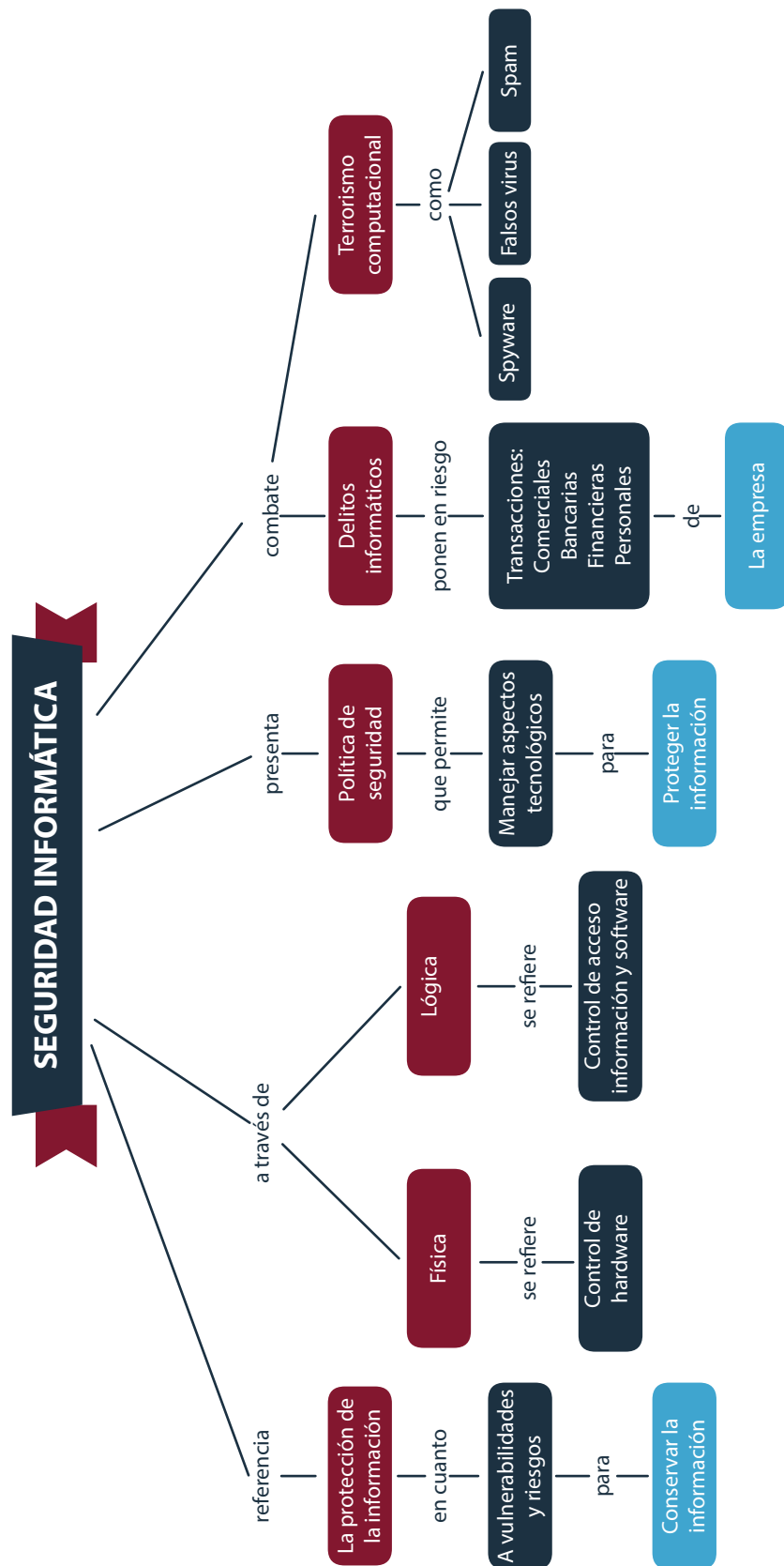


SEGURIDAD INFORMÁTICA

INTRODUCCIÓN	3
1. GENERALIDADES	4
2. SEGURIDAD LÓGICA - FÍSICA	5
¿QUÉ ES LA SEGURIDAD LÓGICA Y QUÉ ES LA SEGURIDAD FÍSICA?	5
LA SEGURIDAD LÓGICA	6
LA SEGURIDAD FÍSICA	
3. POLÍTICA DE SEGURIDAD INFORMÁTICA	7
4. DELITOS INFORMÁTICOS	8
5. TERRORISMO COMPUTACIONAL	10
BIBLIOGRAFÍA	11
GLOSARIO	12







INTRODUCCIÓN

Debido a la globalización, a los grandes avances tecnológicos, las empresas u organizaciones deben estar a la vanguardia en sus procesos informáticos, por lo cual deben asegurar su infraestructura computacional a través de todo su sistema de procesamiento y almacenamiento de datos de tal manera que se garantice la confidencialidad, integridad y disponibilidad de los mismos en el momento en que se requiera.

La seguridad física y lógica de la información cada vez más está siendo amenazada por el incremento en los delitos informáticos y el terrorismo computacional, es por eso que las organizaciones se deben encontrar preparadas para no dejar ninguna vulnerabilidad en su sistemas y utilizar todos los recursos a su alcance para proteger todos los recursos computacionales y de información estratégicos para el negocio.



1. GENERALIDADES



La informática hace referencia a todos los recursos que están relacionados con el manejo de la información, como es conocido la información viene a representar el motor en la era digital en la que nos estamos moviendo. Dada la importancia de esta información para todos los procesos en una organización será necesario mantenerla segura, para que se encuentre en donde se necesita, en el momento que se necesita y en las condiciones que es requerida.

