CAPÍTULO VI

VI. SEGURIDAD DE LA INFORMACIÓN Y ÉTICA EN INFORMÁTICA.

Debido a que el uso de Internet se encuentra en aumento, cada vez más las compañías permiten a sus clientes, socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección, para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información.

Adicional es importante aplicar la ética en el manejo de la información y todas las actividades desarrolladas en un entorno informático.

1.1 Seguridad informática.

La seguridad informática es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática. Es una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización.

Objetivos de la seguridad informática.

Entre los objetivos de la seguridad informática podemos mencionar:

- Proteger los recursos informáticos del daño, la alteración, el robo y la pérdida de equipos, medios de almacenamiento, software y los datos
- Mantener la continuidad de los procesos organizacionales que soportan los sistemas de información

1.1.1 En sistema de computadora.

Las computadoras son utilizados para realizar incontables tareas, tales como: transacciones financieras, sean ellas bancarias o compra de productos y servicios; comunicación, por ejemplo, a través de e-mails; almacenamiento de datos, ya sean personales o comerciales, etc. por lo cual es de gran importancia la seguridad en las computadoras.

Son muchas las amenazas que se corren en la privacidad al navegar por la Web, mientras se está conectado a internet, sin saberlo, alguien pudiese estar entrometiéndose en la computadora para acceder a los datos y a cualquier información de interés para cualquier ilícito a provocar. Esta situación se vuelve aún más crítica, si la computadora no tiene instalada un antivirus actualizado u otras herramientas para la protección de la computadora.

1.1.2 En sistema operativo.

La seguridad de los sistemas operativos son mecanismos para controlar el acceso de los programas, procesos o recursos definidos por un sistema. Se debe mantener

el sistema operativo y el software de su computadora actualizado. Esto le ayudará a eliminar las vulnerabilidades de seguridad en su software o sistema operativo.

1.1.3 En sus redes.

La seguridad en redes es mantener bajo protección los recursos y la información que se encuentra en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

1.2 Medidas de seguridad.

Las medidas de seguridad es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, las probabilidades de ocurrencia de las amenazas y el impacto en la organización. Existen herramientas para garantizar la seguridad como los antivirus, parches, copias de seguridad, entre otras.

1.3 Amenazas (Malwares).

Amenazas son cualquier evento accidental o intencional que puede ocasionar algún daño e el sistema informático, provocando perdidas materiales o financieras dentro de la organización. Los malware son códigos malignos o software malicioso con el objetivo de infiltrarse o dañar una computadora. Incluye virus, gusanos, troyanos, etc.

1.3.1 Spam.

Se le llama spam a mensajes de email no deseados o no solicitados que provienen de un remitente que usted no conoce. Los emails de spam se mandan en grandes volúmenes y su contenido es casi idéntico.

El spam se divide en dos categorías:

Mensajes que molestan, como solicitaciones para que compre productos o servicios.

Emails maliciosos que buscan engañarlo para que usted revele su información personal para que alguien pueda defraudarlo o dañar su computadora.

La gran mayoría del spam pertenece la primera categoría:

1.3.2 Phishing.

Phishing se refiere a la captación de datos personales realizada de manera ilícita o fraudulenta a través de internet. Es una palabra del inglés que se origina de su homófona “fishing”, que significa ‘pesca’, en alusión al objetivo del phishing: pescar datos, ver “quién muerde el anzuelo”. El phishing es ejecutado por un phisher o 'pescador'.

El phishing es una técnica de ingeniería social que emplea el envío masivo de correos electrónicos spam en nombre de una entidad bancaria, con la finalidad de obtener datos personales y financieros (principalmente aquellos asociados a claves de acceso), o de redirigir a los usuarios a una página web falsa de la entidad donde estos tengan que depositar sus datos.

Como rasgos característicos, los correos de phishing suelen solicitar al usuario, con carácter de urgencia, la confirmación o el envío de determinados datos bajo la excusa de problemas técnicos, cambios en la política de seguridad, detección de posibles fraudes, promociones o concursos. Incluso, puede incorporar la

fórmula coactiva de que si el usuario no realiza la acción solicitada inmediatamente, su tarjeta o cuenta podrá ser bloqueada.

1.3.3 Virus.

Un virus informático es un malware que tiene por objetivo alterar el normal funcionamiento del ordenador sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

1.3.4 Troyanos.

Los troyanos son software malicioso que se le presenta al usuario como un programa legitimo, pueden crear una puerta trasera que permite la administración remota.

1.3.5 Gusanos

Se duplica a sí mismo, se propaga sin la ayuda de una persona, causan problemas en la red.

1.3.6 Ramsomware**.**

- ✓ Restringe el acceso a archivos o partes del sistema.
- ✓ Piden un rescate a cambio de eliminar la restricción.
- ✓ Cifra los archivos con una clave que solo el creador conoce.
- ✓ Se propaga como un Troyano o Gusano.

