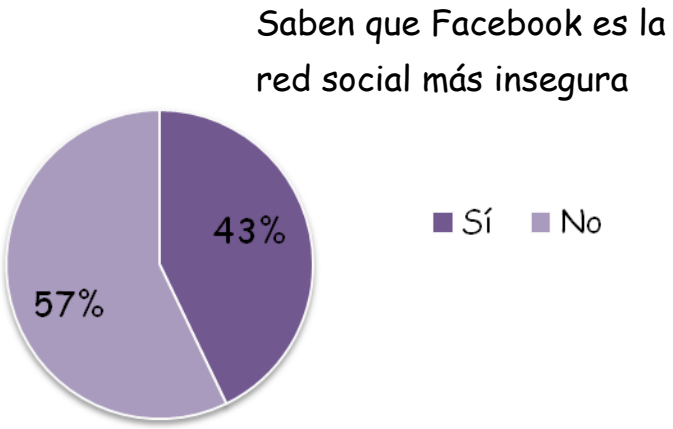


Gráficas 4.3: Protección de bienes informáticos por parte de los usuarios.

Otro dato que resultó muy interesante para este trabajo es el relacionado con las redes sociales y específicamente con Facebook. Dicha encuesta arrojó que del total de los encuestados 66.66% hace uso de la red social, y el 57.14%, admitió no tener conocimiento alguno acerca de que dicha red social es la más insegura que existe en la actualidad (Gráfica 4.4).

La inseguridad de dicha red social se debe a que por lo mismo que es la más utilizada, los atacantes buscan la forma de vulnerarla y realizar ataques usando de por medio a dicha red. Actualmente más de 600,000 cuentas de Facebook son comprometidas por medio de aplicaciones maliciosas que buscan obtener información confidencial de los internautas, reveló la red social a través de su blog oficial. [98]





Gráficas 4.4: Uso y conocimiento de la seguridad de Facebook.

[98] http://www.bsecure.com.mx/featured/diariamente-son-hackeadas-600000-cuentas-de-facebook/

Como ya se había mencionado, el 47.61% de los usuarios comentaron hacer uso del antivirus como medida de seguridad para sus equipos, sin embargo, pese a este resultado, al preguntar específicamente sobre si contaban con dicha herramienta, se obtuvo que el 85.71% de los usuarios, sí tienen un antivirus instalado, lo que deja una brecha de información al pensar que quizá el 38.1% de diferencia, no conocen la importancia o utilidad del antivirus. Lo mismo sucede con el caso de las contraseñas, ya que como se mencionó, sólo el 14.28% indicó el uso de éstas como medida de seguridad, mientras que la encuesta arrojó que realmente el 66.66% de los usuarios hacen uso de ellas.

Todos estos datos refleja la falta de educación que se tiene sobre el tema, pues se puede ver que gran parte de las personas no saben la importancia ni la utilidad de las herramientas de seguridad, o lo que es peor, no saben que deben proteger sus bienes.

Lo mismo ocurre con la siguiente información obtenida de la encuesta:

El 52.38% de los encuestados afirmó hacer uso del correo electrónico para enviar todo tipo de información y el 66.66% envía mensajes personales, puntos que resultan críticos tomando en cuenta la enorme cantidad de perpetradores que se encuentran a la expectativa para ejecutar un robo de información o interceptar los canales de comunicación. Del mismo modo ocurre con las redes públicas que existen en los diferentes lugares como son cafeterías, aeropuertos y plazas comerciales, ya que 47.61% de los usuarios encuestados afirmó hacer uso de estas redes y admitieron que las usan del mismo modo que las redes privadas como son las de su casa u oficina. Esto resulta preocupante pues dichas redes son muy inseguras y son frecuentemente utilizadas para la ejecución de gran variedad de ataques informáticos, por lo que los usuarios deben saber acerca de los cuidados que son indispensables al hacer uso de dichos recursos.

Por otra parte, se les cuestionó a los usuarios acerca de un conjunto de términos relacionados con la seguridad informática. De dichos términos el

total de los encuestados tiene conocimiento sobre los virus informáticos, más de la mitad de ellos conoce o ha escuchado hablar sobre lo que son los privilegios, conexión no segura, malware, hacker, cracker, spam, gusano, troyano, denegación de servicio, ataque informático y keylogger. Sin embargo, el 80.95% no sabe lo que es el carding y desconoce el término exploit; el 57.14% no sabe lo que son los perpetradores ni la ingeniería social.

Se puede considerar que quizá dichos términos no son muy comunes, sin embargo, si se toma en cuenta que hoy día, los fraudes y delitos relacionados con las tarjetas de crédito son muy frecuentes, los exploits son herramientas muy usadas para la obtención de contraseñas y la ingeniería social se está convirtiendo en el medio más utilizado para la ejecución de delitos informáticos, se puede visualizar la importancia que tiene el hecho de que los usuarios tengan conocimiento acerca de dichos términos y la manera de protegerse de ellos.

Sobre los servicios de seguridad, la mayoría de los usuarios considera de suma importancia contar con la confidencialidad y la autenticación y minimizan el resto de los servicios y únicamente el 4.76% indicó que se debe contar con los 6 servicios de seguridad que existen.

Finalmente el 23.8% admitió que la principal causa de los ataques informáticos es la falta de conocimiento por parte de los usuarios en el tema. El 28.57% sabe que el término "seguridad informática", se refiere a la protección de los bienes informáticos, el 38.09% limita el concepto a la protección de la información y un dato que llamó mucho la atención es que al preguntar sobre dicho término el 4.76% dijo que era algo que no existía.

Continuando con los conocimientos en el tema, se encuentran las áreas de IT de las dependencias. En teoría, dichas áreas deberían estar muy bien preparadas en cuestiones de seguridad y de este modo evitar o resistir a los ataques informáticos. Sin embargo, en la mayoría de las empresas en México no hay presupuestos para ciberseguridad y, en las que hay, éste es muy

pequeño. Los trabajadores que ahí laboran en su mayoría son becarios o recién egresados que no cuentan con la experiencia necesaria para implementar las medidas adecuadas para resistir a los ataques.[99]

Luego de Operación Tequila, un grupo de activistas digitales en el país conocido como Operación Mexico acaparó el escenario tras anunciar que atacaría el sitio web de la Presidencia de la República, el de la Secretaría de Comunicaciones y Transportes y el de la Secretaría de Hacienda y Crédito Público. Según un correo que circuló por las áreas de IT el 16 de febrero de 2011, no les quedó más que preparar café y esperar el ataque. [100]

En América Latina hay 1,000 profesionales IT certificados en seguridad, lo cual representa un nivel muy bajo de profesionalización, destacó Anderson Ramos ejecutivo de la firma de consultoría en seguridad ISC. En el marco del Octavo bSecure Conference, se dio a conocer los resultados de una encuesta realizada en la región que reveló cuál es el nivel de profesionalización de los expertos dedicados a la seguridad informática en las empresas.[101]

La profesionalización en seguridad IT es relevante debido a que tener empleados certificados es necesario para 44% de las empresas encuestadas a nivel mundial por ISC. En América Latina 54% de las empresas consideran que es mejor tener personal certificado y en México la cifra se eleva a 59%. En México 52% de los profesionales dedicados a la seguridad posee un título universitario y 46% cuenta con estudios de posgrado. Además hay más hombres, 86%, dedicados a la seguridad que mujeres, 14% en nuestro país [102](Gráficas 4.5 y 4.6).

---

[99] http://www.bsecure.com.mx/opinion/hackivismo-como-para-que/

[100] Ídem

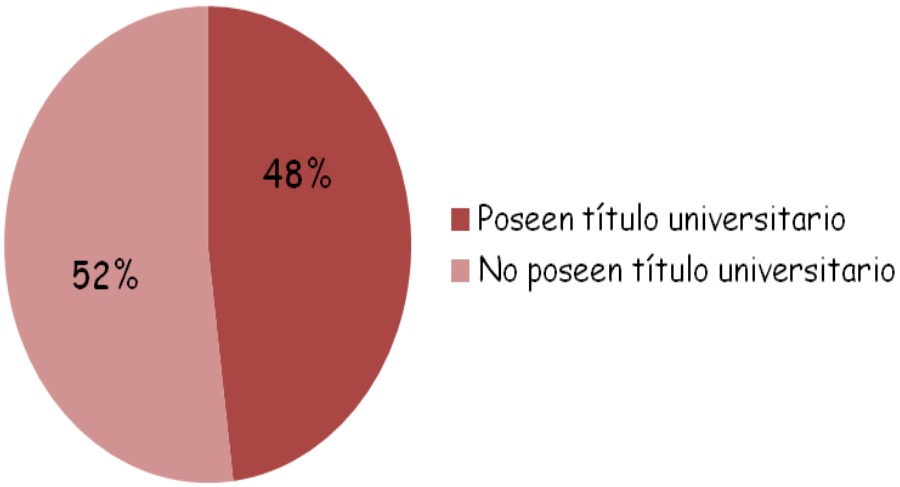
[101]http://www.bsecure.com.mx/featured/america-latina-necesita-mayor-profesionalizacion-en-seguridad-it/

[102] http://www.bsecure.com.mx/featured/america-latina-necesita-mayor-profesionalizacion-en-seguridad-it/

"El problema de la seguridad en las empresas es un problema humano" aseguró el ejecutivo de ISC.

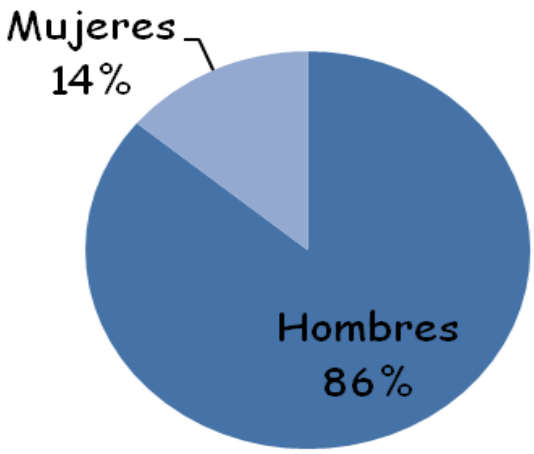
Los profesionales de seguridad tienen un nivel de experiencia muy alto en Latinoamérica equivalente a 10 años, muy similar a la media mundial que es de 11 años. En México al igual que Chile y Colombia se tienen 9 años de práctica.

Argentina es el caso con más años de experiencia trabajando en esta materia con 12 años.[103]



Gráficas 4.5 Nivel de titulación de los profesionales dedicados a la seguridad informática en México

[103] http://www.bsecure.com.mx/featured/america-latina-necesita-mayor-profesionalizacion-en-seguridad-it/



Gráficas 4.6 Género de los profesionales dedicados a la seguridad informática en México

4.2 Amenazas provocadas por el usuario

Como ya se mencionó, una amenaza es todo aquello que pretende o puede causarle algún daño a los bienes. Esto puede ser de manera intencional o no, sin embargo, aunque no sea intencionalmente el daño que se provoque, por el simple hecho de tener la capacidad de perjudicar a los activos, es que se considera como amenaza algo o alguien. Es por ello, que en este trabajo se tiene la hipótesis de que el usuario es una amenaza para su propio equipo.

Los motivos en los cuales se basa este trabajo al realizar dicha afirmación, son la gran cantidad de situaciones que se presentan cotidianamente, en los que los equipos e información se ve dañada debido a circunstancias que podrían evitarse, y que no son otra cosa más que descuidos por parte de los usuarios.

Ejemplos de estas situaciones son los derrames de agua o de cualquier líquido en algún dispositivo de hardware, problemas con los equipos como un corto circuito o mal funcionamiento de los sistemas debido a las malas conexiones que se realicen, pérdida de contraseñas por olvido o porque se dejaron anotadas en algún lugar visible, etcétera. Como puede verse son cuestiones que a veces pueden parecer insignificantes, pero que son muy comunes y que si se logran evitar, consecuentemente se podrían evitar problemas más complicados.

Con la finalidad de justificar un poco la hipótesis mencionada, se retoma el asunto de los derrames en los dispositivos, con el cual puede verse un ejemplo claro del por qué se considera al usuario como una amenaza para su equipo o información, planteando la siguiente situación:

Cierto usuario se encuentra trabajando en su oficina, tiene en su escritorio su laptop con una taza de café a un lado y documentos importantes en el otro. En este ejemplo puede visualizarse con claridad quién es la amenaza: la taza de café no lo es pues con todo y que se encuentre situada a un lado de la información o de la PC, es imposible que le cause por sí misma algún daño a dichos activos. Es el usuario y nadie más, quien por un lado colocó la taza de café en ese sitio, y por otro lado es él quien tiene la capacidad de tirar por descuido el café sobre los activos.

Este tipo de situaciones son por una parte lo que se refiere al usuario como amenaza, pero por otra parte se encuentran aquellas situaciones en las que no precisamente es el usuario quien es la amenaza, pero que indirectamente son los causantes de que existan amenazas externas a sus bienes. Esto se refiere a que muchas veces existen agentes amenazantes que podrían suprimirse si el usuario tomara medidas simples o en su defecto si no realizara ciertas acciones que consecuentemente derivan en las amenazas.

Ejemplo de ello, está la amenaza de sufrir un robo de información. De acuerdo con Larry Ponemon, fundador y presidente del Instituto Ponemon, la negligencia y el descuido continúan siendo los principales generadores de brechas de información. [104]

El estudio señala que 31% de los casos registrados de brechas de información estuvo relacionado con la pérdida de discos duros, archivos y equipos de cómputo por parte de los empleados de las empresas (Gráfica 4.7).

Por otra parte, tanto Symantec como el Instituto Ponemon, subrayaron que la falta de educación y concientización de los empleados es el motivo por el cual los casos de brechas de información continúan en aumento.[105]

Otro ejemplo de este tipo de situaciones, son las posibles intrusiones por parte de los perpetradores hacia los equipos de los usuarios.

