Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Fundamentos de seguridad informática / Carlos Arturo Avenía Delgado, / Bogotá D.C., Fundación Universitaria del Área Andina. 2017

978-958-5459-61-8

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

Edición:
Fondo editorial Areandino
Fundación Universitaria del Área Andina
Calle 71 11-14, Bogotá D.C., Colombia
Tel.: (57-1) 7 42 19 64 ext. 1228
E-mail: publicaciones@areandina.edu.co
http://www.areandina.edu.co

Primera edición: noviembre de 2017

Corrección de estilo, diagramación y edición: Dirección Nacional de Operaciones virtuales
Diseño y compilación electrónica: Dirección Nacional de Investigación

Hecho en Colombia
Made in Colombia

Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

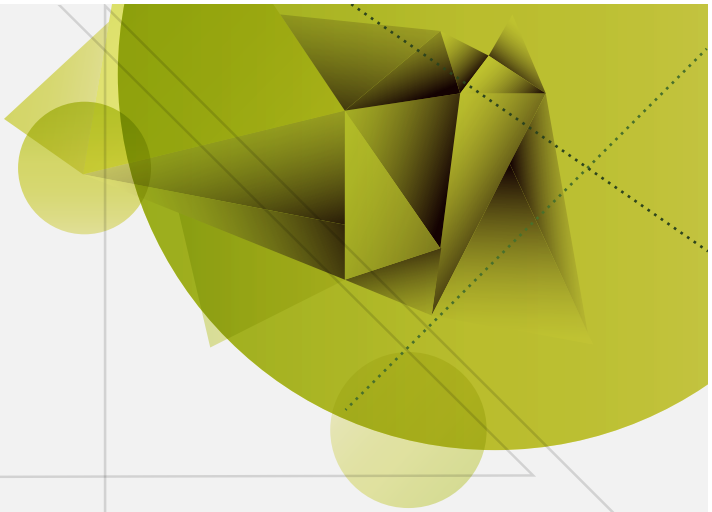
Índice

Índice

1

Unidad 1

Introducción y conceptos básicos de la seguridad informática



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Seguridad de TI es minimizar los riesgos asociados con el acceso y el uso de cierta información del sistema de forma no autorizada y, en general maliciosamente. Este punto de vista de la seguridad implica la necesidad de una gestión, sobre todo la gestión de riesgos. Para ello, debe evaluar y cuantificar los activos a proteger (información), y en base a estos análisis, aplicar medidas preventivas y correctoras para eliminar los riesgos asociados o para reducirlos a niveles que puedan transmitir o tomar el riesgo.

Imagen 1

Fuente: http://www.hanoberkk.net/images/tecnologiahanob/suguridad.jpg

En general, cualquier persona consideraría razonable contratar a un agente de seguridad exclusivamente para proteger su hogar o negocio, puede ser una gran medida de seguridad para evitar el acceso no autorizado, sin embargo, muy pocos podrían considerar simplemente por razones económicas. Después de evaluar el valor de los bienes a proteger, lo de siempre consideraría otras medidas más en línea con el valor de nuestros activos.

Podríamos pensar en una puerta blindada, compartido con otros vecinos o incluso unos sensores basados en el servicio de seguridad privada, alarmas y marcar con un mostrador de seguridad central. La combinación de estas medidas preventivas con otra correctiva, ya que podría ser una póliza de seguro contra el robo, queremos llegar a un nivel de seguridad que podría considerarse adecuada. A menudo, sin hacer explícitamente, nos hubiera evaluado el valor de nuestros activos, riesgos, el costo de las medidas de seguridad disponibles en el mercado y el nivel de protección que ofrece.

En seguridad informática, los principios mostrados por nuestro ejemplo la seguridad en el hogar son igualmente aplicables. Las únicas diferencias aparecen por las características técnicas asociadas a los sistemas informáticos. La valoración económica de los bienes a proteger a menudo puede ser una tarea compleja, la casuística de los grandes riesgos potenciales, y la complejidad y variedad de medidas de seguridad disponibles dificulta su selección. Sin embargo, la línea de fondo sigue siendo el mismo, la seguridad consiste en la protección de una entidad con una serie de riesgos y en este caso los riesgos relacionados con los sistemas informáticos.

En el módulo vamos a dar una visión general de los aspectos más importantes de la seguridad de la información, comenzando con una visión de la seguridad como parte integrante de la gestión empresarial, vamos a seguir con la descripción de las amenazas más comunes que pueden comprometer los sistemas informáticos y la descripción de las medidas más eficaces para contrarrestarlos.

U1 Metodología

En aras de un adecuado acercamiento al conocimiento puesto en juego y a la adquisición de habilidades que se pretende desarrollar, inicialmente se recomienda al estudiante tener siempre presente la guía de actividades y objetivos correspondientes a cada una de las semanas. En lo que concierne a cada una de las cartillas se recomienda su cuidadosa lectura, ya que realmente representan un punto de partida o puerta de entrada a recursos que le contribuirán a desarrollar habilidades relacionadas con las temáticas tratadas.

U1

Desarrollo temático

Introducción y conceptos básicos de la seguridad informática

Definiciones

¿Qué es la seguridad?

La seguridad tiene múltiples usos. En términos generales, se puede decir que este concepto proviene del latín *securitas* se centra en la propiedad de seguro, es decir, mejorar la propiedad de algo donde hay peligro, daño o la comprobación de riesgos. Una cosa es segura es algo fuerte, cierta e indudable. La seguridad, por lo tanto, puede ser considerada como una certeza.

¿Qué es información?

En cuanto a su definición, se puede decir que es la acción de la presentación de informes, sobre la base de un informe de noticias sobre algo, declarar aprendido. Este término también se utiliza para referirse a los conocimientos que añade a los que ya posee en una zona determinada, y por extensión, se llama de esta manera también a esos conocimientos.

También se puede definir como el conocimiento emitió o relativas organizó un evento o circunstancia, que se genera por una parte, en la mente de la gente y por el otro, transmitida o expresa algún tipo de apoyo, ya que puede ser la televisión, la radio, periódico, ordenador, etc. de esto también se puede inferir que es la manera de comunicar el conocimiento que hace que el pensamiento humano.

La información puede existir en muchas formas:

- Puede ser impresa o escrita en papel.
- Almacenada electrónicamente,
- Transmitida por correo o por medios electrónicos,
- Presentado en imágenes, o
- Expuesta en una conversación

¿Qué es riesgo?