Estos recursos informáticos pueden sufrir diferentes daños los cuales pueden provenir tanto del interior como del exterior de la organización. Por ejemplo: Robo, destrucción, uso no autorizado. Deben existir controles que de alguna manera realicen actividades de prevención, detección y corrección de cualquier problema con los recursos informáticos. Las estadísticas de ataques informáticos muestran que más del 70% provienen de gente que se encuentra dentro de la organización, la cual tiene el conocimiento de las vulnerabilidades de los sistemas y de cuáles son los datos más sensibles en una organización.

La información se encuentra expuesta a muchos riesgos a lo largo de todo su manejo, desde que es generada, hasta que es almacenada. Es por eso que las empresas deben establecer políticas de seguridad de tipo lógico y físico. Ambas de la misma importancia para conservar a la información segura.

Se hace necesario que las empresas dicten estrategias que les permiten disminuir los niveles de vulnerabilidad y llevar una administración eficiente de riesgos a esto se le conoce como políticas de seguridad.

El uso de las telecomunicaciones incrementa sin lugar a dudas los riesgos a los cuales se enfrenta la información en una empresa. Dado que el acceso a la información se puede realizar desde cualquier lugar del mundo. Las empresas encuentran que su información está expuesta a diferentes riesgos, entre ellos los más conocidos son: virus, caballos de troya, gusanos, códigos maliciosos. No se puede olvidar a los hackers quienes han sofisticado su manera de atacar a las empresas, descubriendo vulnerabilidades sobre los sistemas para lograr accesos no autorizados y dañar la información.

Conceptos

Algunos conceptos relacionados con la seguridad informática son:

Activo Recurso necesario para el funcionamiento de la organización y el cumplimiento de objetivos.

Riesgo Posibilidad de que algo suceda sobre uno o más activos de la organización.

Impacto El resultado de que una amenaza ocurra.

Amenaza Evento que al ocurrir ocasionaría un daño sobre los activos.

Vulnerabilidad Posibilidad de que ocurra una amenaza sobre un activo.

2. SEGURIDAD LÓGICA - FÍSICA

¿Qué es la seguridad lógica y qué es la seguridad física?