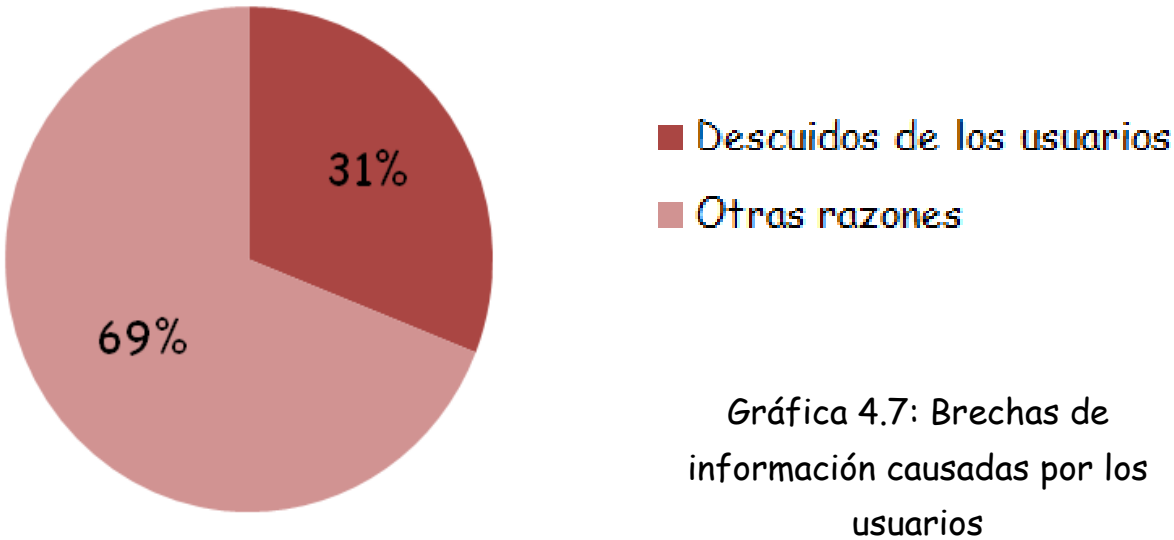
Existe una gran cantidad de ataques que para su ejecución se requiere de los permisos de los usuarios, mismos que éstos proporcionan. Cuando se tiene una aplicación con malware y se desea instalar en el equipo, es muy común que se pida la autorización del usuario para poderse ejecutar. Lo mismo sucede en las aplicaciones malware de las redes sociales. Es este tipo de códigos maliciosos, es muy común que se soliciten permisos para acceder a la información de los usuarios, o de lo contrario no se puede continuar, por lo que es el usuario mismo quien le proporciona todos esos permisos para instalación o ejecución de ese tipo de ataques.

Estas acciones por parte del usuario no son malintencionadas, sin embargo el hecho de que no esté informado o que simplemente no lea lo que le están

[104] http://www.bsecure.com.mx/featured/brechas-de-informacion-aumentan-7-durante-2010-generan-perdidas-por-7-2-mdd
[105] Ídem

solicitando hace que se convierta en una amenaza para sus bienes informáticos al brindar los permisos que le están solicitando, muchas veces sin saber qué es lo que está realizando, o simplemente dando click en el botón siguiente, o acepto.

Por lo tanto, mientras se tenga usuarios mal informados o no capacitados para hacer uso de los recursos informáticos, se debe considerar la amenaza que esto involucra, pues cómo sabrán qué hacer o no hacer o cómo actuar ante ciertas situaciones, si no tiene los conocimientos básicos acerca del tema, y por lo tanto pueden realizar acciones dañinas para dichos bienes. Es por ello que efectivamente los recursos informáticos son una herramienta que facilitan en gran medida las actividades y labores de la personas, pero es importante que el usuario sepa cómo puede y debe hacer uso de dichas herramientas y cuáles son los cuidados que debe tener en las mismas, para evitar futuros problemas.



Gráfica 4.7: Brechas de información causadas por los usuarios

4.3 Vulnerabilidades no identificadas por el usuario

La falta de conocimientos por parte de los usuarios acerca de las vulnerabilidades que poseen sus equipos o su información es muy común debido a la poca información con la que cuenta la mayoría de ellos. Esto es, si no logran identificar sus activos y la importancia de cada uno de ellos, jamás podrán identificar las vulnerabilidades que éstos poseen.

Generalmente esta situación, es decir, las vulnerabilidades no identificadas por el usuario, se presenta debido a que una gran cantidad de personas no le dan la importancia requerida a sus bienes.

Ejemplos de este tipo de situaciones son desconocer la importancia de cierta información, esta vulnerabilidad deriva en que las personas brinden dicha información pensando que es irrelevante.

Carlos Fernández, editor de bSecure expuso: Si la gente en general no se preocupa por la información que debiera importarle, como revisar su estado de cuenta bancario y se envía datos sensibles de la empresa al correo electrónico, demuestra que hay una inconsciencia sobre el manejo de la información personal y empresarial.[106]

En ocasiones sí se tiene conocimiento sobre la importancia de la información o de los bienes que se poseen, sin embargo, hay casos en los que aunque se le da la importancia adecuada, no se toman las medidas necesarias para resguardar dichos activos de la manera adecuada.

Un estudio a cargo de la firma de soluciones de seguridad financiera CCP reveló que los mexicanos no cuentan con las medidas de protección adecuadas para resguardar sus datos personales.

[106] http://www.bsecure.com.mx/featured/expertos-en-seguridad-ti-debaten-sobre-diversas-tecnologias

La firma señaló que los mexicanos se convierten en blancos perfectos para el robo de identidad debido a los hábitos que mantienen al gestionar su situación financiera.[107]

Así mismo, se deben considerar los hábitos que se tienen para el manejo de la información, ya que una gran cantidad de usuarios tienen malas costumbres con sus bienes como por ejemplo, no revisar los estados de cuenta, publicar información personal en redes sociales y descuidar la tarjeta de crédito al realizar un pago, entre otros.

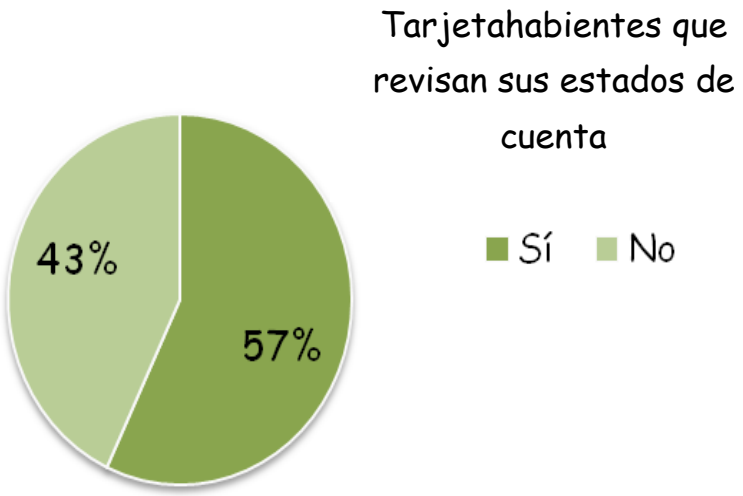
Un estudio revela que el 43% de los cuentahabientes mexicanos nunca revisa sus estados de cuenta (Gráfica 4.8), lo que le impide percatarse sobre la existencia de cobros o cargos irregulares a su tarjeta de crédito.[108]

La última brecha citada por el estudio es el descuido de la tarjeta por parte del propietario al momento de pagar. De acuerdo con los resultados, 27% de los tarjetahabientes descuida el plástico al realizar un pago, momento que puede ser utilizado para obtener los datos del usuario, alerta la firma.[109] (Gráfica 4.9)

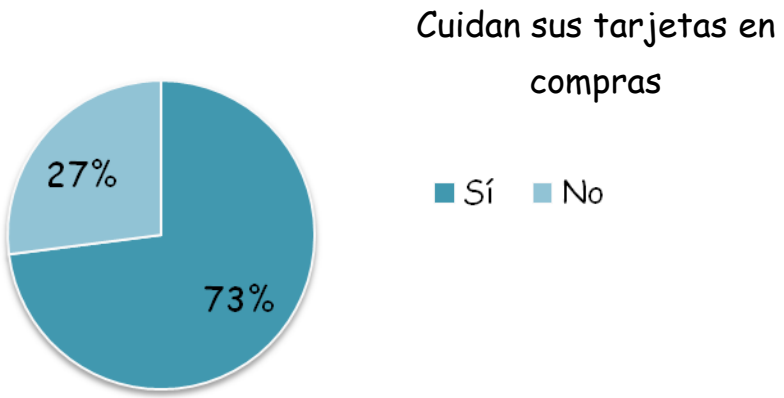
[107] http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion-deficientes-estudio

[108] http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion-deficientes-estudio/

[109] http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion-deficientes-estudio/



Gráfica 4.8: Revisión de estados de cuenta de los usuarios.



Gráfica 4.9: Descuido de las tarjetas al realizar compras.

También cabe mencionar el descuido que se tiene a la hora de brindar información vía telefónica.

Los resultados subrayan que 11% de la población proporciona información confidencial vía telefónica, incluso tratándose de extraños.[110]

Por obvias razones esto es demasiado alarmante, pues como se sabe, hoy en día los delincuentes suelen utilizar como técnica las llamadas telefónicas, para efectuar los llamados robos de identidad.

La información robada puede ser utilizada por los delincuentes para abrir cuentas bancarias, solicitar préstamos y financiar vehículos, además de comprar bienes y servicios o incluso establecer contratos como la renta de una vivienda, todo esto bajo la identidad de otra persona, asegura la firma de seguridad CCP.[111]

Otra vulnerabilidad de este tipo, es el exceso de confianza que algunas personas poseen. Esto es principalmente porque piensan que las personas más cercanas son de confianza y que se puede estar seguro en un ambiente de trabajo compartido, es decir, si se encuentran laborando en una empresa u organización, la mayoría de las veces se cree que se está más seguro dentro de la misma, y que de quien se deben proteger es de los agentes externos. Esto finaliza en un descuido de seguridad respecto al ambiente interno.

De acuerdo con diversos estudios que se han realizado, se obtuvo que en muchas ocasiones el principal enemigo de la compañía se encuentra dentro de ella.[112] Y si no se identifica dicha vulnerabilidad, es común que se tengan ataques imprevistos.

Existen además varias vulnerabilidades que se ocasionan buscando facilitar las tareas a realizar y sin tener conciencia de lo que se está realizando y las

[110] Ídem
[111] Ídem

[112] http://www.theinquirer.es/2011/01/03/la-tercera-parte-de-todos-los-virus-de-la-historia-se-han-generado-en-2010.html

consecuencias que se podrían tener. Ejemplo de esto son acciones como la sincronización de los celulares con las cuentas de correo. La mayoría de las personas que cuentan con un Smartphone, lo sincroniza a los equipos de cómputo de su trabajo, hogar y redes públicas, además en su mayoría cuentan con servicios de almacenamiento en la nube, lo que compromete aún más su información.[113] Sincronizar estos equipos sería una buena práctica si contaran con sistemas de cifrado de datos, pero considerando que la mayoría de los dispositivos inteligentes disponibles en el mercado no cuentan con sistemas de cifrado, lo único que se ocasiona es comprometer más la información.

Casi la mitad de los usuarios de las áreas IT de empresas alrededor del mundo aseguran que no existen políticas en sus áreas IT con los lineamientos para el uso de teléfonos celulares, Smartphones, PDA o incluso de las PC.

"Al tiempo que este tipo de dispositivos móviles entran al ambiente empresarial, los empleados están cuestionando las políticas IT. El entorno ha creado una sensación de urgencia por utilizar dispositivos móviles y medios sociales en internet y los empleados buscarán adoptarlos a pesar de las políticas IT", pronosticó en el reporte Nasrin Rezai, director de Cisco Security.[114]

El IT Risk/Reward Barometer reveló que 28% de los encuestados considera que los dispositivos móviles representan un riesgo para la seguridad, 73% reconoció estar al tanto de la posibilidad de que los empleados almacenen datos de la empresa en sus equipos móviles de forma insegura. Por lo que las netbooks y computadoras portátiles corporativas son los dispositivos que, a juicio de los participantes, constituyen el mayor peligro para las organizaciones, aun sobre los smartphones.[115]

[113] http://www.bsecure.com.mx/featured/que-tan-seguros-son-los-smatphones/

[114] http://www.bsecure.com.mx/ultimosarticulos/mitad-de-empresas-carecen-de-politicas-it-de-uso-de-celulares-pda-y-pc/

[115]http://www.bsecure.com.mx/ultimosarticulos/mcafee-libera-software-seguridad-para-smartphones-con-android/

Symantec agrega que el poco interés en el cifrado de datos no es la única brecha con la que cuentan los sistemas operativos, denunciando que la ausencia de herramientas para bloquear ataques de ingeniería social y spam es otro factor que pone en riesgo al usuario. "Actualmente los ataques de ingeniería social suelen tener más éxito que un ataque tradicional, debido a que en la mayoría de las ocasiones los embates de phishing incluyen información que resulta atractiva a los clientes", indican analistas de la firma.[116]

La principal causa de que se presenten este tipo de situaciones es la ignorancia y a la falta de cultura informática.

En el artículo "Bendita ignorancia que nada da y mucho quita" de la revista en línea de seguridad informática b: secure, se afirma que la mayoría de los administradores IT tienen mucha desinformación de los peligros que existen en la red, el problema es que la mayoría de ellos "suponen" lo que realmente sucede, por comodidad, ignorancia o simplemente por apatía.[117]

4.4 Ataques causados por el usuario

En este trabajo, al hablar de ataques causados por el usuario, no se hace referencia a que el usuario sea un atacante como tal para los equipos y en ningún momento se pretende afirmar que el usuario es un perpetrador, pues de ser así, entonces lo ideal sería que no existieran los usuarios, lo cual es ilógico.

Concretamente, a lo que hace referencia este subtema, es a que en diversas ocasiones se presentan ataques que pudieran evitarse si los usuarios tomaran las medidas preventivas adecuadas, o en su defecto, si no se pudieran evitar,

[116] Ídem
[117] http://www.bsecure.com.mx/opinion/bendita-ignorancia-que-nada-da-y-mucho-quita/

por lo menos sí se lograrían minimizar las consecuencias derivadas de dichos ataques.

Como ya se mencionó, existen vulnerabilidades y un ataque es cuando se explotan dichas vulnerabilidades, por lo tanto, el hecho de que existan amenazas y vulnerabilidades provocadas por el usuario, consecuentemente habrá ataques causados por el usuario.