El riesgo es la posibilidad de que una amenaza se provoque, lo que resulta en un equipo sea un ataque. Esto no es más que la probabilidad de que el ataque se produzca por parte de la vulnerabilidad que se encuentra por la amenaza.

El riesgo es principalmente el análisis de vulnerabilidades en un sistema informático. El riesgo permite tomar decisiones para proteger mejor el sistema. Se puede comparar con el límite para aceptar riesgos en un ordenador, por lo que si el riesgo calculado es inferior a la de referencia, se convierte en un riesgo residual que podemos considerar el riesgo forma aceptable.

¿Qué es Informática?

La informática se refiere al **procesamiento automático de información** mediante **dispositivos electrónicos y sistemas computacionales**. Los sistemas informáticos deben contar con la capacidad de cumplir tres tareas básicas: **entrada** (captación de la información), **procesamiento** y **salida** (transmisión de los resultados). El conjunto de estas tres tareas se conoce como **algoritmo**.

Imagen 2
Fuente: http://www.educanet.com.mx/wp-content/uploads/2015/04/Aula-Clases-Tablet.jpg

¿Qué es Amenaza?

Una amenaza para un sistema informático es una circunstancia que tiene el potencial de causar daños o pérdidas. Es decir, las amenazas pueden dar lugar a un ataque en el equipo.

Ejemplos de amenazas son los ataques de personas, como los desastres naturales que pueden afectar a su equipo. Ellos también pueden ser considerados amenazas faltas cometidas por los usuarios para utilizar el sistema, o fallas internas tanto de hardware como de software cómo.

¿Qué es vulnerabilidad?

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

Ingeniería social

En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

¿Qué es seguridad de la información?

Es la protección de la información y de los sistemas de información del acceso, uso, divulgación y destrucción no autorizada a través de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recursos humanos.

La seguridad de la información protege a esta de una amplia gama de amenazas, a fin de garantizar la continuidad de una organización.

Imagen 3
Fuente: https://dtyoc.files.wordpress.com/2016/01/seguridad_informatica.jpg

No importando la forma que se adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser Protegida en forma adecuada.

¿Por qué es importante la seguridad de la información?

Porque la información, los procesos, sistemas y redes de apoyo son activos organizacionales importantes y en algunos casos estratégicos.

Porque definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, a nivel del flujo de caja, rentabilidad, observancia legal e imagen organizacional.

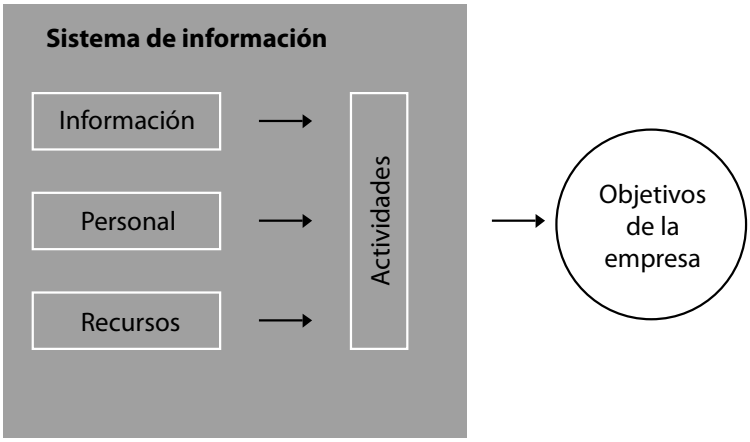


Figura 1
Fuente: Propia.

El 94 % de las empresas que pierden su información desaparece.

Donde es más vulnerable nuestra información:

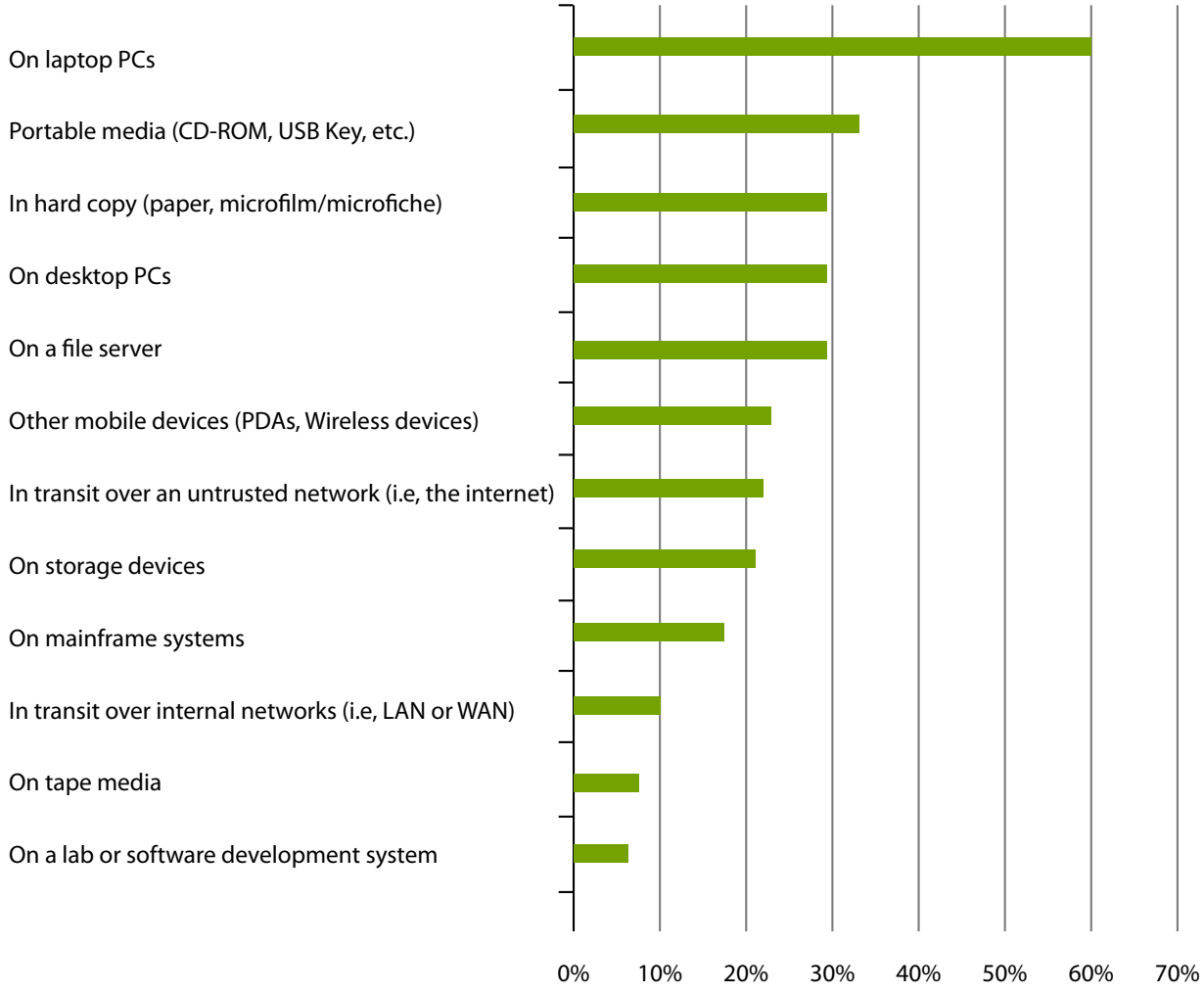


Figura 2
Fuente: Propia. (basado en Informe de investigación de ESG, Protecting Condential Data Revisited).

Según gráfica anterior se evidencia que la mayor vulnerabilidad de muestra información están en nuestros medios de trabajo Laptos PCs, dado que son herramientas que siempre están conectadas a una Red o en un entorno laboral donde siempre se buscara la manera de poder ingresar a información empresarial o institucional con algún fin, más del 90% del robo de información son por errores humanos atados a la inconciencia de la persona.

Un sistema de información siempre tendrá una margen de riesgo, para poder afrontar esta tipo de riesgo es necesario conocer:

a. Los elementos que componen el sistema, este tipo de información se obtiene mediante entrevista a los responsables o directivos de la organización.
b. Los peligros que afectan los sistemas, que pueden ser accidentales o provocados, de este modo se tratan de deducir mediante los factores que la organización ha estipulado según los activos y mediante la realización de estudios o pruebas sobre el sistema.
c. Las medidas que se deberían adoptar para poder conocer, prevenir, impedir, reducir o controlas cualquier tipo de riesgo. Estas medidas abarcan toda la parte de la infraestructura a nivel de hardware y software, personal humano y ambientales.

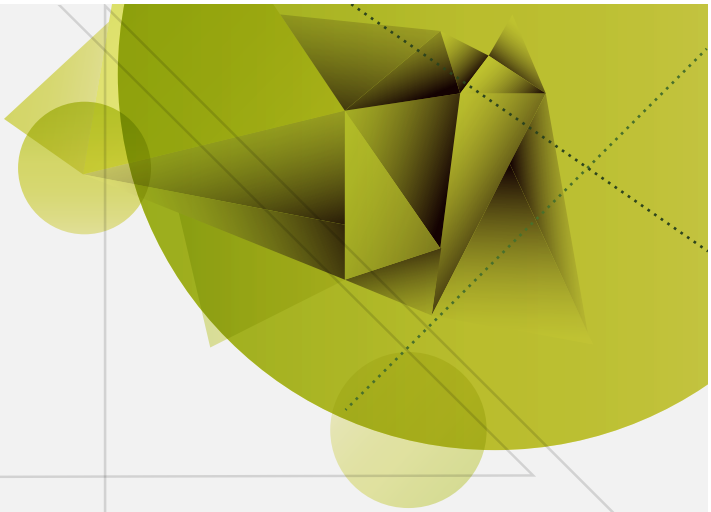
Imagen 4

Fuente: http://static.batanga.com/sites/default/files/styles/full/public/tech.batanga.com/files/Seguridad-informatica-cuidado-con-el-uso-de-una-sola-contrasena-1.jpg?itok=0dk9WIXa

1

Unidad 1

Historia la seguridad informática



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

El objetivo de la seguridad informática es proteger los valiosos recursos informáticos de la organización, tales como la información, hardware o software. A través de la adopción de las medidas adecuadas, la seguridad de TI ayuda a la organización a cumplir sus objetivos, la protección de sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros activos tangibles e intangibles. Por desgracia, a veces se ve a la seguridad informática como algo que dificulta la consecución de los mismos objetivos de la organización, la imposición de reglas y procedimientos rígidos a los usuarios y administradores de sistemas. Pero debe mirar a la seguridad informática, no como un objetivo en sí mismo sino como un medio para apoyar el logro de los objetivos de la organización.

En general, el principal objetivo de las empresas lucrativas y públicas, es proporcionan un servicio eficiente y de calidad a los usuarios. En las empresas privadas, la seguridad informática debe apoyar el capital socioeconómico. A esto los sistemas deben estar protegidos para evitar posibles pérdidas, que podrían causar la degradación de la funcionalidad del sistema o el acceso de personas no autorizadas.

El fin de esta cartilla es poder conocer la historia de la seguridad informática y cada uno de los aspectos que dieron a conocer y posicionar la seguridad informática como uno de los activos vitales en las empresas y/o hogar, dando un lugar a entender y concientizar sobre los peligros eminentes y los errores que una persona o empresa puede cometer, convirtiéndose en un riesgo o amenaza.

U1 Metodología

En aras de un adecuado acercamiento al conocimiento puesto en juego y a la adquisición de habilidades que se pretende desarrollar, inicialmente se recomienda al estudiante tener presente la guía de actividades y objetivos correspondientes a cada una de las semanas. En lo que concierne a cada una de las cartillas se recomienda su cuidadosa lectura, ya que realmente representan un punto de partida o puerta de entrada a recursos que le contribuirán a desarrollar habilidades relacionadas con las temáticas tratadas.

Analizar cada uno de los hechos relevantes en la historia sobre la seguridad informática, con el fin de estudiar cómo fueron los primeros indicios y pasos para darse como un tema critico en el transcurso del tiempo. Entender los principios bases de la seguridad y alguno de los errores comunes que se presentan en la seguridad informática.