La seguridad informática por lo regular se concentra más en la seguridad lógica que en la seguridad física ya que se piensa que por ahí pueden llegar más ataques, pero muchas empresas llegan a dejar caminos abiertos de manera física y resulta que es más fácil acceder directamente al sitio haciendo una copia de un archivo desde el mismo lugar en donde este se encuentra.

La seguridad lógica

Tiene que ver con todo lo relacionado con el control de acceso a la información y software, por ejemplo el llevar un control de quién acceso a una base de datos para consultar o para modificar información. Se puede decir que una empresa está protegiendo su seguridad lógica cuando:

- Las personas autorizadas son las que hacen uso de los archivos y programas.
- Los procesos y programas utilizan los datos correctos.
- La información que se envía por lo red llega a al destinatario correctamente.

- La comunicación falla y se tienen procesos alternativos.
- Los operadores realizan sus tareas y no se les permite modificar datos o programas.
- Utiliza Firewalls.
- Utiliza y actualiza Antivirus.
- Utiliza y actualiza Antispyware.
- Actualiza los sistemas y los servidores continuamente.
- Desactiva los servicios de red que no se utilizan.
- Utilizar sistemas de detección de intrusos.
- Crear respaldos (backups).
- Uso de passwords.
- Codificación de información (Criptografía).
- Utilizar software con garantía (no pirata).
- Reducir los permisos de usuarios.
- Monitorear la entrada a la red por correo, páginas de web y la entrada a bases de datos desde laptops.

Aunque los puntos anteriores no son todos los que se deben considerar, permiten tener un panorama para definir los aspectos que deben ser cubiertos por políticas de seguridad lógica.

La seguridad física

Va enfocada a la aplicación de barreras físicas y procedimientos de control relacionados con todo el hardware utilizado para el manejo de información incluyendo los dispositivos de almacenamiento y los medios utilizados para el acceso remoto, aquí también es necesario incluir los edificios y sitios en donde se tiene la información.

Cuando una empresa está pensando y actuando teniendo en mente los riesgos tanto naturales como humanos, a los cuales se enfrentan sus instalaciones puede comenzar por establecer políticas y procedimientos de seguridad física. Por ejemplo: protección contra incendios, terremotos, huracanes, humedad, motines, disturbios sociales, robos, sabotajes, alteración en equipo sensible, fallas en equipo etc.

Se puede hacer uso de los siguientes puntos para disminuir los riesgos que atentan contra la seguridad física: guardias, detectores de metales, sistemas biométricos, verificación automáticas de firmas, protección electrónica, etc. Estos así, como otras medidas de seguridad deben ser evaluadas para ser implementadas como políticas de seguridad informática en la empresa.



3. POLÍTICA DE SEGURIDAD INFORMÁTICA



El establecimiento de una política de seguridad informática es una necesidad para las empresas que utilizan las redes como una forma de mejora en procesos y de poder competir en un mundo globalizado.

Las políticas vienen a representar una forma consensuada de hacer y manejar todos los aspectos tecnológicos de la organización ya que de no hacerlo así podrían ocasionar serios problemas a la organización.

Las políticas de seguridad deberán ser definidas tomando en cuenta riesgos y vulnerabilidades y sobre todo deberán estar actualizándose constantemente ya que al estar relacionadas con aspectos tecnológicos sus consideraciones cambian con gran rapidez.

Las políticas de seguridad informáticas deben ser definidas tomando en cuenta lo que se debe proteger y el porqué se debe proteger y por supuesto, deben tomar en cuenta al personal que hace uso de esa información o de los recursos y redactarlas en un lenguaje que sea comprensible para ellos

La seguridad informática tiene un dicho: "lo que no está permitido debe estar prohibido" pero esto no se logra fácil. Es necesario establecer una política de seguridad siguiendo un procedimiento en donde se analizan los riesgos a los cuales está expuesta la información y los recursos tecnológicos con los que cuenta la empresa.