Retomando los ejemplos mencionados en los subtemas anteriores, se pueden enunciar algunos ataques ocasionados directamente por el usuario como el daño de hardware por el derrame de sustancias, robo de equipo o información por la obtención de contraseñas de manera fácil, entre otros.

En concreto, existe una gran cantidad de ataques que podrían evitarse o por lo menos minimizar la posibilidad de su ejecución, si el usuario no realizara acciones para facilitar dichos ataques. Ejemplo de esto son aquellos que se llevan a cabo mediante las redes sociales.

Como ya se mencionó, las redes sociales son un medio por el que actualmente se está llegando al usuario y así ejecutar cualquier tipo de acción o mal uso de la información de éstos. Facebook, que es una de las redes sociales más utilizadas en la actualidad, día con día es el medio de propagación de una gran cantidad de malware y un medio de extracción de información muy utilizado. Recientemente la red social se convirtió en la víctima de una nueva forma de spam llamada likejacking. Los ataques de likejacking se propagan a través del perfil de los usuarios y la forma más común para atraparlos es por medio de la creación de sitios apócrifos. Al final, el usuario es víctima del engaño y se convierte en parte de la estafa desarrollada por los cibercriminales.[118]

[118] http://www.bsecure.com.mx/featured/facebook-busca-evitar-que-curiosidad-sea-responsable-del-robo-de-cuentas/

Uno de los principales problemas que se tienen en el uso de estas redes, es la ignorancia que miles de usuarios le dan a las políticas de privacidad. Es increíblemente común que los usuarios que hacen uso de dichas redes simplemente den click en siguiente y aceptar, a todo lo que les aparece, esperando que con el transcurso del tiempo y el uso de las aplicaciones, se den cuenta de lo que acaban de consentir para el futuro, sin tener la menor idea de que lo realmente hicieron fue permitir acceder a su información y de ahí surgen futuros ataques. Uno de los métodos utilizados para los ataques vía redes sociales, es el uso de los posts. El malware postea invitaciones a los amigos de los usuarios infectados mediante links de enlace, los cuales direccionan a sitios maliciosos.

En 2010 los cibercriminales encontraron un nuevo mecanismo para robar información e infectar equipos sin necesidad de vulnerar sistemas o violar infraestructura. Bastaba con convencer al usuario. Los cibercriminales saben que basta con vulnerar al usuario antes que al sistema y las redes sociales proporcionan el campo ideal para la ingeniería social. "Antes de la redes sociales la única forma de que te contactaran era a través de un correo electrónico. Con Facebook y Twitter eso cambió, ahora son tus amigos o conocidos, en quienes confías, los que te envían archivos o ligas, que pueden estar comprometidas", afirmó Juan Pablo Castro, gerente de Desarrollo de Negocios de Trend Micro México.

Para 2011 Trend Micro espera un aumento en la calidad y cantidad de ataques de ingeniería social, impulsados por las redes sociales, plataformas web 2.0 e incluso la ignorancia del usuario, como fue el caso de los antivirus falsos o scareware. [119]

Por lo pronto, reportes sobre este asunto se publican constantemente, dando la alerta a usuarios, proveedores e incluso autoridades de gobierno a que

[119] http://www.bsecure.com.mx/featured/un-2011-riesgoso-y-urgente-de-cambio/

tomen las medidas de precaución más adecuadas, no obstante la respuesta tecnológica para disminuirlas avanza lentamente. Esto indica que el mejor mecanismo defensivo es adquirir conocimientos mínimos de seguridad de la información entre tanto no aparezca un sistema o código de programación perfecto. [120]

Continuando con los ataques en los cuales el usuario brinda facilidades para su ejecución, se encuentra como ejemplo uno de los más sonados ataques recientemente. Dicho ataque es el realizado en contra de Sony.

En estos ataques se logró ingresar a la base de datos, y se extrajo gran cantidad de información de los usuarios registrados.

Recientemente se ha hablado acerca de la culpa por parte de los usuarios para facilitar dicho ataque, pues estudios recientes revelaron que sólo 4% de las contraseñas empleadas en una página de Sony usan más de tres tipos de caracteres y menos de 1% utilizan caracteres no alfanuméricos. Además, dos tercios de las personas ocupan la misma contraseña en otros sitios.[121]

Los datos anteriores fueron descubiertos por el arquitecto en software Hunt Troya, quien analizó las cuentas de usuarios de la página sonypictures.com publicados por LulzSec luego del ataque realizado por este grupo donde obtuvieron más de un millón de contraseñas que se encontraban almacenadas en texto simple. "Sony es culpable de la brecha, de eso no hay duda, pero un montón de personas empeoraron todavía más la situación al reusar contraseñas" señala Troya en su blog.[122]

[120] http://www.seguridad.unam.mx/doc/?ap=articulo&id=219

[121] http://www.bsecure.com.mx/ultimosarticulos/clientes-de-sony-podrian-haber-facilitado-el-robo-de-informacion/

[122] http://www.bsecure.com.mx/ultimosarticulos/clientes-de-sony-podrian-haber-facilitado-el-robo-de-informacion/

El trabajo del arquitecto de software consistió en comparar dos de las bases de datos de Sony publicados por el grupo de hackers y encontró que más de 2,000 direcciones de correo electrónico eran idénticas, lo que significa que esas personas se habían registrado en esas bases. Sin embargo, 92% habían utilizado la misma contraseña en ambos casos.

Troya también encontró que 88 cuentas de email que estaban registradas en Sony estaban en un sitio llamado Gawker, el cual fue hackeado el año pasado por LulzSec y cuyos datos igualmente fueron publicados por el grupo y que varios de los usuarios usaban la misma contraseña para los dos sitios.[123]

Como puede verse, es cierto que existe una gran cantidad de atacantes y amenazas que siempre estarán latentes hacia los bienes informáticos de todas las personas, sin embargo, si se toman las medidas preventivas necesarias para estar preparados para este tipo de situaciones, se puede minimizar el riesgo que puedan sufrir dichos bienes.

La reutilización de contraseñas por parte de los usuarios en los sitios que utilizan y el hecho de que las personas eligen claves susceptibles de crackear no son situaciones nuevas, sin embargo, los investigadores de seguridad señalan que otro problema importante es que muchos sitios en internet no almacenan en lugares seguros esa información tan sensible trayendo como resultado la vulnerabilidad de dichas páginas.

Por mencionar más ejemplos que justifican el por qué del subtema de este trabajo, se puede mencionar, el robo de información y la infección de equipos con malware. Ambos son ataques muy comunes y con los cuales se culpa en su totalidad a los perpetradores. Sin embargo, es importante mencionar que para la gran mayoría, el principal factor de riesgo para el primer ataque es la pérdida de información corporativa al extraviar los dispositivos móviles (64%), y con respecto al segundo ataque, la principal causa se debe a la infección de la red empresarial al conectar un móvil con malware (59%),

[123] Ídem

descargar aplicaciones con contenido malicioso (37%) o utilizarlo como medio para extraer información sensible del negocio (36%).

Desde el punto de vista del experto Saurabh Bhatnagar, director de producto de Websense, esta realidad tan solo es una de las áreas de riesgo, porque falta sumarle la complejidad ya existente de la infraestructura de IT, malware, APT, vulnerabilidades, fuga de datos y riesgos relacionados al uso de plataformas del web 2.0 u otros servicios de internet.[124]

Finalmente, es importante mencionar que tanto las amenazas, las vulnerabilidades y consecuentemente los ataques provocados por los usuarios, de ninguna manera se deben a que el usuario tenga en algún momento la intención de dañar sus bienes, sino básicamente se debe a la falta de conocimiento sobre la seguridad informática por parte de ellos, el exceso de confianza con respecto a los lugares donde laboran o las personas con quienes interactúan, la curiosidad por saber qué pasa si le dan un simple click en un link, o qué pasa si se mueve tal cable o se presiona cierto botón; descuido de sus pertenencias por confiar en que no sucederá nada inesperado, o simplemente por falta de cultura.

[124] http://www.bsecure.com.mx/featured/el-periferico-de-ciudad-ciberseguridad/

Capítulo 5: Buenas prácticas para el uso de bienes informáticos en general

Como se pudo ver en los capítulos anteriores, es una realidad que existen muchas amenazas, vulnerabilidades y ataques contra los bienes informáticos, que podrían suprimirse o en su defecto minimizarse si se tomaran en cuenta medidas simples y básicas de seguridad para la protección de los recursos e información.

Es muy cierto que gran cantidad de los usuarios no conocen todos los peligros a los que sus bienes están propensos día con día. Sin embargo, aún desconociendo esa información, si se les informa acerca de las medidas que deben tomar para el cuidado de dichos activos, es un hecho que se encontrarán mejor protegidos y se podrán evitar daños innecesarios.

Para preservar la seguridad de los recursos informáticos es necesario que se implementen y se lleven a cabo ciertas medidas, ya sean a nivel individual o a nivel organización acerca del uso adecuado que se le debe dar a los equipos de cómputo, conexiones de internet, correo electrónico, y otras fuentes de contenido de información. Esto incluye una clasificación de la información, control de accesos y privilegios, roles y tareas a desempeñar por cada elemento de la organización.

A continuación se presenta un conjunto de buenas prácticas dirigidas a cualquier persona que sea usuario de un recurso informático. Con esto se pretende que sus bienes informáticos se preserven en un estado más óptimo, y se disminuya la posibilidad de ser víctimas de futuros ataques.

Las siguientes recomendaciones de seguridad abarcan los aspectos básicos que todo usuario debe considerar al hacer uso de sus bienes informáticos.

Al llevarlas a cabo se evitarán problemas futuros que le ocasionarían posibles fallas que pueden suprimirse o en su defecto minimizar el impacto de éstas.

Dichas recomendaciones se redactaron de acuerdo con el comportamiento que se debe tener ante posibles escenarios que son muy comunes, con lo que se busca orientar al usuario para evitar en lo posible futuros ataques informáticos.

5.1 Buenas prácticas para el manejo de contraseñas

Si las contraseñas que las personas utilizan día con día en sus diferentes cuentas, llegan a caer en las manos equivocadas, pueden ser víctimas de distintos tipos de ataque como es la usurpación, robo de información, entre otros. (Figura 5.1)

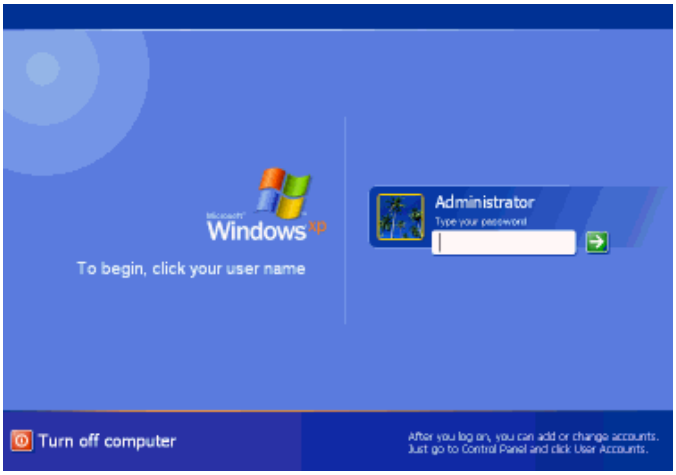


Figura 5.1 Uso de contraseñas

Es por ello que se debe ser cuidadoso con el manejo de las contraseñas.

- Al crear contraseñas ya sean para el acceso de un dispositivo de hardware (computadora, celular, control biométrico, etcétera) o para

una cuenta de cualquier tipo (correo electrónico, red social, bancaria, etcétera), siempre use un conjunto de caracteres variados, alfanuméricos y de gran extensión en lo posible (8 caracteres mínimo).

- Evite usar fechas de nacimiento o fechas importantes que quizá alguien pueda adivinar con facilidad. Así mismo evite utilizar nombres o palabras importantes para usted, que de igual modo sean fáciles de inferir.

- Memorice lo antes posibles todas sus contraseñas y evite dejarlas en lugares visibles o accesibles para las demás personas.

- Use contraseñas diferentes en sus cuentas, es decir, evite usar la misma contraseña para todas sus cuentas.

- Cambie periódicamente sus contraseñas. De ser posible, programe la actualización de éstas para que así, no se olvide de realizarlo.

- Evite brindar las contraseñas a cualquier persona.

- Si existe alguna razón para creer que una contraseña se encuentra comprometida, debe cambiarla inmediatamente.

- Cada que realice la modificación de las contraseñas, evite hacer uso de contraseñas similares a las anteriores.

- Evite en lo posible, el envío de contraseñas o resguardo de éstas en el correo electrónico.

5.2 Buenas prácticas para el control de acceso

Es importante que se dificulte en cierta medida el acceso a los bienes de cualquier persona. Para esto es conveniente que primero se determine la importancia de dichos bienes para saber qué tanta seguridad se requiere en éstos.

Una de las medidas básicas en seguridad informática es el control de acceso. Si se limita el acceso a cualquier cuenta, equipo o cualquier recurso informático, se tendrá un mejor control de la información. (Figura 5.2)

Figura 5.2: Control de acceso

- Implemente medidas de control de acceso a cualquier dispositivo. Establezca por lo menos una contraseña de acceso para cualquier dispositivo informático.

- Asigne cuentas de usuario propias y haga uso correcto de ellas.
- Almacene la información relevante en lugares a los que no cualquier persona tenga acceso con facilidad. Para el resguardo de las memorias USB, CD, y demás medios de almacenamiento de información, puede hacer uso de cajones o estantes para resguardarlos bajo llave.

- Active el sistema de protección de pantalla de tal modo que se active después de determinado tiempo de inactividad del equipo y requiera de la contraseña para reanudar la actividad.

- Defina perfiles y privilegios, así como permisos para el uso de los recursos, de tal forma que se proteja la información relevante o el sistema, de modificaciones o eliminaciones no autorizadas.

5.3 Buenas prácticas para el manejo de información

"La información es poder." Francis Bacon

Como es sabido, la información es un arma muy poderosa, que si cae en manos de las personas incorrectas puede resultar en graves consecuencias para el propietario de dicha información.

Es por ello que es de suma importancia darle el debido cuidado a toda clase de información de las personas, pues lo que puede parecer insignificante para algunos, para otros puede ser el medio que les permita realizar algún ataque informático a cualquier individuo.