U1

Desarrollo temático

Historia la seguridad informática

Historia

Fecha	Antecedente
1948	Von Neumann ya daba conferencias hablando de la autorreproducción de las maquinas. Solo el sentido común le decía que las maquinas serian capaz de reproducirse por sí solas si contaba con las moléculas necesarias.
1959	En este año, en el laboratorio de Bell Computers, tres jóvenes: Robert Thomas Morrison, Douglas McIlroy y Víctor Vysottsky crean un juego denominado *CoreWar*, basado en la teoría de Von Neumann. *CoreWar* (el precursor de los virus informáticos) es un juego donde programas combaten entre sí con el objetivo de ocupar toda la memoria de la maquina eliminando así a los oponentes.
1970	El Dr. Gregory Benford (Físico y escritor de ciencia ficción) publica la idea de un virus informático en el número del mes de mayo de la revista Venture Magazine describiendo el término "*computer virus*" y dando como ejemplo un programa llamado "*Vacuna*" para eliminarlo.
1972	*Creeper.* Se trata del primer virus de la historia. Nació en 1971 y dejó huella porque infectó los computadores PDP-11, los cuales estaban conectados a red de computadores precursora de Internet, Arpanet. Una de las características de *Creeper* es que mostraba un mensaje que infectaba el sistema y decía: "Soy el más aterrador *(creeper);* atrápame si puedes". Fue creado por Robert Thomas Morris, quien trabajaba para la empresa BBN, en la misma que se encontraba el creador del correo electrónico, Ray Tomlinson. A partir de este virus se creó para eliminarlo el programa Reaper, que tenía la capacidad de distribuirse a los equipos infectados tan rápido como el virus.

1973	Un año después del virus *Reaper*, se crea la vacuna para dicho virus llamado *Reaper*. Es un misterio la creación de dicha vacuna, solo se especula que pudo haber sido el mismo creador del virus. Arpanet era una red que estaba militarizada, por lo que también se piensa que se mantuvo en el anonimato el nombre del programador, ya que estaban probando la fortaleza de dicha red. Se puede decir que aquí nace el primer antivirus, aunque no lo es como los que hoy conocemos, pero cuenta con las características necesarias para llamarlo antivirus.
1975	En enero de 1975, John Walker (*Creador de Atudesk*), descubre una nueva forma de distribuir un juego en su UNIVAC 1108 y sin darse cuenta da vida al primer virus *troyano*. Se llama *Animal/Pervade*; *Animal* porque consistía en que el software debía adivinar el nombre de un animal en base a preguntas realizadas por un usuario y *Pervade* porque era la rutina capaz de actualizar las copias de *Animal* en los directorios de los usuarios cada vez que era ejecutado, de ahí viene el nombre *troyano.*
1980	Se fundamentan las bases de la seguridad de la información. James P. Anderson escribe un documento titulado '*Computer Security Threat Monitoring and Surveillance'*, donde se da una definición de los principales agentes de las amenazas informáticas como "ataque" o "vulnerabilidad".
1984	Fred Cohen usa la palabra virus para definir un programa que se reproduce a sí mismo.
1986	En este año se detecta la primera epidemia de virus totalmente compatible con las IBM PC. Este virus llamado (c) *Brain* fue desarrollado por el programador pakistaní Basiq Farrq Alvi y sus hermanos Shajid y Amjad. En el mismo año Ralf Burger creó otro virus llamado "*Virdem*" que infectaba archivos ejecutables .COM y estaba programado para autorreproducirse y borrar archivos del sistema huésped. En 1987 Burger escribe un libro sobre los virus informáticos donde revelaba el código del virus *Virdem* y cómo solucionarlo manualmente, generando mucha polémica, ya ahora cualquier persona podría crear su propio virus, y así fue, durante los próximos años se desencadenó una enorme cantidad de virus nuevos basados en este código.
1988	El 30 de noviembre ha sido declarado "**Día Internacional de la Seguridad informática**" desde 1988, con el objeto de concientizar sobre la importancia de la seguridad de la información y de los sistemas y entornos que operan con ella.

1989	Aparece el poderoso virus "*Datacrime*" el cual formateaba a bajo nivel el cilindro cero (donde se aloja el FAT) del disco y que solo actuaba del 13 de octubre hasta el 31 de diciembre. El mismo año se lanzó la vacuna "*anti-datacrime*" el cual tuvo muchos errores pero gracias a este acontecimiento, comenzó el mercado de los antivirus. En este mismo año aparecen otro grupo de compañías dedicadas a programar y vender antivirus como lo eran S&S, F-Prot, ThunderByte y el IBM Virscan.
1990	Al 18 de diciembre de 1990 la lista de antivirus era la siguiente: *Antivirus Plus de Iris, Artemis (Panda), Certus, Data Physician, Dr. Solomon's Antivirus Toolkit, F-Prot, ThunderByte, Turbo Antivirus, Virex-PC, Vaccine, V-Analyst, Vet, Virscan, VirusBusters, Virucide, Virusafe y Viruscan*.
2001	*Code Red.* El 13 de julio de 2001 por primera vez se conoció acerca de este gusano que se propagaba por las redes sin necesidad de un correo electrónico o un sitio web. El objetivo de *Code Red* era contagiar a los computadores que tuvieran el servidor Microsoft Internet Information Server (IIS); se conocen cifras de que en una sola semana alcanzó a infectar a casi 400.000 servidores. En agosto de ese mismo año salió *Code Red II,* con un comportamiento similar al primero.
2004	***Sasser.*** A sus 17 años, Sven Jaschan no imaginó que iba a ser el creador de uno de los virus informáticos más terribles y dañinos de la historia. Entre abril y mayo de 2004, esta plaga informática alertó a más de una compañía por su alto grado de peligrosidad debido a que, para contagiar el equipo, no era necesario que el usuario abriera un archivo. Entre la actividad maliciosa de ***Sasser*** se recuerda que sacó provecho de los baches en la seguridad de los sistemas operativos Windows 2000 y Windows XP y se fue expandiendo a velocidades sorprendentes, hasta alcanzar unos 250 mil equipos infectados. El gusano puso en aprietos a corporaciones y empresas de gran importancia en países como Inglaterra, Taiwán, Australia y Finlandia.

Diseño y realización de la seguridad

Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

Sistemas, redes y políticas deben ser diseñadas, implementadas y debidamente coordinadas para optimizar la seguridad.

Un enfoque es más viejo, pero no exclusiva de este esfuerzo se encuentra en el diseño y la adopción de mecanismos y soluciones que salvaguarden o limiten las posibles amenazas o vulnerabilidades de daños idénticos.