El establecimiento de dichas políticas debe ser de arriba hacia abajo en la organización ya que requiere de un apoyo económico pero también de dirección muy importante para hacer que esto tenga éxito y no sea considerado como algo superficial que no tiene impacto en la empresa.

El error de muchas empresas es pensar que a sus sistemas y a sus recursos informáticos nunca les pasará nada, es por eso que nos encontramos con frases como las siguientes:



Mi sistema no es importante para un hacker.

Por lo tanto no le pongo passwords. Un hacker y un Virus entran a donde puede así que si le dejas la puerta abierta entrará y ya estando ahí tomará lo que se le antoje.



Estoy protegido pues no abro archivos que no conozco. Los sistemas realizan acciones sin necesidad que el usuario lo supervise o autorice a veces los usuarios desconocen y aceptan algunas operaciones que pueden resultar peligrosas para el sistema.



Como tengo antivirus estoy protegido. No basta con esto, es necesario estar actualizando el antivirus y en ocasiones ni esto es suficiente dado que se genera el virus y después el antivirus.



Como dispongo de un firewall no me contagio. El contagio puede realizarse por usuarios con altos privilegios a los cuales el sistema de firewall puede estar permitiendo accesos autorizados por supuesto.

4. DELITOS INFORMÁTICOS



El uso de la tecnología en todos los ámbitos incluyendo industrial, comercial, gubernamental, social y personal ha permitido que estos sectores se desarrollen y sean mucho más eficientes en todas sus operaciones o tareas. Sin embargo es importante mencionar que también el uso de estos recursos tecnológicos permite que se incrementen las formas en que se pueden cometer delitos.

El delito informático se puede definir como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento electrónico de datos y/o transmisiones de datos.
















Como ya se mencionó anteriormente, el desarrollo tecnológico también puede ocasionar que la delincuencia se extienda de maneras que no se habían contemplado con anterioridad. Los servidores pueden ser manejados con el fin de lograr dañar datos y programas o hacer uso no autorizado de la información. Los daños pueden llegar a ser tanto materiales como de tipo ético o moral. Se considera que el impacto en los daños por un delito computacional es muy superior al ocasionado con la delincuencia tradicional y a eso tendríamos que agregarle que la manipulación de la tecnología de una manera astuta permite que estos delitos no puedan ser descubiertos y ni siquiera puedan ponerse una pena o multa a quien lo realiza.

La facilidad de acceso a los datos de alguna manera provoca que delitos como fraude o estafas se den de una manera rápida y sencilla.

Qué ha resultado mal en todo este uso de tecnología como es que la información puede estar tan expuesta a ser destruida o robada. Están en riesgo desde transacciones comerciales, bancarias, financieras, personales que día a día se manejan en la red. Nos enfrentamos a la existencia de personas sin escrúpulos que agrupadas o de forma individual hacen mal uso de la información que los sistemas contienen para satisfacer sus intereses personales. A medida que la tecnología siga evolucionando también se encontrarán delitos que lo harán.

Actualmente existen diferentes legislaciones que de alguna manera tratan de proteger la información contra los delitos. Estas legislaciones son definidas por cada país, dependiendo de la protección que se quiera dar a la información.

A continuación se listan algunas acciones que se pueden realizar utilizando el computador y son considerados delitos computacionales:

-  Acceso no autorizado.
-  Destrucción de datos.
-  Estafas electrónicas en comercio electrónico.
-  Falsificación o alteración de documentos (tarjetas de crédito, cheques, etc).
-  Transferencia de fondos no autorizado.
-  Leer información confidencial (robo o copia).
-  Modificación de datos de entrada / salida.
-  Utilizar sin autorización programas computacionales.
-  Alterar el funcionamiento del sistema (poner virus).
-  Obtención de reportes residuales impresos.
-  Entrar en áreas de informática no autorizadas.
-  Planeación de delitos convencionales (robo, fraude, homicidios)
-  Intervenir líneas de comunicación.
-  Interceptar un correo electrónico.
-  Espionaje, terrorismo, narcotráfico, etc.