Si se toman en cuenta las siguientes medidas de protección para la información, el riesgo de que se sufra un mal manejo de ésta disminuirá notablemente. (Figura 5.3)

Figura 5.3 Protección de información

- Haga una clasificación de la información para implementar las medidas necesarias de seguridad según corresponda. Seleccione debidamente el nivel de criticidad que corresponda a su información y proporcione el nivel de seguridad adecuado, realizando un manejo de riesgo y evitando así fugas de información.

- Proteja la información sensible (crítica) mediante el respaldo de ésta en un servidor externo o en su defecto un medio de almacenamiento externo y no en el dispositivo. Cabe señalar que en caso de que utilice un medio de almacenamiento externo, debe tener sumo cuidado con éste y resguardarlo debidamente.

- Realice los respaldos de información en por lo menos 2 medios diferentes. Dichos respaldos los debe realizar de manera periódica.

- Evite eliminar la información útil hasta cerciorarse que se encuentra debidamente respaldada.

- Tenga extremo cuidado con la información que se lleva a la Nube (Cloud), ya que esa información tendrá un alto grado de riesgo, debido a que no habrá fronteras en la cobertura. Evite subir aquella información que sea crítica.

- Una vez que se ha decidido hacer uso del Cloud, es recomendable que se lean de manera minuciosa los contratos que se tienen, para asegurarse que la información no quedará respaldada en centros de procesamientos de datos (data centers) de la competencia.

- Evite dejar los documentos importantes en lugares visibles o de fácil acceso para otras personas.

- Evite en lo posible trabajar en lugares públicos como los cafés o aeropuertos o de hacerlo tener el debido cuidado que la información que se está manejando y la cual pueden ver las personas a su alrededor, no sea tan descriptiva, pues muchas veces se piensa que hacer una presentación no es importante para alguien más, sin embargo, quizá con dicho documento las personas podrían enterarse de dónde trabaja, por dar un ejemplo, sin contar con otros datos que podrían deducir las personas con ver la información. (Figura 5.4)

Figura 5.4 Manejo de información en lugares públicos

- En caso de que recurra frecuentemente al uso de la laptop o dispositivo móvil en lugares públicos, opte por adquirir un filtro de pantalla, el cual opaca la pantalla prácticamente desde cualquier ángulo, a excepción del frontal.

- Evite traer el gafete de identificación en la calle y lugares públicos, haga uso de él exclusivamente para las actividades que se lo demanden y guárdelo siempre que le sea posible.

- Deseche la información relevante como la información bancaria, sólo si ésta ha sido destruida previamente.

- Al desechar un documento con información privada, personal o confidencial, procure destruirla a manera que no sea legible.

- Cuando desee desechar información de un CD, éste debe ser destruido en su totalidad, no basta con sólo tirarlo.

- Tenga cuidado a la hora de realizar búsquedas web. Es importante conocer que cuando se está navegando por internet y se desea acceder a un link, al posicionarse sobre éste, en la parte inferior de la página aparece la URL a donde se direccionará. Si se duda de dicha dirección, evite acceder a ella.

- Por ningún motivo revele datos personales a través de llamadas telefónicas o a personas desconocidas.

- Implemente un sistema de autenticación por sencillo que éste sea, para una mejor protección de la información.

- Procure tener siempre instaladas herramientas de bloqueo y detección de virus y archivos maliciosos, así como firewalls y filtros de contenido.

"La información lo es todo, en la guerra como en la paz, en la política como en la economía." Fouché

5.4 Buenas prácticas para la protección de virus y malware

Hoy en día todos los usuarios de un bien informático están expuestos a sufrir daños en sus activos a causa de algún virus o código malicioso. Es por ello que se deben tener medidas básicas para la protección de estas amenazas.

Las recomendaciones básicas son:

- Verifique que los equipos cuenten con programas de detección y eliminación de virus, y código malicioso. (Figura 5.5)

Figura 5.5 Herramientas de protección de virus y malware

- Solicite a un experto recomendaciones sobre el software más adecuado para su sistema.

- Supervise que dichos programas se encuentren en buen estado, es decir, se encuentren vigentes.

- Cuando dichos programas soliciten el escaneo del equipo o muestren posibles amenazas, no omita dichos mensajes y realice las tareas que recomiende el sistema.

- Verifique que el firewall del equipo esté siempre activo.

- Realice revisiones periódicas del estado del equipo.

- Siempre que se introduzca un dispositivo de almacenamiento externo a los equipos, realice el escaneo de detección de virus y malware.

- Evite en lo posible hacer uso de los medios de almacenamiento de uso cotidiano en equipos diferentes al suyo. En caso de que sea necesario hacerlo, realice el escaneo de éste al ingresarlo en su equipo.

- Evite al máximo introducir sus medios de almacenamiento en dispositivos públicos como los que se encuentran en un café internet, es muy común que dichos equipos posean virus y código maligno.

- Realice descargar de internet sólo si es necesario y hágalo preferentemente desde sitios conocidos.

- Nunca se debe acceder a los links recibidos vía Messenger o correo electrónico hasta cerciorarse con el remitente realmente es quien lo está enviando.

5.5 Buenas prácticas para el cuidado físico de cualquier dispositivo informático

Es muy importante que no se deje a un lado la protección física de los dispositivos. Si bien la protección del aspecto lógico es de mucha ayuda, también se debe considerar el cuidado de los dispositivos de los factores ambientales y amenazas físicas que pueden causar algún daño en éstos.

- Por ningún motivo debe realizar modificaciones en las configuraciones de los dispositivos si no tiene los conocimientos necesarios para realizar tal acción.

- Proteja los equipos de los factores ambientales, haciendo uso de fundas y protectores para el polvo, agua, etcétera. (Figura 5.6)

Figura 5.6: Protectores para equipos móviles

- Evite en lo posible consumir alimentos y bebidas cerca de los dispositivos para reducir la posibilidad de que ocurra algún accidente.

- Tenga cuidado al momento de seleccionar el lugar en el que se instalará un equipo informático. Nunca se debe colocar en zonas de riesgo como son instalaciones de agua, ni demás factores que puedan representar un peligro para los equipos.

5.6 Buenas prácticas para el manejo de bienes financieros

Adquirir mejores hábitos bancarios reduce los índices de fraudes financieros. [155] Entre algunos buenos hábitos financieros se encuentran:

- Procure mantener una clave exclusiva para la tarjeta y evite que ésta corresponda a datos personales fáciles de adivinar.

- Evite en lo posible proporcionar las contraseñas de acceso de las tarjetas bancarias a otras personas. Dicha clave se debe mantener en absoluta reserva y nunca se debe anotar en lugares de fácil acceso para terceras personas.

[155] http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion-deficientes-estudio/

- Nunca pida ayuda a desconocidos para el manejo de los cajeros automáticos, ni permita que personas extrañas se encuentren cerca de usted al hacer uso de dichos cajeros.

- Evite hacer uso de cajeros automáticos ubicados en lugares muy solitarios o cajeros que se visualicen en malas condiciones. (Figura 5.7)

Figura 5.7: Uso de cajeros automáticos

- Si el cajero automático se encuentra fuera de servicio, evite hacer uso de él y mucho menos introduzca su tarjeta o digite su número secreto.

- Asegúrese de retirar su tarjeta después de realizar una operación en el cajero automático.

- Revise los estados de cuenta entre 2 y 3 veces por semana. Esto con la finalidad de monitorear los movimientos que se van registrando y detecte a tiempo cualquier cargo que se realice de manera ilícita. Existen algunos bancos que proporcionan como servicio un sistema de alertas por medio de las cuales se les notifica a los tarjetahabientes, las operaciones relevantes en el historial crediticio. Si se cuenta con dicho servicio, lo ideal es hacer uso de él.

- Mantenga siempre a la vista las tarjetas que se manejen. Al pagar en establecimientos, de ser posible, pida que le lleven la terminal a su lugar para que vea el uso que le dan a dicha tarjeta.

- Al realizar un pago con tarjeta verifique que el voucher que firma corresponde al importe de la compra que realizó y verifique que no se encuentren cargos no reconocidos.

- Conserve los vouchers de las compras realizadas con las tarjetas para futuras aclaraciones.

- Si identifica cargos extraños a sus estados de cuenta o tiene dudas sobre el funcionamiento de su tarjeta bancaria, notifique cuanto antes al proveedor bancario.

5.7 Buenas prácticas para el manejo de dispositivos móviles

Como se mencionó, hoy en día el uso de dispositivos móviles es muy frecuente en la vida cotidiana de las personas. Es por ello que los atacantes han visto estos medios como formas de propagar amenazas y ejecutar gran diversidad de ataques.

Algunas de las recomendaciones son:

- Tenga cuidado con el manejo de los dispositivos móviles. Es muy recomendable cifrar los equipos para evitar que se acceda con facilidad a la información contenida en dicho equipo.

- En lo posible procure restringir el acceso a los dispositivos mediante contraseñas de acceso. Actualmente las medidas básicas que se pueden aplicar a prácticamente cualquier dispositivo móvil, es una contraseña para el acceso al dispositivo y otra para la tarjeta SIM o chip mediante el cual funciona el dispositivo. Se recomienda hacer uso de ambas.

- Debe tomar conciencia del uso de los dispositivos móviles. Existe una gran variedad de éstos y siempre habrá uno que satisfaga las necesidades de cada usuario. No adquiera dispositivos de los cuales desconoce su uso ya que más que útil, puede resultar riesgoso.

- Defina adecuadamente la información que se requiere resguardar en los dispositivos móviles y tablets. Evite cargar información confidencial y valiosa en este tipo de dispositivos, ya que son más vulnerables a su extravío.

5.8 Buenas prácticas para el uso de redes sociales

Del mismo modo que los dispositivos móviles, las redes sociales son un recurso muy utilizado por los usuarios. Por ello se le debe dar mayor importancia al uso de éstas y cuidar la forma en que utilizan.

Recomendaciones:

- Lea previamente todas las condiciones de uso de las redes sociales antes de dar click en aceptar.

- Una vez que ha creado un perfil en cualquier red social, dedique tiempo para conocer el funcionamiento de dicha red y defina los niveles de seguridad deseados.

- Tenga sumo cuidado con la información que se comparte, así como con las fotos que incluye en el perfil. Evite incluir información personal detallada, que en un futuro pueda ser usada con intenciones perjudiciales.

- Evite aceptar a personas como "amigos", sólo por tener gran cantidad de contactos que regularmente ni siquiera conoce ni mantiene comunicación con ellos. Nunca se sabe qué clase de personas andan navegando por las redes.

- Lea cuidadosamente todos los permisos que le solicitan las diferentes aplicaciones. Si alguna aplicación le solicita permisos que considera innecesarios, lo mejor es cancelar el acceso a dicha aplicación.

- Tenga cuidado con los correos electrónicos enviados supuestamente desde las páginas de las redes sociales. Existe una serie de correos electrónicos enviados a los usuarios en los que se les envían notificaciones para cambiar la contraseña. Expertos señalaron que Facebook jamás utiliza correo electrónico para realizar dichas acciones, además de que la empresa no suele adjuntar contenido en sus envíos.[156]Ponga completa atención en dichos correos, intentando identificar el remitente. Se aconseja que ponga atención en el nombre de la red social. En ocasiones los correos falsos se delatan al estar escrito incorrectamente el nombre de la red, por ejemplo FaceBook, o facebook, en vez de Facebook.

- Evite abrir los links enviados desde supuestas páginas de las redes sociales. Así mismo nunca debe abrir el contenido adjuntado en dichos mails.

- En caso de que no se logre identificar si es verídico o no el remitente de un correo, se recomienda que no acceda a la página de la red social desde el link enviado, sino que abra la página de dicha red social y desde ahí acceda a lo solicitado. Si efectivamente se trata de una notificación de la red social, ésta aparecerá en la página del usuario, de lo contrario, es un correo falso.

- Haga caso a todas aquellas campañas de concientización que llaman a los usuarios a utilizar estas herramientas tecnológicas de manera racional

[156] http://www.bsecure.com.mx/featured/facebook-infecta-usuarios-a-traves-de-correo-electronico/

no sólo en el empleo, sino también en el contenido que en ellas depositan. (Figura 5.8)

Figura 5.8: Peligros en las redes sociales

5.9 Recomendaciones para una organización

Cualquier organización, por muy pequeña que sea, debe tomar medidas básicas para la protección de sus trabajadores y sobre todo de la organización mínima.

Además de todas las buenas prácticas mencionadas anteriormente, para la seguridad de los activos, cualquier organización requiere tener políticas sobre un uso aceptable de los equipos, conexiones a internet y correo, así como otras fuentes de contenido, clasificación de información, accesos y privilegios, roles y tareas de cada departamento. Lo que se busca aquí es ser

consistente en los objetivos de las tecnologías de información y los de la organización.

Una de las medidas básicas que debe tomar una organización es la asignación de una persona o grupo de personas que se encarguen de las tareas relacionadas con la administración de la seguridad informática. Dichas personas tendrán las siguientes responsabilidades:

- Realizar un plan de contingencias, para estar preparados ante cualquier suceso que se pueda presentar y que pueda provocar daños en la organización. Lo ideal es plantear los diferentes escenarios que se puedan presentar y planear un método de defensa, o en su defecto, de recuperación ante dichos sucesos.

- Los planes de contingencia que se elaboren, deben ser totalmente aplicables y funcionales, esto para que se puedan aplicar siempre que sea necesario.

- Contar con estrategias para prevenir la pérdida de datos. Es necesario saber cómo reaccionar ante un ataque.

- Adoptar programas de prevención de brechas de información.

- Hacer una correcta selección de la información que será subida a la nube. Esto además de brindar mayor seguridad a la información, servirá para aprovechar al máximo los recursos y suprimir los costos que no son necesarios.

- Tener siempre en mente que debe existir una educación hacia los empleados y miembros de la organización. Establecer reglas, políticas y realizar las capacitaciones necesarias.

- Implementar políticas de seguridad en las que se exprese explícitamente la visión, misión y objetivos de la organización. Del mismo modo se deben documentar y revisar los procesos de la empresa. Los empleados deben conocer y tomar en cuenta dichas reglas para sus actividades.