1.4 Ataques.

Los ataques son acciones que vulneran la confidencialidad, integridad y disponibilidad de la información. Ejemplo de ataques virus, spam, troyanos, gusanos, entre otros.

1.4.1 Ingeniería social

Es el conjunto de técnicas y trucos empleados por intrusos y hackers para extraer información sensible de los usuarios de un sistema informático.

1.4.2 Denegación de servicio

También llamado ataque DoS (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

1.5 Privacidad y confidencialidad de la información.

1.5.1 Definición

La privacidad se define como el derecho de mantener de forma reservada o confidencial los datos de la computadora y los que intercambia con su red. Existen herramientas para garantizar la privacidad de la información: criptografía, contraseñas, firewall, etc.

La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

1.5.2 Computadoras y privacidad: amenazas

Es esencial mantener su computadora segura para proteger su privacidad, reducir el riesgo del robo de identidad y evitar que los hackers controlen su computadora. Desafortunadamente, no siempre es fácil proteger su computadora. Los hackers con frecuencia parecen estar un paso más adelante del público, incluso de las personas que utilizan los mejores métodos de seguridad

1.5.3 Protección a la privacidad.

Para proteger su privacidad e información sensitiva usted necesita tomar varias medidas, incluyendo prevenir, detectar y responder a una gran variedad de ataques. Hay muchos riesgos, y unos son más serios que otros. Algunos de los peligros son:

- ✓ Virus que infectan todo su sistema.
- ✓ Personas que entran a su sistema y hacen modificaciones a sus archivos.
- ✓ Hackers que usan su computadora para atacar a otros.
- ✓ Ladrones que roban su computadora y su información personal.

No existen garantías de que algunas de estas cosas no sucedan, incluso si usted toma las mejores precauciones. Sin embargo, usted puede tomar medidas para minimizar los riesgos a su computadora e información personal. Finalmente, la seguridad de su computadora depende de usted.

1.6 Aspectos éticos de la profesión y Responsabilidades.

1.6.1 Propiedad Intelectual.

La propiedad intelectual, es toda creación del intelecto humano. Los derechos de propiedad intelectual protegen los intereses de los creadores al ofrecerles prerrogativas en relación con sus creaciones.

1.6.2 Plagiarismo.

El plagiarismo es una infracción al derecho de autor a cerca de una obra artística o intelectual de cualquier tipo, en la que se incurre cuando se presenta una obra ajena como propia u original.

1.6.3 Software pirata.

El software pirata es un programa que ha sido duplicado y distribuido sin autorización. Una serie de actividades se podrían considerar como piratería de software, la más común es cuando se hace múltiples copias de un programa para luego venderlas sin pagar ningún tipo de regalías al creador de dicho software.

La piratería de software daña su reputación del fabricante porque el software pirata puede estar defectuoso o cargado de malware. El software pirata es inseguro, puede ser utilizado para recoger información personal, cargar una

computadora con virus, o participar en otras actividades que perjudican a los usuarios.

1.6.4 **Derechos de copia**.

Es una limitación al derecho exclusivo que la ley concede al autor y al propietario de contenidos a hacer copias de ellos.

1.6.5 Ética y responsabilidades en el manejo de la información.

La Ética en la informática estudia la forma de tratar los problemas que involucran el uso de la información, garantizar que los métodos que son utilizados para transformar la información sean los correctos.

La cantidad de información disponible en internet es gigantesca, por lo que el usuario debe tener en cuenta ciertos valores para hacer uso de la misma, tales como:

- Respeto hacia a las opiniones ajenas y la propiedad intelectual.
- Responsabilidad por las opiniones emitidas, que no deben ofender o dañar a terceros.
- Prudencia para distinguir el tipo de contenido que se observa en Internet.
- Actitud critica frente a las opiniones e información mostradas en internet, así como en cualquier otro medio de comunicación.

1.6.5.1 Ética en general.

La ética es una disciplina que analiza problemas de valores y principios morales que son creados por la tecnología de los ordenadores analizando los impactos de la tecnología de la información en los valores humanos y sociales. La tarea de la ética informática consiste en crear guías de actuación cuando no hay reglamentación o cuando la existente es obsoleta.

1.6.5.2 Concepto de ley y su diferencia con la ética.

La ley y la ética son dos mundos que están relacionados, pero que no necesariamente se identifican. Primero, porque la ética es más amplia que la ley: hay aspectos del actuar humano donde la ley no debe entrar; pero, aunque esas acciones no estén reguladas por la ley, siguen siendo objeto de valoración ética.

Otro aspecto es que las leyes las hacemos los seres humanos, y de vez en cuando los seres humanos se equivocan y pueden hacer leyes que sean inmorales.