Principios se bases en la seguridad:

- Gestión de la seguridad: la gestión de la seguridad debe basarse en la valoración de los riesgos y ser dinámico y debe incluir todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones.
- Reevaluación: constantemente se descubren nuevas amenazas y vulnerabilidades. Los participantes deben, en este sentido, revisar y evaluar, y modificar todos los aspectos de la seguridad de manera continua, con el fin de hacer frente a los riesgos siempre en evolución.
- Metodología:

  a. Evaluación: análisis de los requisitos ambientales y de seguridad del sistema. Durante esta fase, se crea y documenta las políticas y planes para implementar estas políticas de seguridad.

  b. Protección: aplicación del plan de seguridad (por ejemplo, la configuración de seguridad, protección de recursos, mantenimiento).

  c. Detección: identificación de los ataques y violaciones de las políticas de seguridad con el uso de técnicas como la monitorización, análisis y detección de intrusos registros.

  d. Respuesta: gestión de incidentes de acuerdo al plan de seguridad.

Ejemplos de modelo de seguridad

Seguridad organizacional:

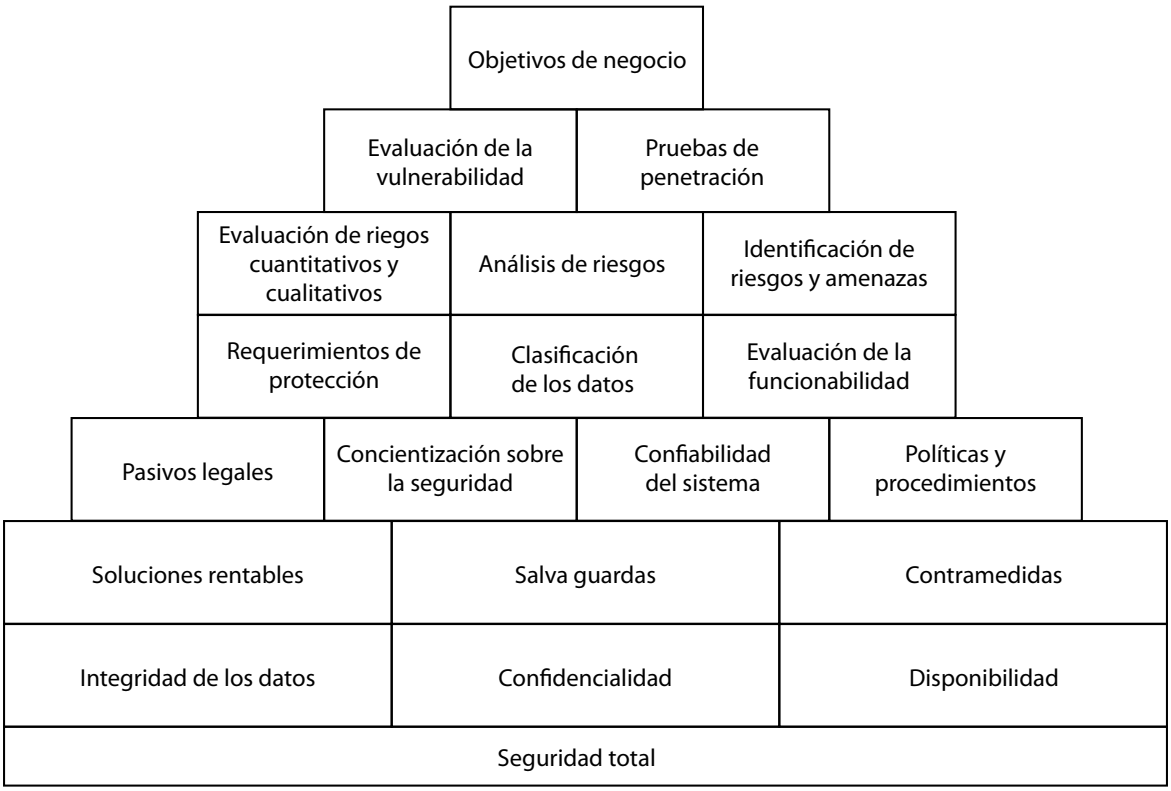


Figura 1
Fuente: Propia.