- Proporcionar a los empleados la inducción correspondiente al manejo de la información de la empresa. Esto no solo será en beneficio del empleado, sino de la empresa misma.

- Restringir los accesos y crear políticas, de modo que existan sanciones en caso de que no se cumplan con ellas.

- Establecer normas sobre el uso de los tablets y equipos móviles. Dichas normas deben contemplar qué información puede ser cargada en dichos dispositivos y la sincronización de éstos con sus computadoras, para usar dichos dispositivos única y exclusivamente de ser requeridos y para tareas específicas, evitando así mayores vulnerabilidades.

- Hacer uso de las redes sociales única y exclusivamente si éstas brindan un beneficio económico para la compañía, de lo contrario pueden convertirse en una amenaza para la propia empresa.

- En caso de ser necesario el uso de las redes sociales, se deben establecer políticas de control de riesgos y de uso de las mismas.

- Tener un estricto control de la información que consultan los trabajadores. Es preciso que se determine si la información a la que tienen acceso es necesaria para realizar sus labores y si implica riesgos para la empresa.

- Hacer una actualización cada determinado tiempo de las cuentas activas. Esto es para evitar que empleados que ya no laboren en la empresa, cuenten aún con acceso a la red de la compañía.

- Implementar una infraestructura sólida en redes y cableado.

- Contar con personal especializado en seguridad, quienes deben adoptar las medidas necesarias para minimizar los riesgos que pueda tener la organización.

- Dicho personal debe ser un equipo capaz de resolver problemas y sobre todo, de anticipar amenazas y proteger su permanencia.

- Realizar pruebas internas de los programas con los que se trabaja en la empresa para determinar el nivel de riesgo que tienen ante posibles amenazas.

- Realizar una evaluación periódica de los sistemas de seguridad con la finalidad de descubrir vulnerabilidades.

- Realizar un monitoreo de los dispositivos que se conectan a la red de la empresa para identificar a tiempo posibles intrusiones.

- Hacer pruebas de penetración de manera regular.

- Analizar si la organización tiene capacidad de responder ante ataques e incidentes.

- Verificar y mantener al día las copias de seguridad. Es importante que las copias de seguridad sean respaldadas en un lugar externo a la empresa, ya que si bien, cuando se tienen los respaldos dentro de la misma empresa, se atacan problemas de pérdida de información, no sirve de nada tener dichos respaldos en caso de algún desastre natural, pues se perdería tanto la información original como los respaldos.

5.10 Difusión de las buenas prácticas

Hoy en día no se tiene la correcta información acerca de las medidas que se deben tomar para la protección de los bienes informáticos. Es por ello que muchas veces los usuarios realizan acciones que van en contra de sus activos, sin saber que están realizándole un mal a dichos bienes.

El tema de seguridad informática, si bien, es un tema de suma importancia para los profesionales dedicados al área, no es un tema lo suficientemente difundido para la mayoría de los usuarios de bienes informáticos.

Considerando que la gran mayoría de las personas hoy en día son usuarios de algún recurso informático, se debe comenzar a crear una "cultura en seguridad informática", de tal modo que se minimicen los riesgos de estos recursos. Con esta difusión se comenzará a crear conciencia sobre la importancia que tiene hoy en día dicho tema y con ello se podrá prevenir futuros ataques informáticos, reduciendo así, la llegada de los atacantes informáticos a los bienes de las personas.

Como parte de esta tesis se realizó una página web (Figura 5.9), en la que se plasman los principales conceptos de la seguridad informática, las definiciones de los términos que todo usuario debe conocer sobre el tema, se abordan los principales problemas informáticos que existen en la actualidad y se brinda un conjunto de buenas prácticas dirigidas al usuario, de tal modo que quien acceda a dicho sitio pueda entender el objetivo primordial de la página web, sin ser necesario que posea conocimientos sobre el tema y se logre crear conciencia sobre la importancia que tiene la protección de la información.

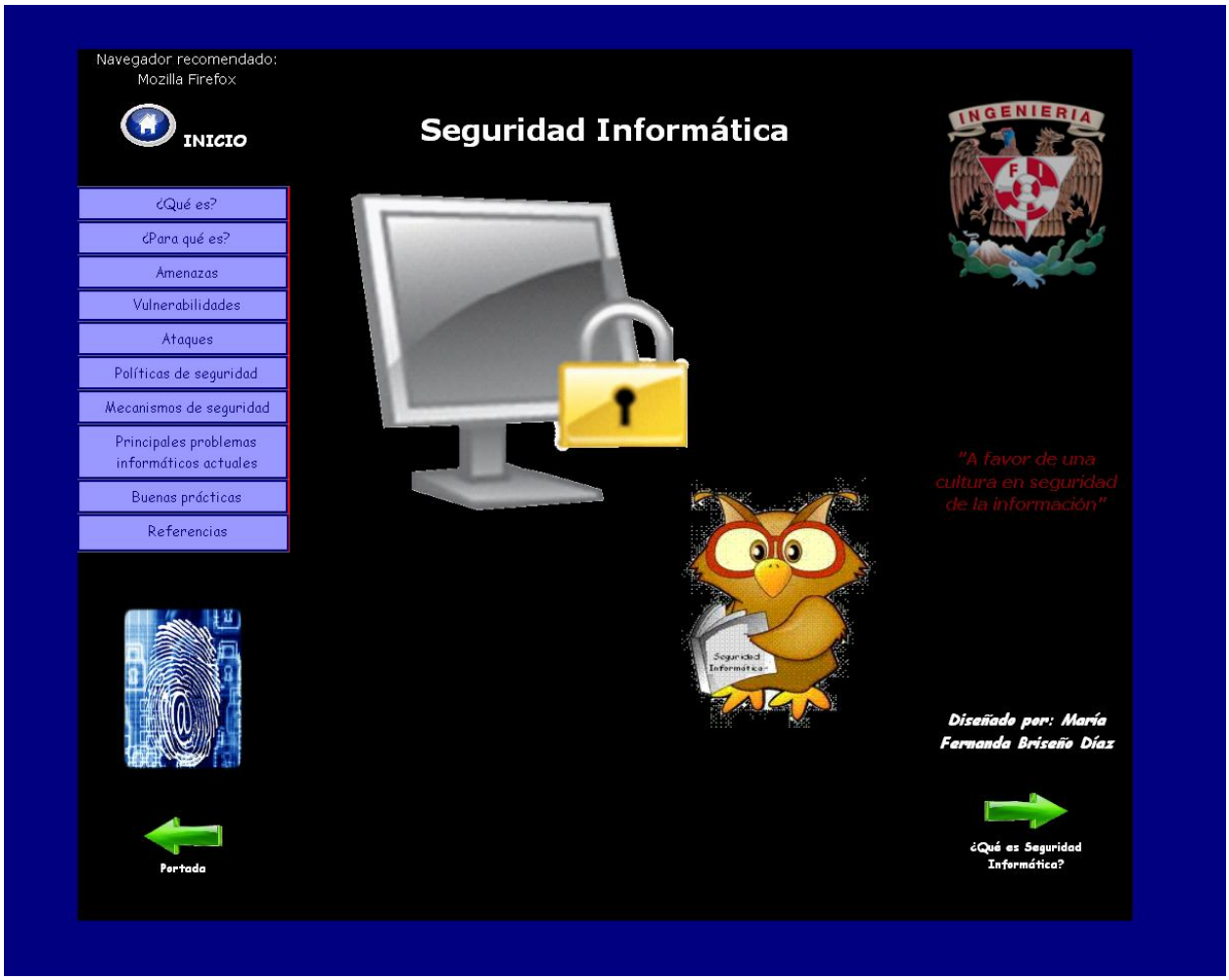


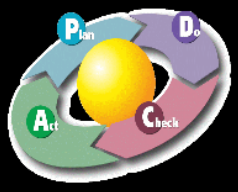
Figura 5.9: A favor de una cultura en seguridad informática

Como puede visualizarse, en el sitio web se proporciona la información necesaria para que cualquier usuario conozca lo que es la seguridad informática, cuáles son los objetivos de dicha disciplina, a qué se refieren los principales términos referentes a la seguridad informática, los principales problemas existentes en cuanto al tema y finalmente pueda darse una idea de cómo puede protegerse ante dichos problemas.

El sitio web consta de varios apartados, cada uno de los cuales está enfocado a la descripción de temas de seguridad específicos.

En el primer apartado: ¿Qué es? (Figura 5.10), se plasma el concepto de seguridad informática, en qué se basa y sus principios fundamentales, de tal modo que cualquier usuario pueda comenzar a involucrarse en el tema y pueda entender con facilidad en qué consiste el tema.

La seguridad informática es un proceso, por lo que se incorpora el PDCA a la gestión de la seguridad de la información.



Cuando se habla de seguridad informática, lo primero que se debe hacer es contestar las siguientes preguntas:

¿Qué se quiere proteger?

Se debe identificar primeramente cuáles son los bienes que requieren protección.

¿De qué se quiere proteger?

Identificar cuáles son las amenazas que están presentes ante dichos bienes.

¿Cómo se quiere proteger?

Cuáles son los mecanismos de seguridad que se utilizarán para lograr la seguridad deseada.

Inicio

¿Qué es la Seguridad Informática?

La seguridad informática se refiere a todas aquellas medidas que se toman para impedir que se lleven a cabo actividades no autorizadas en un dispositivo o sistema informático, y que puedan causar algún daño en la información o en los equipos.

El PDCA también conocido como círculo de Deming, es una estrategia de mejora contínua que consiste en 4 pasos:

Plan (Planificar), es la primera fase del proceso, la cual consiste en evaluar los riesgos de seguridad que tienen los activos que se desean proteger, y definir la mejor forma de hacer frente a dichos riesgos.

Do (Hacer), es la siguiente fase mediante la cual se implementan las medidas y mecanismos definidos previamente para hacer frente a las amenazas y vulnerabilidades presentes, con la finalidad de proteger a los activos y evitar en lo posible los ataques informáticos.

Check (Verificar), consiste en realizar un análisis acerca de si realmente se están cumpliendo los objetivos con las medidas implementadas, de no ser así se debe realizar una replaneación sobre cómo se debe atacar el problema.

Act (Actuar), se realizan los cambios requeridos para obtener una mejora en el proceso y se cumplan con los objetivos iniciales.

Es muy importante que se preserve la seguridad de la información, ya que de no ser así se puede afectar gravemente la vida profesional y personal de las personas.

Diseñado por: María Fernanda Briseño Díaz

¿Para qué es la seguridad informática?

Figura 5.10: Definición de seguridad informática

El siguiente apartado: ¿Para qué es? (Figura 5.11), contiene los objetivos de la seguridad informática, y la descripción de los distintos servicios de seguridad que existen, para poder entender la finalidad del tema.

Figura 5.11: Objetivos de la seguridad informática

Continuando con el desarrollo de la página, en el siguiente apartado Amenazas (Figura 5.12), se define lo que es una amenaza y los distintos tipos que existen.

Figura 5.12: Amenazas

En el apartado de Vulnerabilidades (Figura 5.13), como su nombre lo dice se define lo que es una vulnerabilidad y los tipos que existen.

Figura 5.13: Vulnerabilidades

El siguiente apartado: Ataques (Figura 5.14), define lo que es un ataque, los tipos de ataques que existen, así como lo que es un perpetrador.

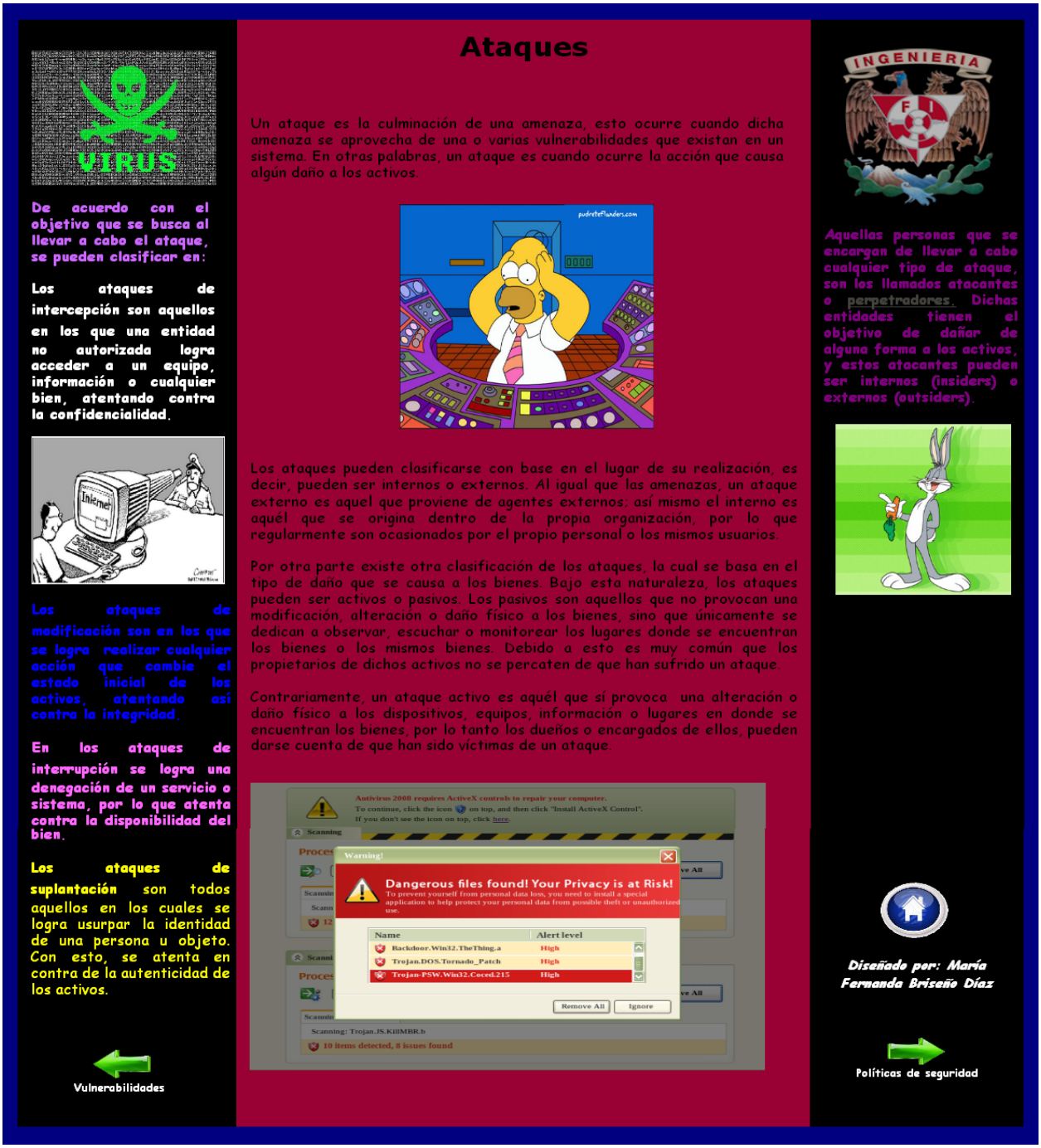


Figura 5.14: Ataques

En el apartado de Políticas de Seguridad (Figura 5.15) se define lo que son éstas, para qué sirven, quiénes intervienen en su creación, las filosofías que existen para su redacción y el modo en que deben ser redactadas para cumplir con los objetivos deseados.