5. TERRORISMO COMPUTACIONAL



Cuando se habla de terrorismo computacional se viene a la cabeza virus, hackers y otros conceptos que han venido posicionándose como elementos no deseados cuando se habla de uso de tecnología de información.

A continuación se presentan algunos tipos de virus:

Spyware: Es un espía que se encuentra en el computador que vigila todo las acciones que se realizan, y de alguna forma obtiene gracias a los hábitos de navegación sus gustos y preferencias. ¿Qué se hace con esta información? Es vendida y utilizada para publicidad en el mejor de los casos, pero en el peor de los casos puede afectar su información.

Hoaxes o Falsos Virus: Son correos que lo único que pretenden es saturar la red u obtener listas de correos, estos mensajes logran captar la atención de los usuarios ya que apelan a la buena voluntad de las personas para ayudar a alguien enfermo o al deseo de hacerse millonario, reenviando el correo, así como también a la esperanza de que se cumpla un milagro por hacer el envío de 7 correos o más en menos de 7 horas, por mencionar algunos ejemplos.

Spam: Tipo de Malware que es un correo electrónico que no ha sido solicitado por quien lo recibe y normalmente es de contenido publicitario y es enviado de forma masiva.

Es muy importante para una empresa tener el conocimiento de los elementos que pueden afectar su seguridad, por lo que deberá tomar en cuenta los aspectos tanto físicos como lógicos para darse una idea de que debe implementar para protegerse, por otra parte es importante que las personas encargadas de la seguridad informática en la organización puedan establecer políticas de seguridad informática para la organización, las cuales deben estar apoyadas por la alta administración y transmitidas en un lenguaje adecuado para todas las personas relacionadas con el uso de tecnología de información y con todo el procesamiento electrónico de datos.

Las legislaciones varían dependiendo del país en donde se viva, aunque hay una tendencia que se tenga un estándar, ya que estamos en un mundo globalizado. Se deben conocer los delitos y virus informáticos a los que más se está expuestos, para establecer políticas de protección adecuada en la organización.



BIBLIOGRAFÍA

Galdámez P. (s.f). Seguridad informática. Actualidad TIC. Recuperado de: <http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf>

Ley 1273 de 2009. Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Recuperado de: <http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf>

Manjarrés, I; Jiménez F. (2012) Caracterización de los delitos informáticos en Colombia. Recuperado de: <http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/view-File/126/149>

Valdés, M. (s.f). Departamento de sistemas de información. Instituto Tecnológico y de estudios superiores de Monterrey. México.

GLOSARIO

ACTIVO: Recurso necesario para el funcionamiento de la organización y el cumplimiento de objetivos.

AMENAZA: Evento que al ocurrir ocasionaría un daño sobre los activos.

IMPACTO: El resultado de que una amenaza ocurra.


RIESGO: Posibilidad de que algo suceda sobre uno o más activos de la organización.

SPAM: Correo electrónico que no ha sido solicitado por quien lo recibe y normalmente es de contenido publicitario y es enviado de forma masiva.


SPYWARE: Software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador

VULNERABILIDAD: Posibilidad de que ocurra una amenaza sobre un activo.

OBJETO DE APRENDIZAJE	SEGURIDAD INFORMÁTICA
Desarrollador de contenido Experto temático	María Imelda Valdés Salazar Elsa Cristina Arenas Martínez
Asesor Pedagógico	Elsa Cristina Arenas Martínez Juan José Botello Castellanos
Productor Multimedia	Adriana Marcela Suárez Eljure Víctor Hugo Tabares Carreño
Programadores	Adriana Rocío Pérez Rojas
Líder línea de producción	Santiago Lozada Garcés


Atribución, no comercial, compartir igual

Este material puede ser distribuido, copiado y exhibido por terceros si se muestra en los créditos. No se puede obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.



Creative Commons