Seguridad profunda

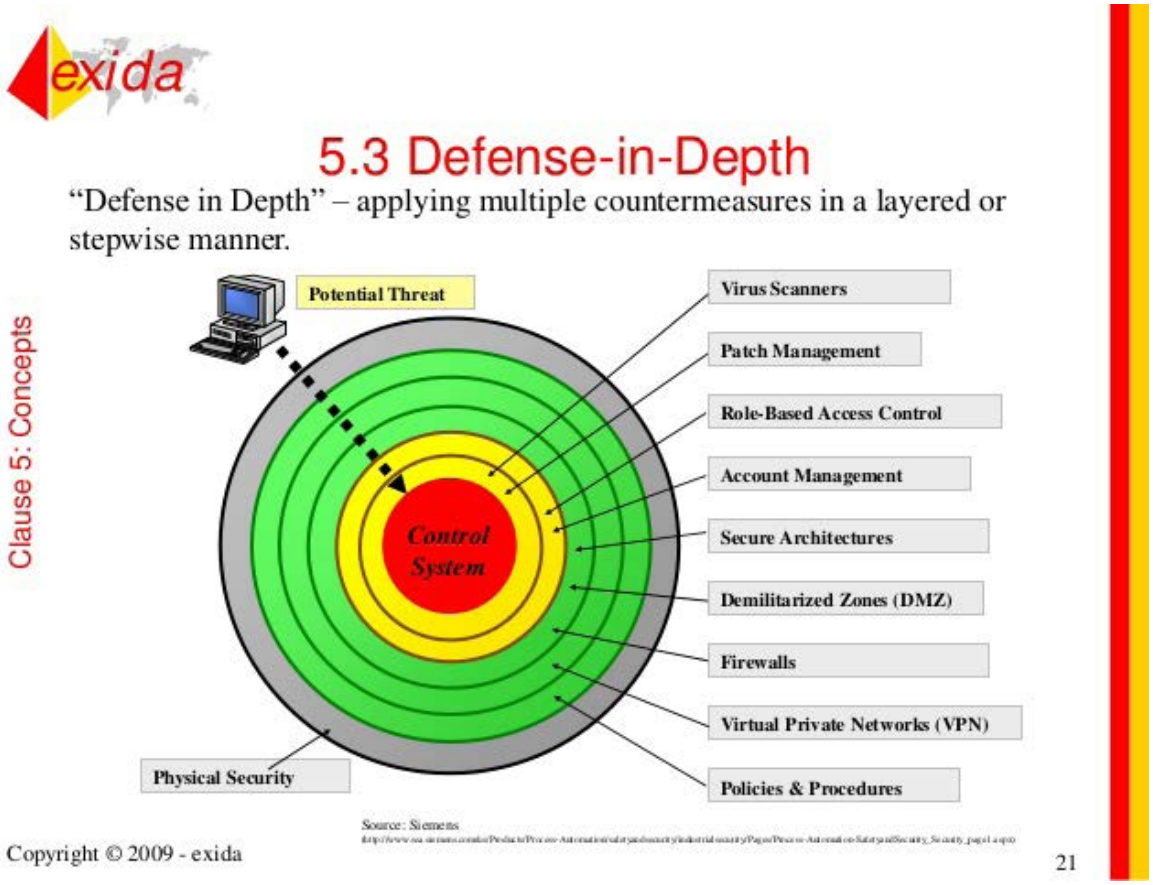


Imagen 1

Fuente: http://image.slidesharecdn.com/controlsystemsecurityunderstandingthebasics-101109145132-phpapp01/95/control-system-security-understanding-the-basics-21-638.jpg?cb=1422644379

Errores de seguridad de TI comunes:

a. No tratar la seguridad como una prioridad: a pesar de la incursión de titulares sobre interrupciones y fallos de seguridad, muchas empresas siguen a aislar las cuestiones de seguridad a un segundo plano. "La seguridad es un elemento caro y no parece ser considerado una parte esencial de la empresa." "Consume una gran cantidad de capital que los ejecutivos prefieren invertir en cualquier otra área de la organización".

b. Estrategia de respuesta inadecuada: cuando una amenaza de seguridad aparece y nadie que tome los controles sobre ella, los retrasos y la mala decisión puede arruinar cualquier respuesta eficaz. "Hoy en día, muchas organizaciones son capaces de identificar los incidentes de seguridad dentro de su entorno de TI, pero carecen de la capacidad para responder con eficacia, sobre todo en el caso de las amenazas que puedan surgir".

c. Sistemas de seguridad integrados de forma deficiente: porque las amenazas de seguridad cambian constantemente, muchas organizaciones se enfrentan a una maraña de aplicaciones, configuraciones de hardware, administradores internos, código de programación, y consultores, los cuales, en su conjunto, puede crear incompatibilidades e ineficiencias.

   "Llega un momento en el que todo se derrumba y la empresa se ve inmersa en el desastre".

d. Falta de aprendizaje para los empleados: un número creciente de amenazas, que también están diseñados para explotar el enlace de seguridad débil de la cadena "Empleados". En particular, las técnicas de ingeniería social como el phishing (suplantación de identidad) y spear phishing (este último se dirige a una persona específica o un grupo pequeño) están causando estragos. "Muchas empresas consideran que el aprendizaje es algo excesivo o creen que sus empleados son improductivos si no están en su trabajo en el más mínimo período de tiempo."

e. Reglas y procedimientos no efectivos: frente a una amenaza, es fácil optar por bloquear la mensajería instantánea o la prohibición flash USB (bus serie universal), que puede transportar datos fuera de los límites físicos de una oficina.

   También puede crear la ilusión de una seguridad estricta al exigir a los empleados a cambiar sus contraseñas cada mes. Por desgracia, estas reglas molestas pueden reducir la productividad o simplemente alentar a los empleados a buscar otros métodos. "Las políticas insuficientes pueden convertirse en un obstáculo para el trabajo y aumentar los riesgos de seguridad".

f. Amenazas internas: a pesar de todo lo que pone de relieve la existencia de hackers e intrusos, muchas violaciones de seguridad se producen dentro de la empresa. Empleados sin escrúpulos o descontentos es una amenaza constante, por lo que un descuido puede ser catastrófico, especialmente entre los empleados con computadoras portátiles y asistentes digitales. Los gerentes y ejecutivos de alto nivel con privilegios de acceso prácticamente sin control, son también de alto riesgo.

   Además, el personal de administración, trabajadores temporales, e incluso los trabajadores de limpieza a menudo pueden vagar libremente alrededor de la instalación.

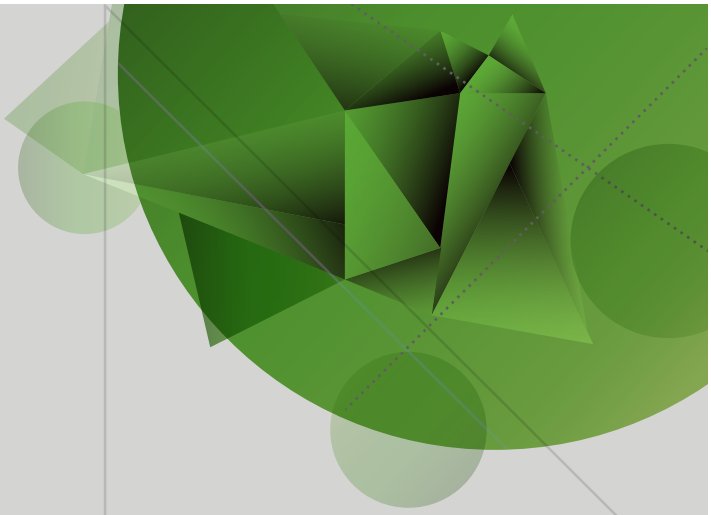
¿Cuándo podemos decir que un sistema es seguro?

"Un sistema de cómputo es seguro si se puede confiar en que él y su software se comportaran como se espera que lo hagan, y que la información almacenada en él permanecerá inalterada y accesible durante el tiempo que el propietario desea".

2

Unidad 2

Principios y ciclo de la seguridad informática



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Todos los elementos de un sistema de información pueden ser afectados debido a las brechas de seguridad, teniendo en cuenta que la información debe ser considerada como el factor más vulnerable. Hardware y otros elementos físicos pueden ser restaurados o reemplazados, el software, en este caso puede ser reinstalado, pero la información que se aloja en estos sistemas no siempre es recuperable, lo que puede causar diversos grados de daño en la economía y la imagen de la organización, así como en algunos casos causar daños a las personas.

Otro aspecto a tener en cuenta que la mayoría de las violaciones de seguridad son causados por el factor humano.

Sobre este módulo veremos los principios de la seguridad informática con el fin de conformar un sistema seguro en una organización, teniendo en cuenta que la información es el mayor activo principal y cómo podemos tener un sistemas seguro para poder resguardarla ante cualquier tipo de amenaza o vulnerabilidad que pueda presentar el entorno donde se aloja.