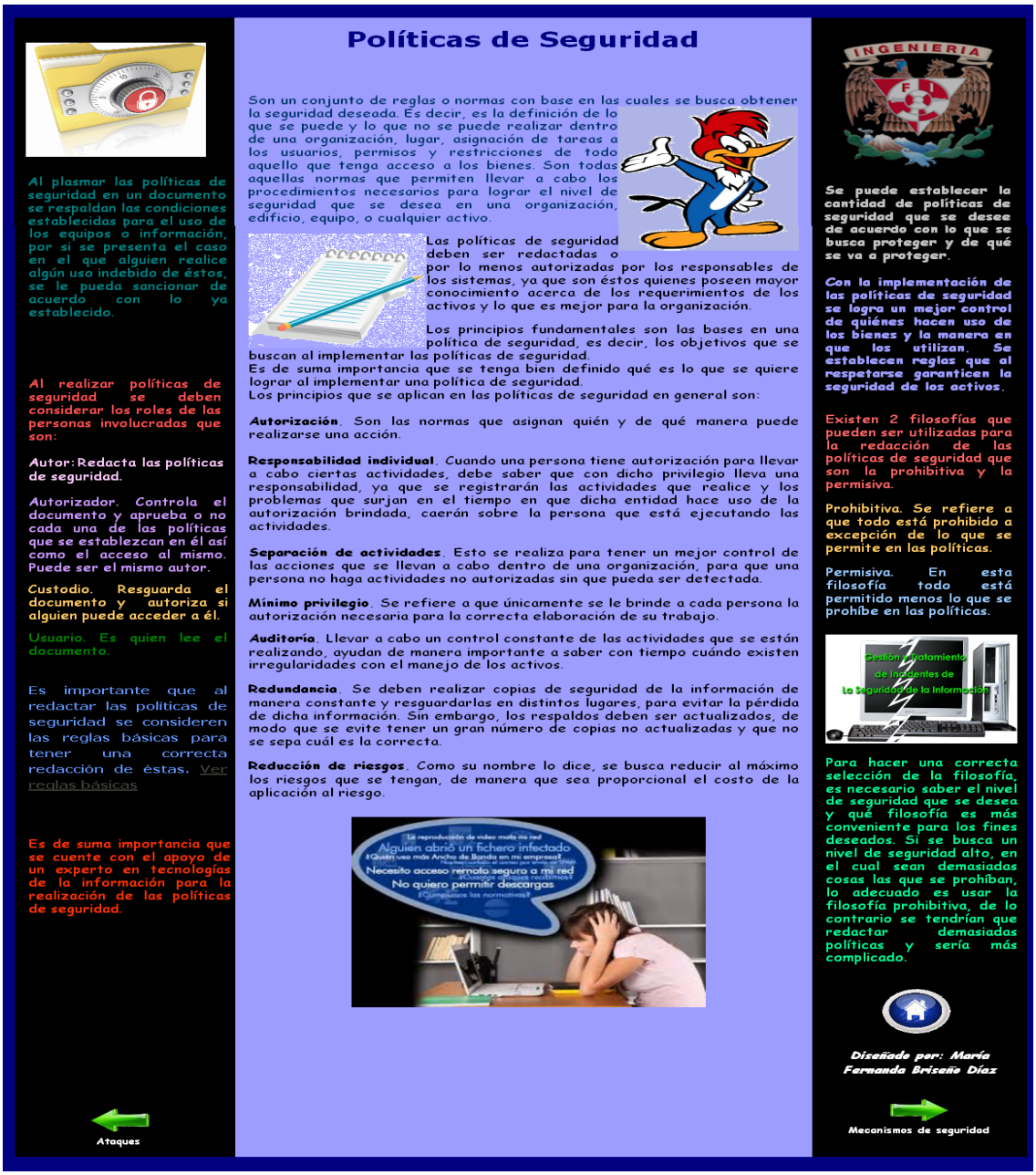


Figura 5.15: Políticas de seguridad

En el apartado de Mecanismos de Seguridad (Figura 5.16) se proporciona información acerca de este subtema para informar al usuario el modo en que puede proteger sus bienes.

Figura 5.16: Mecanismos de seguridad

En el penúltimo apartado: Principales problemas informáticos actuales (Figura 5.17), se proporciona información acerca de los principales problemas de seguridad informática que existen en la actualidad, de esta forma el usuario puede conocer el modo en que puede ser víctima de un ataque.

Figura: 5.17: Principales problemas informáticos

En el último apartado, Buenas Prácticas (Figura 5.18), se proporciona una serie de buenas prácticas de los diferentes aspectos más importantes en cuestiones de seguridad, para que los usuarios aprendan las medidas que pueden tomar para la protección de sus bienes.

Figura 5.18: Buenas prácticas

Con la información que se proporciona en el sitio web, se busca minimizar con facilidad los riesgos que sufran los usuarios en cuestiones de seguridad informática, tomando medidas de seguridad simples y fáciles de aplicar.

Además de estos apartados el sitio contiene un glosario de términos en el cual se definen algunos conceptos que se encuentren al consultar dicho sitio y que puedan resultar desconocidos para los usuarios. Así mismo se incluyen las referencias que fueron consultadas para la elaboración del sitio.

Finalmente se tendrá como objetivo mantener al día la información, de tal modo que los usuarios interesados en conocer más sobre el tema, sepan a dónde pueden acudir o qué sitios informativos pueden visitar y puedan ampliar sus conocimientos.

Con este sitio lo que se busca es comenzar la difusión de la seguridad informática con el objetivo de que a largo plazo se logre una cultura informática, y el tema en un futuro pueda ser visto con la importancia que le corresponde, no solo por los profesionales dedicados a la seguridad informática sino por la mayoría de los usuarios de los bienes informáticos.

Conclusiones

Como pudo visualizarse a lo largo de este trabajo, hoy en día es de suma importancia tomar medidas en cuestión de la seguridad informática. El nivel de impacto que representa el ser víctimas de un ataque informático es demasiado alto. Hoy en día por medio de los bienes informáticos se puede llegar a dañar la integridad profesional o personal de una persona u organización de manera realmente impresionante.

Es por ello que si bien la mayoría de los ataques son provocados por agentes externos, si no se toman las medidas de protección y cuidados por parte de cada uno de los usuarios, el nivel de impacto de dichos ataques es exponencialmente mayor.

De acuerdo con los resultados que se obtuvieron en la investigación realizada para la elaboración de este trabajo, si bien es una realidad que gran parte de los ataques que se sufren hoy en día son consecuencia de actividades realizadas o desencadenadas por los usuarios mismos, es una realidad que no se puede limitar a éstos el acceso a las herramientas o dispositivos, ya que dichas herramientas son necesarias para aumentar la productividad de los usuarios y organizaciones.

Para minimizar todos estos riesgos de seguridad que se tienen en los bienes informáticos, lo que se debe realizar es un análisis de lo que implica poner información en manos del usuario y posteriormente crear e implementar mecanismos de seguridad y planes de contingencia que ayuden a reducir las amenazas y vulnerabilidades que son causadas por dichos usuarios.

Con la implementación de dichos mecanismos, se logrará reducir de manera considerable la posibilidad de que los usuarios sean víctimas de ataques informáticos, pero una de las medidas que se deben tomar como parte de la seguridad, es la capacitación y concientización de las personas que hacen uso de los bienes informáticos.

Es de suma importancia que se comience a tratar el tema de la seguridad informática con la misma importancia que se le da a cualquier otro aspecto de seguridad como es la seguridad en las calles, en la escuela o en el hogar, ya que es tan importante como los anteriores. Por una parte se debe capacitar al personal de las organizaciones de acuerdo con el nivel de acceso que tengan a los bienes informáticos, y por otra es importante que se elaboren campañas de concientización para que todas las personas que tengan acceso a un activo informático también tenga acceso a la información que necesiten para conocer cómo debe cuidar dichos bienes y lo que debe y no debe realizar con éstos.

En la actualidad las personas acostumbran llevar información importante en sus dispositivos móviles a través del correo o en aplicaciones, por lo que se debe aprender de qué manera tienen que proteger sus recursos e intentar que si las personas no saben cómo utilizarlos, mejor no lo hagan hasta conocer el funcionamiento adecuado de éstos.

De acuerdo con Michael Kaiser, líder de la iniciativa nacional para educar a la gente sobre la importancia de navegar seguro en internet en los Estados Unidos, la estrategia de la NSCA (Alianza Nacional para la Ciberseguridad) ha sido procurar que la población estadounidense entienda la ciberseguridad como entiende las prácticas de seguridad cuando anda por la calle o cuando maneja. "El objetivo ha sido que la ciberseguridad se convierta en la segunda naturaleza, como cuando volteamos a ambos lados antes de cruzar una calle,

cuando usamos el cinturón de seguridad o cuando nos cubrimos con la parte interior del codo cuando tosemos".[157]

"Todas son prácticas de seguridad que adquirimos e interiorizamos como conductas que practicamos ya siempre, hábitos que hacemos automáticamente, de forma natural, de manera inconsciente. Las conductas que comprenden prácticas seguras deben ser aprendidas, pero alguien debe enseñarlas", explicó Kaiser.

Como puede visualizarse, los expertos en seguridad han considerado el tema abordado en esta tesis, por lo que es una realidad el hecho de que se debe comenzar a hacer difusión sobre la seguridad informática y a enseñarles a los usuarios todo lo básico en cuestión del tema para que aprendan a protegerse y a utilizar adecuadamente sus activos.

De este modo, si los usuarios conocen acerca del tema antes de hacer uso de los bienes informáticos, comprenderán los riesgos y aprenderán a evitar los problemas potenciales, sabiendo así que las acciones que estén realizando no tendrán un impacto en su seguridad posteriormente.

Todo esto es cuestión de hábitos. Es una realidad que inicialmente lograr una cultura en materia de seguridad informática será muy difícil y quizá llevará demasiado tiempo, sin embargo, con el transcurso de los años se logrará que el tema forme parte de la vida cotidiana de las personas y que la seguridad informática sea parte de sus rutinas diarias. Es por ello, que ya es tiempo de iniciar con dicho cambio y dicha concientización hacia los usuarios.

[157] http://www.bsecure.com.mx/featured/detente-piensa-y-conectate-creando-conciencia-al-navegar-en-internet/

Una vez que se les muestre a las personas el nivel de impacto que puede tener una brecha de seguridad informática en sus vidas, dichas personas comenzarán a tomar conciencia sobre las acciones que realizan cotidianamente en cuestión del uso de las herramientas informáticas, por lo que será más fácil hacer que la gente se interese en el tema y comprendan la importancia de la materia.

De este modo se puede concluir que la prevención es la mejor manera de enfrentar cualquier situación que puede poner en peligro la seguridad de una persona u organización. Al cumplir con la materia de seguridad en la información, se podrá hacer frente con mayor facilidad, a los incidentes que se presenten, logrando una recuperación en tiempo y forma, y al mismo tiempo minimizando las posibilidades de ser víctimas de un atacante informático, logrando que los usuarios puedan anticiparse ante cualquier posible amenaza, y puedan protegerse de cualquier acontecimiento.

Mientras no se mejore la conciencia y se instruya a los usuarios acerca de la importancia del tema, el hecho de vulnerar los activos de éstos y atacarlos, seguirá siendo relativamente tan sencillo como lo es en la actualidad, ya que en muchas de las veces, las víctimas de los ataques cibernéticos, ni siquiera tienen el conocimiento de que fueron atacados.

Todo esto puede resumirse en 2 palabras: educación y cultura. Si se fomenta la educación y cultura en materia de la seguridad informática, llegará el día en que los atacantes informáticos requieran más que la ingeniería social, herramientas de fácil manejo y un simple descuido del usuario para lograr sus objetivos.

Anexo: Encuesta

Presentación

Mi nombre es María Fernanda Briseño, vengo de la Facultad de Ingeniería y estoy realizando una encuesta acerca de los conocimientos que tienen las personas sobre el tema de Seguridad Informática. La información que proporcione será utilizada para realizar estadísticas sobre el mismo tema que serán evaluadas como tema de tesis y con la cual se busca brindar una solución para promover la cultura en dicho tema. Gracias

El siguiente cuestionario consta de 19 preguntas. En las preguntas abiertas responda en la línea o en el recuadro según corresponda y en las de opción múltiple marque con una cruz su respuesta. En algunos casos puede seleccionar más de una opción.

Perfil del encuestado

Edad		Sexo	Hombre	Mujer

Nivel de estudios: Básico Medio superior Licenciatura en: _____

Posgrado en: _____

Encuesta

1.- ¿Trabajas? Sí No ¿En qué?_____

2.- ¿Qué tan frecuentemente haces uso de un equipo de cómputo?

No uso	Ocasionalmente	Frecuentemente	Muy frecuentemente	Diario	Es una herramienta básica, es imprescindible para mí

3.- ¿Para qué utilizas los equipos de cómputo? (Puedes marcar más de una opción)

Trabajo Escuela Uso personal Comunicarme

Otra (por favor, especifique)	

4.- ¿Has tomado algún curso de computación? Sí No

Tu curso fue: De la escuela (Curricular) En la escuela pero extracurricular Externo a la escuela

5.- El o los cursos que tomaste de computación te sirvieron para obtener conocimientos en: (marca la opción que consideres de acuerdo con el grado de conocimientos que posees respecto a cada tema)

Tema	Escala				
	Insuficiente		Bien		Excelente
1. Windows	1	2	3	4	5
2. Linux	1	2	3	4	5
3. Otros sistemas operativos	1	2	3	4	5
4. Office	1	2	3	4	5
5. Otra paquetería	1	2	3	4	5
6. Manejo de internet	1	2	3	4	5

7.	Lenguajes de programación	1	2	3	4	5
8.	Reparación de computadoras	1	2	3	4	5
9.	Seguridad Informática	1	2	3	4	5

6.- De los siguientes recursos informáticos, indica cuáles utilizas: (Puedes marcar más de una opción)

PC o laptop Internet Ipod Teléfono celular Ipad Data center Servidores

7.- ¿Cómo proteges esos bienes?

_____
_____
_____

8.- ¿Qué servicios utilizas? (Puedes marcar más de una opción)

Correo electrónico Facebook Twitter Descarga de archivos
Búsqueda de información Servicios bancarios en línea Mensajería instantánea (Messenger)

9.- Cuál de los siguientes recursos posee en sus equipos informáticos o conoce a qué se refiere el término

Recurso	**Lo conozco**	**Cuento con él**
Antivirus		
Firewall		
Contraseña de acceso		
Antimalware		
Control biométrico		

10.- ¿Conoce los siguientes términos o sabe a qué se refieren?

	Sí	No
Keylogger		
Ataque informático		
Denegación de servicio		
Virus		
Gusano		
Troyano		
Spam		
Hacker		
Cracker		
Carding		
Perpetradores		
Malware		
Ingeniería social		
Conexión no segura		
Privilegios		
Exploit		

10.- Sabe usted que: (Marque las opciones de las que tenga conocimiento)

☐ Existen antivirus falsos ☐ Existe el robo de información ☐ Facebook es la red más insegura
☐ Existe el robo de identidad

11.- Para la elaboración de sus contraseñas usted usa:

☐ Fechas importantes ☐ Nombres de conocidos ☐ Palabras importantes
☐ Caracteres variados sin secuencia ☐ Otros(Especifique):_____

12.- Haces uso del correo electrónico para enviar:

☐ Tareas/Trabajo ☐ Mensajes personales ☐ Información privada ☐ Toda clase de información

13.- ¿Haces uso de conexiones públicas gratuitas? (Ejemplo: Aeropuertos, cafeterías, centros comerciales)

☐ Sí ☐ No

14.- ¿Utilizas estas conexiones del mismo modo que las privadas? (Ejemplo: La de tu casa)

☐ Sí ☐ No → ¿Por qué?_____

15.- ¿Sabía usted que el principal medio de propagación de virus es mediante las descargas de internet?

☐ Sí ☐ No

16.- ¿Qué navegador utilizas?

☐ Internet Explorer ☐ Mozilla ☐ Google Chrome ☐ Opera ☐ Otro

17.- Para usted es importante que sus recursos informáticos cuenten con:

☐ Disponibilidad ☐ Integridad ☐ Confidencialidad ☐ Autenticación
☐ Control de acceso ☐ No repudio

18.- ¿Cuál considera qué es la principal causa de un ataque informático?

_____

19.- ¿Qué entiende por seguridad informática?

_____

Glosario de Términos

Glosario de términos

Activo. Bien tangible o intangible. Cualquier elemento que tiene cierto valor para alguien, por lo que necesita algún tipo de protección.

Agente amenazante. Persona o proceso que puede atacar a los bienes, infringiendo las normas de seguridad.

Amazon. Compañía estadounidense de comercio electrónico.

Amenaza. Cualquier peligro potencial para la información o los sistemas.

Anonymous. Pseudónimo utilizado mundialmente por un grupo internacional de hacktivistas que se dedican a realizar ataques cibernéticos a manera de protesta ante las situaciones sociales.

Antispyware. Tipo de aplicación cuya funcionalidad es detectar y eliminar las programas espías que se filtran en los equipos de cómputo.

Antivirus. Programas cuya funcionalidad radica en detectar y eliminar los virus informáticos.

APT. Advanced Packaging Tool (Herramienta avanzada de empaquetado), es un sistema de gestión de paquetes.

Ataque. Método por el cual un individuo intenta tomar el control o causar algún daño a un sistema informático.

Autenticación. Acto por el cual se confirma la identidad de alguien.

Autenticidad. Calidad y carácter de verdadero o autorizado.

Bien. Activo. Cualquier objeto, sistema o persona que tiene importancia y valor para un individuo u organización.

BIOS. Basic Input/Output System (Sistema básico de entrada y salida), software que localiza todos los dispositivos para cargar el sistema operativo en la memoria RAM.

Blog. Sitio web que se actualiza periódicamente, recopilando información sobre algún tema.

Bomba lógica. Código malicioso insertado intencionalmente en algún programa informático. Dicho código permanece oculto hasta que se activa por medio de alguna acción ejecutada por el usuario, causando algún daño al equipo de éste.

Botnet. Conjunto de programas que se ejecutan de manera automática, logrando el control de los ordenadores.

Brechas de seguridad. Término referido a la existencia de algún hueco en la seguridad de un sistema. Rotura o falla de seguridad.

bSecure. Sitio Web en México dedicado a la seguridad informática.

bSecure Conference. Foro más reconocido de seguridad de la información en México.

BusinessWeek. Revista empresarial.

Carding. Término que se le da a cualquier tipo de ataque relacionado con las tarjetas de crédito (uso ilegal de éstas).

CC. Criterios Comunes. Proceso de evaluación mediante el cual se establece el nivel de confianza de un producto IT.

CCP. Empresa dedicada a soluciones de seguridad financiera.

CD. Compact Disk (Disco Compacto), medio digital óptico de almacenamiento de información.

Centro de cómputo. Centro de procesamiento de datos. Entidad que se encarga de la gestión de información mediante el uso de computadoras.

Certificación. Garantía que asegura la certeza o autenticidad de algo.

Ciberseguridad. Seguridad informática.

Cifrado. Proceso mediante el cual se vuelve ilegible la información.

Cisco. Empresa multinacional dedicada principalmente a la fabricación, mantenimiento y consultorías de equipos de redes.

Cloud. Cloud Computing.

Cloud Computing. Propuesta tecnológica que permite ofrecer servicios de cómputo por medio de internet.

Código. Texto escrito en algún lenguaje de programación que ha de ser interpretado por la computadora para ejecutar alguna acción.

Código Malicioso. Tipo de software que tiene como objetivo infiltrarse para dañar una computadora.

Confidencialidad. Propiedad de la información por la que se garantiza que únicamente está accesible para el personal autorizado.

Configuración. Conjunto de variables que controlan la operación general de un programa.

Contraseña. Clave. Forma de autenticación que utiliza información secreta para controlar el acceso a algún recurso.

Control biométrico. Control de acceso físico que autentica a las personas mediante sus características físicas.

Control de acceso. Conjunto de mecanismos mediante los cuales se limita el acceso a algún recurso, únicamente a personas autorizadas.

Correo electrónico. Servicio de red que permite a los usuarios enviar y recibir mensajes.

Crackear. Romper algún sistema de seguridad para acceder a la información de manera no autorizada.

Cracker. Persona que se dedica a crackear.

Cuarto de telecomunicaciones. Espacio cerrado en el que se almacena equipo de telecomunicaciones y terminaciones de cables.

Data center. Centro de datos, centro de cómputo.

DDos. Distributed Denial Of Service (ataque distribuido de denegación de servicios), ampliación del ataque DOS (Denial of service).

Delito cibernético. Término que se le da a las operaciones ilícitas realizadas mediante internet o que tiene como finalidad causar daños a los bienes informáticos.

Denegación de servicios. DOS (Denial of service), ataque a un sistema que causa la inaccesibilidad de un recurso o servicio.

Dirección IP. Etiqueta numérica que identifica de manera lógica a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP.

Disponibilidad. Cualidad de un recurso informático de encontrarse a disposición de acceder a éste cuando sea requerido.

Dispositivos. Periféricos auxiliares e independientes conectados a una red de computadoras.

Enciclomedia. Sistema de e-learning conformado principalmente por una base de datos didáctica. Se conforma por una computadora, un pizarrón electrónico y un proyector.

Error de capa 8. Problema causado por quien hace uso del equipo de cómputo, debido a que realiza algo incorrecto.

Exploit. Segmento de datos o secuencia de comandos que aprovechan un error o vulnerabilidad para violar las medidas de seguridad de un sistema para acceder al mismo de manera no autorizada.

Facebook. Sitio web de redes sociales.

Fiabilidad. Probabilidad de buen funcionamiento de un sistema.

Firewall. Parte de un sistema diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Fuga de información. Revelación de información no autorizada debido a errores en los procedimientos de trabajo.

Google. Empresa cuyo principal producto es el motor de búsqueda en internet.

Gusano. Malware que tiene la propiedad de duplicarse a sí mismo, causando un alto consumo de banda y recursos, por lo que los sistemas se vuelven lentos e inclusive inútiles.

Hacker. Persona con alta capacidad para el manejo de los bienes informáticos. Poseen grandes conocimientos y destreza para la utilización de los dispositivos de cómputo.

Hacktivismo. Uso no violento de herramientas informáticas para la ejecución de ataques informáticos con fines ideológicos.

Hardware. Partes físicas de un sistema informático.

HTML. Hypertex Markup Language (lenguaje de marcado de hipertexto), lenguaje para la elaboración de páginas web.

ID. Nombre de usuario o identificador.

IMEI. International Mobile Equipment Identity (identidad internacional de equipo móvil), código que identifica un teléfono móvil y es transmitido por éste al conectarse a la red.

IMSI. International Mobile Suscriber Identity (identidad internacional de suscripción de equipo móvil), es un código de identificación único para cada dispositivo de telefonía, que está integrado al SIM.

Ingeniería Social. Práctica mediante la cual se obtiene información confidencial mediante la manipulación de los usuarios.

Integridad. Cualidad de los recursos informáticos que se refiere a que se mantengan en su estado ideal, es decir que no sean modificados por ninguna razón.

Internet. Conjunto de redes de comunicación mundialmente interconectadas entre sí.

Intrusión. Acción de introducirse a algún lugar, red o dispositivo sin tener autorización para ello.

iOS. Sistema operativo móvil desarrollado por Apple para los dispositivos de dicha marca iPhone, iPod Touch, iPad.

ISC. Empresa dedicada a la consultoría en seguridad informática.

IT. Tecnologías de la información.

Kaspersky Lab. Empresa especializada en productos para la seguridad informática.

Keylogger. Tipo de software o dispositivo que registra las pulsaciones que se ejecutan en el teclado.

Likejacking. Amenaza que afecta a las redes sociales, mediante el botón like de éstas. Al dar click en dicho botón se publica en el muro de los usuarios enlaces de malware.

Link. Referencia de un documento de hipertexto a otro documento o recurso.

Malware. Código malicioso.

McAfee. Compañía de software de seguridad informática.

MessageLabs. Proveedor de servicios integrados de mensajería y seguridad para sitios web.

Monitoreo. Supervisión y control de las actividades registradas en un sistema o red.

MVS. Estación de radio de noticieros en México.

MySpace. Servicio de red social.

NASA. National Aeronautics and Space Administration (administración nacional de aeronáutica y del espacio), agencia gubernamental de Estados Unidos responsable de los programas espaciales.

Netbook. Ordenador portátil de reducidas dimensiones, utilizado principalmente para navegar en internet y funciones básicas como los procesadores de texto y hojas de cálculo.

No repudio. Característica mediante la cual no se puede negar la participación de alguna de las entidades implicadas en la comunicación.

Nube. Cloud

Oracle. Compañía de software especializada en la gestión de bases de datos.

Ordenador. Computadora.

Panda Security. Empresa informática especializada en la creación de soluciones de seguridad informática.

PandaLabs. Red de laboratorios de investigación de virus.

Paquetería. Programa informático diseñado para facilitar determinadas tareas del usuario.

PC. Personal Computer (computadora personal), computadora diseñada para ser usada por un usuario a la vez.

PDA. Personal Digital Assistant (asistente personal digital), es un ordenador de bolsillo u organizador personal.

Perpetrador. Atacante.

Phishing. Delito informático que consiste en adquirir información confidencial de manera fraudulenta.

Piratería informática. Reproducción, apropiación y distribución de medios y contenidos sin permiso del autor.

Políticas de seguridad. Conjunto de reglas mediante las cuales se describe el uso que se debe hacer de los bienes.

Post. Mensaje o entrada en algún blog, grupo de noticias, foro o red social.

Privacidad. Control de quién puede acceder a la información y quién no.

Privilegios. Permisos que posee un usuario para hacer uso de algún recurso.

Protocolo. Conjunto de reglas usadas por computadoras para comunicarse unas con otras por medio de una red.

Red. Conjunto de equipos informáticos conectados entre sí, los cuales comparten recursos e información.

Redes sociales. Estructuras sociales compuestas por grupos de personas que intercambian y comparten información haciendo uso del internet.

RFC. Request For Comments (Mecanismo de petición de comentario). Protocolos que sirven de referencia para la comunidad de internet.

Ringtones. Tonos para celular.

Rogueware. Scareware.

Scareware. Software mediante el cual se estafa a los usuarios engañándolos de que es necesario la instalación de éste para la mejora de sus equipos. Una vez instalado, se provocan daños y obtención de información del usuario de manera ilícita.

Seguridad. Ausencia de riesgo. Conjunto de protecciones mediante las cuales se resguarda algún bien.

Seguridad informática. Protección de la infraestructura computacional y todo lo relacionado con ésta, software, bases de datos, etcétera.

Servidores. Computadora que provee servicios a otras.

SIM. Suscriber Identity Module (módulo de identificación del suscriptor), tarjeta inteligente usada para identificarse en la red.

Sistema informático. Conjunto de hardware y software que permite almacenar y procesar información.

Sistema operativo. Conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático y que permite la ejecución de las operaciones.

Sitios web. Colección de páginas web relacionadas y comunes a un dominio

Smartphones. Teléfono inteligente, teléfono móvil que ofrece más funciones que un teléfono celular común.