Otro aspecto importante es contar con una metodología que complementaria los principios para tener un control de ellos mismos.

U2 Metodología

Leer y entender el contenido plasmado sobre la cartilla, apoyarse en el documento de lecturas complementarias y auto investigación sobre los temas que serán vistos en esta semana. Tener como apoyo los recursos complementarios para la profundización del tema visto.

Es importante conocer los principios básicos de la seguridad, teniendo en cuenta que son unos de los principales factores al momento de ser aplicados en una compañía, muchos de los temas se desconocen pero es importante abarcar cada punto para contextualizar y entender la finalidad que busca la seguridad informática.

U2

Desarrollo temático

Principios y ciclo de la seguridad informática

Diseño y realización de la seguridad

"Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información".

Sistemas, redes y políticas deben ser diseñado, implementado y coordinado adecuadamente para optimizar la seguridad, pero no es el enfoque exclusivo de este esfuerzo se encuentra en el diseño y la adopción de mecanismos y soluciones que salvaguarden o limitar los daños potenciales amenazas o vulnerabilidades identificadas.

La gestión de la seguridad debe basarse en la evaluación de riesgos y ser dinámico y debe incluir todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones.

Prácticas de la gestión de la seguridad

- Definir metas y niveles de seguridad.
- Tipos de controles (medidas).
- Análisis y administración del riesgo.
- Elementos para gestionar la seguridad.
- Roles y responsabilidades en seguridad.
- Clasificar la información.
- Sensibilización y formación.

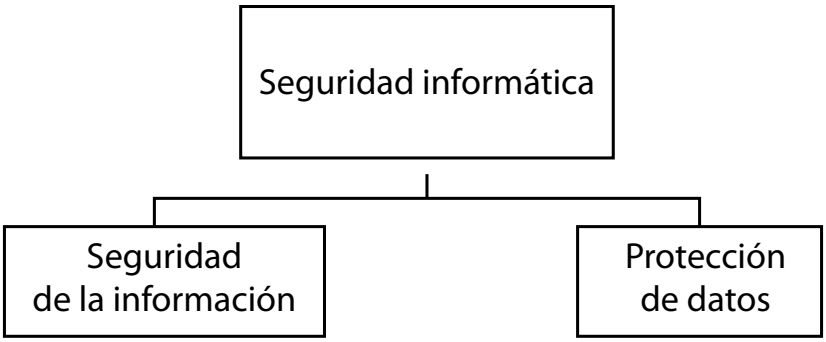


Figura 1
Fuente: Propia.

¿Que no es la seguridad informática?

1. La seguridad no es la llave de la organización.
2. La seguridad no es un aspecto técnico más a considerar.
3. La seguridad no se resuelve con un producto.
4. No hay sistemas 100 % seguros.

" El único sistema totalmente seguro es aquel que está apagado, desconectado de la red, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy bien armados y muy bien pagados. Aun así, no apostaría mi vida por él." -- Eugene Spafford.

Tipos de seguridad

a. Activa: se comprende el paquete o defensas, que tiene por objeto prevenir o reducir los riesgos que podrían amenazar el sistema.

   Ejemplo: impedir el acceso a la información a los usuarios no autorizados a través de niveles de autenticación con un nombre de usuario y contraseña; Acceso a evitar los virus mediante la instalación de software antivirus, usando encriptación para evitar que los mensajes de correo o accesorios no autorizados de lectura.

b. Pasiva: son medidas que se aplican una vez que el incidente ocurrió como para minimizar el impacto y facilitar sistemas de recuperación.

   Ejemplo: las copias de seguridad escénicas y datos calculados estipulado tiempo.

Principios de la seguridad informática

La mayoría de los daños que son producidos es por la falta de seguridad que se implanta a un sistema, provocando pérdidas económicas o credibilidad de su negocio u organización.

El origen puede ser factor de:

- Fortuito: errores cometidos accidentalmente por los usuarios, accidentes, cortos del fluido eléctrico, averías sobre el sistema y desastres naturales.
- Fraudulento: son ocasionados por Software maliciosos, intrusos o mala voluntad de algún tipo de medio o persona que puede tener acceso al sistema, robo o accidentes provocados.

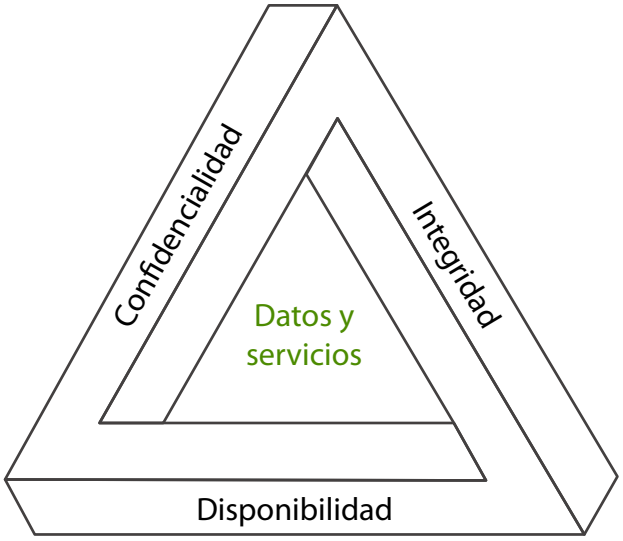


Figura 2
Fuente: Propia.

Para considerar un sistema seguro debe cumplir con las siguientes propiedades que son el pilar de la seguridad:

1. Integridad.
2. Confidencialidad.
3. Disponibilidad.

Cada una de estas propiedades conlleva a la formación de sistemas de seguridad acorde a la necesidad de la organización y de mecanismos seguros para la protección de la información.

Integridad

Este principio garantiza la autenticidad y exactitud de la información en cualquier momento que se solicitó o se envía de un entorno tecnológico en que los datos no han sido alterados o destruidos de forma no autorizada.

El objetivo de la integridad, entonces, evitar la modificación no autorizada de la información.

La integridad hace referencia a:

- La integridad de los datos (el volumen de la información).
- La integridad del origen (la fuente de los datos, llamada autenticación).

Es importante hacer insistencia en la integridad de la fuente, ya que puede afectar su precisión, credibilidad y confianza que la gente pone en la información.

A menudo sucede que cuando se habla de la integridad de la información que no se encuentra en estos dos aspectos.