Software malicioso. Software malintencionado que se infiltra en las computadoras para provocar algún daño en éstas.

Software. Equipamiento lógico de un sistema. Programas y aplicaciones de un equipo de cómputo.

Spam. Correo basura recibido vía electrónica sin ser solicitado.

SpyEye. Tipo de malware muy avanzado y peligroso para los sistemas.

Spyware. Software que recopila información de un ordenador y después lo transmite a una entidad externa sin el consentimiento del propietario.

Symantec. Corporación internacional que desarrolla y comercializa software para computadoras particularmente de seguridad informática.

Tablets. Computadora portátil con la que se puede interactuar a través de una pantalla táctil.

Tecnologías de la información. Elementos y técnicas usadas para el tratamiento y gestión de la información.

TI. Tecnologías de la información.

Troyano. Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, que al ejecutarlo provoca daños en los sistemas.

Twitter. Red social basada en el envío y publicación de mensajes breves.

URL. Uniform Resource Locator (localizador de recursos uniforme), secuencia de caracteres de formato estándar, que se usa para nombrar recursos en internet para su localización o identificación.

Virus. Malware que altera el normal funcionamiento de una computadora sin consentimiento del usuario.

Voucher. Recibo de pago.

Vulnerabilidad. Deficiencia de seguridad de un sistema o recurso informático. Debilidad.

Web 2.0. Aplicaciones web que facilitan el compartir información en internet.

Wikileaks. Organización mediática internacional que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materias de interés público.

Wikis. Sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web.

XSS. Cross Site Scripting, tipo de inseguridad informática basado en la explotación de vulnerabilidades del sistema de validación HTML.

Zero-day. Día cero. Ataque basado en encontrar vulnerabilidades aún desconocidas en las aplicaciones informáticas.

Referencias

Referencias

- Calle Guglieri José.A, Reingeniería y Seguridad en el Ciberespacio, , Editorial Díaz de Santos, Madrid, España, 1997
- López Barrientos María Jaquelina, Fundamentos de seguridad Informática, 1ª. Edición, UNAM, Facultad de Ingeniería, México D.F, 2006.
- Royer Jean-Marc, Seguridad en informática de la empresa: Riesgos, amenazas prevención y soluciones, Colección Recursos Informáticos, Ediciones ENI, Barcelona, España, 2004.
- Libro electrónico de seguridad informática y criptografía: 21 de abril de 2011 http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- Revista Digital Universitaria: La seguridad informática y el usuario final: 21 de noviembre de 2011 http://www.revista.unam.mx/vol.9/num4/art20/int20.htm
- Revista Seguridad, Defensa digital, UNAM, Número 11, Agosto 2011. http://revista.seguridad.unam.mx/
- RFC 1244: Site Security Handbook. J. Reynolds - P. Holbrook. Julio 1991
- América Latina necesita mayor profesionalización en IT: 12 de julio de 2011 http://www.bsecure.com.mx/featured/america-latina-necesita-mayor-profesionalizacion-en-seguridad-it/
- Ataque contra android: 25 de abril de 2011 http://www.bsecure.com.mx/featured/aprovechan-actualizacion-de-seguridad-para-reinfectar-a-usuarios-de-android/
- Ataque contra usuarios de Facebook: 25 de Abril de 2011 http://www.bsecure.com.mx/featured/averigua-quien-robo-tu-cuenta-en-facebook/
- Ataque DDos contra WordPress: 25 de abril de 2011 http://www.bsecure.com.mx/featured/por-segundo-dia-consecutivo-wordpress-sufre-el-mayor-ataque-de-ddos-en-su-historia/
- Ataques DDos crecen durante el 2011: 25 de Abril de 2011

http://www.bsecure.com.mx/featured/ataques-ddos-crecen-22-durante-2011-estudio/

- Alerta en empresas por uso de redes sociales de empleados: 25 de abril de 2011 http://www.bsecure.com.mx/featured/empresas-deben-estar-alerta-por-uso-de-redes-sociales-de-empleados/
- Amenazas en cine, música y tecnología: 19 de abril de 2011 http://www.bsecure.com.mx/featured/musica-cine-tecnologia-y-ciberamenazas-en-el-sxsw/
- Anonymous tumba sitios de Sony: 12 de julio de 2011 http://www.bsecure.com.mx/featured/anonymous-cumple-lo-prometido-tumba-sitios-de-sony/
- Ataque de Robo de información: 21 de abril de 2011 http://www.bsecure.com.mx/featured/atacan-rsa-y-roban-informacion-de-clientes-de-secureid/
- Aumentan brechas de información: 21 de noviembre de 2011 http://www.bsecure.com.mx/featured/brechas-de-informacion-aumentan-7-durante-2010-generan-perdidas-por-7-2-mdd/
- Bendita ignorancia que nada da y mucho quita: 06 de julio de 2011 http://www.bsecure.com.mx/opinion/bendita-ignorancia-que-nada-da-y-mucho-quita/
- Botnet más poderosas de 2010: 25 de abril de 2011 http://www.bsecure.com.mx/ultimosarticulos/las-10-botnet-mas-poderosas-de-2010/
- Cibercriminales se mudan de la PC al dispositivo móvil: 25 de abril de 2011 http://www.bsecure.com.mx/featured/cibecriminales-siguen-la-tendencia-se-mudan-de-la-pc-al-dispositivo-movil/
- Clientes de Sony podrían haber facilitado el robo de información: 27 de julio de 2011 http://www.bsecure.com.mx/ultimosarticulos/clientes-de-sony-podrian-haber-facilitado-el-robo-de-informacion/
- Cloud Malware, robo de datos y dinero a domicilio

http://www.bsecure.com.mx/featured/el-cloud-malware-robo-de-datos-y-dinero-a-domicilio/

- Conceptos de seguridad informática: 21 de abril de 2011 http://es.wikibooks.org/wiki/Seguridad_inform%C3%A1tica
- Creando conciencia al navegar en internet: 12 de julio de 2011 http://www.bsecure.com.mx/featured/detente-piensa-y-conectate-creando-conciencia-al-navegar-en-internet/
- Debate sobre seguridad en la nube y en dispositivos móviles: 21 de abril de 2011 http://www.bsecure.com.mx/featured/expertos-en-seguridad-ti-debaten-sobre-diversas-tecnologias/
- Definición de estándar: 21 de abril de 2011 http://enciclopedia.us.es/index.php/Est%C3%A1ndar http://www.wordreference.com/definicion/est%C3%A1ndar
- Diariamente son hackeadas más de 600,000 cuentas de facebook: 21 de noviembre de 2011 http://www.bsecure.com.mx/featured/diariamente-son-hackeadas-600000-cuentas-de-facebook/
- El Periférico de ciudad Ciberseguridad: 27 de julio de 2011 http://www.bsecure.com.mx/featured/el-periferico-de-ciudad-ciberseguridad/
- Empresas carecen de políticas IT de uso de celulares, PDA y PC: 12 de julio de 2011 http://www.bsecure.com.mx/ultimosarticulos/mitad-de-empresas-carecen-de-politicas-it-de-uso-de-celulares-pda-y-pc/
- Espionaje corporativo y terrorismo son principales causas de pérdidas de datos: 21 de noviembre de 2011 http://www.bsecure.com.mx/ultimosarticulos/espionaje-corporativo-y-terrorismo-son-principales-causas-de-perdida-de-datos/
- Facebook busca evitar que la curiosidad genere robo de cuentas: 12 de julio de 2011 http://www.bsecure.com.mx/featured/facebook-busca-evitar-que-curiosidad-sea-responsable-del-robo-de-cuentas/

- Facebook infecta usuarios vía correo electrónico: 25 de abril de 2011
  http://www.bsecure.com.mx/featured/facebook-infecta-usuarios-a-traves-de-correo-electronico/
- Facebook y Twitter fallaron en la última evaluación de seguridad: 27 de julio de 2011
  http://www.securecomputing.net.au/News/237848,facebook-twitter-fail-latest-security-assessment.aspx
- Faceworm o la era de amenazas para las redes sociales: 12 de julio de 2011
  http://www.seguridad.unam.mx/doc/?ap=articulo&id=219
- Falso antivirus distribuido vía Twitter: 25 de Abril de 2011
  http://www.idg.es/pcworldtech/Twitter_-amenazado-por-una-estafa-de-falso-antivir/doc105175-actualidad.htm
- Fraudes en línea generan más de 300,000 quejas al año: 27 de junio de 2011
  http://www.bsecure.com.mx/featured/fraudes-en-linea-generan-en-eu-mas-de-300000-quejas-al-ano/
- Hackean perfil del fundador de facebook: 25 de abril de 2011
  http://www.bsecure.com.mx/ultimosarticulos/hackean-pagina-en-facebook-del-fundador-de-facebook/
- Hacktivismo: ¿Para qué?: 12 de julio de 2011
  http://www.bsecure.com.mx/opinion/hackivismo-como-para-que/
- Hactivistas de anonymous:14 de Abril de 2011
  http://www.noticiasmvs.com/noticias/capital/los-hacktivistas-de-anonymous-atacan-una-firma-de-seguridad--606.html
- Infecciones informáticas: 21 de abril de 2011
  http://www.fundaciotrams.org/full/full8/virus.pdf
- ISO 27000: 05 de marzo de 2011
  http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-degestion/estandares-esquemas/ISOIEC-27001/
  http://iso27000.wik.is/Area_Normas
- ISO 27000: 21 de abril de 2011
  http://www.iso27000.es/download/doc_iso27000_all.pdf

http://es.wikipedia.org/wiki/ISO/IEC_27000-series

- Ley de protección de datos personales en México: 12 de julio de 2011
  http://www.bsecure.com.mx/featured/mexico-con-una-de-las-leyes-de-proteccion-de-datos-personales-mas-modernas-del-mundo/
- Limitados, los recursos para enseñanza de inglés y computación: 21 de noviembre de 2011
  http://www.oem.com.mx/laprensa/notas/n1085982.htm
- Lo malo de creer que Cameron Díaz es tu amiga en Facebook: 27 de julio de 2011
  http://www.bsecure.com.mx/opinion/cameron-diaz-es-mi-amiga-en-facebook-ahh-no-es-un-apt/

- Los carteristas de la web son los cibercriminales: 12 de julio de 2011
  http://www.bsecure.com.mx/featured/los-carteristas-de-la-web-son-los-cibercriminales-video/
- McAfee libera software seguridad para smartphones con android: 12 de julio de 2011
  http://www.bsecure.com.mx/ultimosarticulos/mcafee-libera-software-seguridad-para-smartphones-con-android/
- Mexicanos expuestos al robo de identidad por medidas de protección deficientes: 24 de junio de 2011
  http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion- deficientes-estudio/
- Mulas, smartphones y redes sociales: las preferencias del cibercrime: 21 de noviembre de 2011
  http://www.bsecure.com.mx/featured/mulas-smartphones-y-redes-sociales-las-preferencias-del-cibercrimen/
- Nuevos ataques DDOS en los sitios web más importantes: 25 de octubre de 2011
  http://msmvps.com/blogs/harrywaldron/archive/2010/02/02/push do-botnet-new-ddos-attacks-on-major-web-sites.aspx
- Pérdida de datos por espionaje corporativo y terrorismo: 25 de abril de 2011

http://www.bsecure.com.mx/ultimosarticulos/espionaje-corporativo-y-terrorismo-son-principales-causas-de-perdida-de-datos/

- Plan de contingencias, indispensable: 12 de junio de 2011 http://www.bsecure.com.mx/featured/apoyo-directivo-indispensable-para-asegurar-continuidad-de-ti-empresarial/
- Políticas de seguridad de la información: 21 de abril de 2011 http://www.segu-info.com.ar/politicas/polseginf.htm

- Primer paso en seguridad IT, ser proactivo: 12 de julio de 2011 http://www.bsecure.com.mx/opinion/el-primer-paso-en-seguridad-it-ser-proactivo/
- Qué hacer cuando el antivirus no da el ancho: 12 de julio de 2011 http://www.bsecure.com.mx/featured/que-hacer-cuando-el-antivirus-no-da-el-ancho/
- Qué tan seguros son los smartphones: 12 de julio de 2011 http://www.bsecure.com.mx/featured/que-tan-seguros-son-los-smatphones/
- Red botnet Cutwail: 25 de abril de 2011 http://www.bsecure.com.mx/featured/cutwail-revive-la-red-botnet-responsable-de-mas-de-4-millones-de-perfiles-apocrifos/
- Robo de identidad en México: 27 de junio de 2011 http://www.bsecure.com.mx/featured/mexicanos-expuestos-a-robo-de-identidad-por-medidas-de-proteccion-deficientes-estudio/
- Troyanos, responsables del 70% de los ataques en 2011: 25 de abril de 2011 http://www.bsecure.com.mx/featured/troyanos-arma-favorita-de-ciberdelincuentes-en-2011/
- Un 2011 riesgoso en materia de seguridad informática: 12 de julio de 2011 http://www.bsecure.com.mx/featured/un-2011-riesgoso-y-urgente-de-cambio/
- Uso de contraseñas reduce productividad: 25 de Abril de 2011

http://www.bsecure.com.mx/ultimosarticulos/el-uso-de-contrasenas-reduce-productividad-y-no-ofrece-seguridad/

- Vulnerabilidad en los bancos: 21 de abril de 2011
  http://www.bsecure.com.mx/ultimosarticulos/los-bancos-podrian-ser-vulnerados-por-medio-de-ingenieria-social/
- Viajando con información de forma insegura: 19 de abril de 2011
  http://www.bsecure.com.mx/opinion/viajando-con-informacion-de-forma-insegura%E2%80%A6/
- Víctimas de ciberfraudes no denuncian por vergüenza: 27 de julio de 2011
  http://www.bsecure.com.mx/ultimosarticulos/victimas-de-ciberfraudes-no-denuncian-por-verguenza/
- Virus generados en el 2010: 27 de junio de 2011
  http://www.theinquirer.es/2011/01/03/la-tercera-parte-de-todos-los-virus-de-la-historia-se-han-generado-en-2010.html
- Zeus resurge: 21 de abril de 2011
  http://www.bsecure.com.mx/featured/zeus-aun-no-ha-muerto-el-virus-resurge-tras-unirse-al-troyano-spyeye/