Por ejemplo, cuando un periódico difunde información cuya fuente no es correcta, podemos decir que la integridad de los datos se mantiene a medida que se difunde a través de impresos, sin embargo, siendo la fuente de esta información errónea no es mantener la integridad de origen, debido a que la fuente no es correcta.

Para evitar cualquier riesgo deba haber una serie de herramientas o mecanismos para prevenir y detectar cualquier alteración como algún tipo de fallo que se produce la integridad y están con la capacidad de recuperar o resolver errores de pruebas.

Confidencialidad

OCDE (Organización para la Cooperación Económica y el Desarrollo), en una de sus Directrices para la Seguridad de los Sistemas de Información, define como "principio de confidencialidad de los datos y la información que sólo están disponibles para el conocimiento de las personas, entidades o mecanismos autorizados, en los necesarios tiempos y con autoridad".

El propósito de la confidencialidad, entonces, evitar la divulgación no autorizada de información.

En general, cualquier empresa pública o privada y cualquier ámbito requiere que cierta información no se accede por diferentes razones. Uno de los ejemplos más típicos es el ejército de un país. Por otra parte, se sabe que los logros más importantes de la seguridad siempre están vinculados a cuestiones estratégicas militares.

Por otra parte, algunas empresas suelen desarrollar diseños que debe proteger a los competidores. La sostenibilidad de la empresa y su posición en el mercado puede depender directamente de la aplicación de estos diseños y por esa razón, para protegerlos a través de mecanismos de control de acceso para garantizar la confidencialidad de dicha información.

Un ejemplo típico de un mecanismo que garantice la confidencialidad es la criptografía, que pretende cifrar o encriptar los datos para que sean incomprensibles para aquellos usuarios que no tienen permisos suficientes.

Pero incluso en estas circunstancias, no hay datos sensibles de ser protegidas y la clave

de cifrado. Esta clave es necesario que el usuario adecuado puede descifrar la información recibida y basado en el tipo de mecanismo de cifrado utilizado, la clave puede/debe viajar por la red y puede ser capturado por herramientas diseñadas para eso. Si se produce esta situación, la confidencialidad de la operación (ya sea bancaria, administrativa o de otro tipo) se ha comprometido...

Disponibilidad

Comenzando en que la información debe estar disponible en cualquier momento para los usuarios autorizados cuando sea necesario.

Una de las referencias a la definición dada por el programa MAGERIT Disponibilidad "define como el grado en que los datos de lugar, tiempo y modo en que se requiere por parte del usuario autorizado. Esta situación se produce cuando se puede acceder a un sistema de información en un período de tiempo considerado aceptable. La disponibilidad está vinculada a la fiabilidad técnica de los componentes del sistema de información".

La disponibilidad objetivo es entonces controlado para evitar interrupciones no autorizadas/de los recursos informáticos.

En términos de seguridad "que está disponible cuando un diseño e implementación del sistema permite que niegan deliberadamente el acceso a determinados datos o servicios." Es decir, un sistema está disponible si usted no puede estar disponible. Y un sistema de "no disponible" es tan malo como ningún sistema. No funciona.

Para resumir los fundamentos de la seguridad que hemos discutido, podemos decir que la seguridad es mantener el equilibrio adecuado entre estos tres factores. No tiene sentido que cada vez confidencialidad para un archivo si es a costa de ni siquiera el usuario administrador puede acceder a ella, ya que está negando la disponibilidad.

Dependiendo del ambiente de trabajo y sus necesidades puede dar prioridad a un aspecto de la seguridad o de otra. En entornos militares prioridad generalmente se proporcionó información confidencial contra la disponibilidad. Aunque cualquier persona puede acceder a ella o incluso eliminarlo puede no saber su contenido y reemplazar esta información será tan fácil como recuperar una copia de seguridad (si las cosas van bien).

En entornos de banca es siempre la integridad prioridad de datos contra la confidencialidad o disponibilidad. Se considera menos perjudicial para un usuario puede leer el saldo a otro usuario puede modificar.

Seguridad de la Información: modelo PDCA

Los sistemas informáticos permiten el análisis de todo el volumen de información al reducir el espacio ocupado, pero sobre todo, lo que facilita el análisis y procesamiento. Se gana en el "espacio", el acceso, la velocidad en el procesamiento de esta información y mejoras en la presentación de esta información.

Pero aparecen otros problemas vinculados a estas instalaciones. Es más fácil para transmitir información también son más propensos a desaparecer 'por el camino'. Es más fácil acceder a ella también es más fácil de modificar su contenido, etc.

Desde la llegada de los grandes sistemas a nuestros días, en los que la red es habitual en cada espacio, los problemas de seguridad de la información también han ido cambiando, evolucionando, pero las solu-

ciones están ahí y han tenido que adaptarse a los nuevos requisitos técnicos. El aumento de sofisticación en el ataque y esto aumenta la complejidad de la solución, pero la esencia es la misma.

También hay diferentes definiciones de Seguridad. De ellos nos quedamos con la definición proporcionada por el estándar para la seguridad de la ISO / IEC 27001, que fue aprobado y publicado en octubre de 2005 por la Organización Internacional de Normalización (ISO) y la Comisión de la Comisión Electrotécnica Internacional (IEC).

"La seguridad informática es la implementación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información también puede incluir otras propiedades tales como la autenticidad, la rendición de cuentas, no repudio y fiabilidad."

Como vemos la seguridad de la información término es más amplio ya que abarca otros aspectos de seguridad más allá de lo puramente tecnológico.

En la organización interna de la cuestión de la seguridad de la información es un capítulo muy importante en el que sé que tengo que dedicar tiempo y recursos. La organización debería considerar en un Management Information System Security (SGSI). El objetivo de SGSI es para proteger la información y hacer lo primero que debe hacer es identificar a cada uno de los 'activos de información' para ser protegido y en qué grado.

A continuación, el plan de PDCA ('Planear- Hacer - Verificar - actuar') debe aplicarse, es decir, el Plan, Do, Check, Act y repetir el ciclo.

La seguridad se entiende como un proceso que nunca termina porque nunca elimina el riesgo sólo puede ser mitigado o transferencia, pero se puede controlar. Los riesgos muestra que los problemas de seguridad no sólo son de naturaleza tecnológica, y por eso nunca se eliminan en su totalidad.

SGSI siempre sirve cuatro niveles repetitivos que comienzan y terminan en la Ley de Planificación, mejorando así la seguridad.

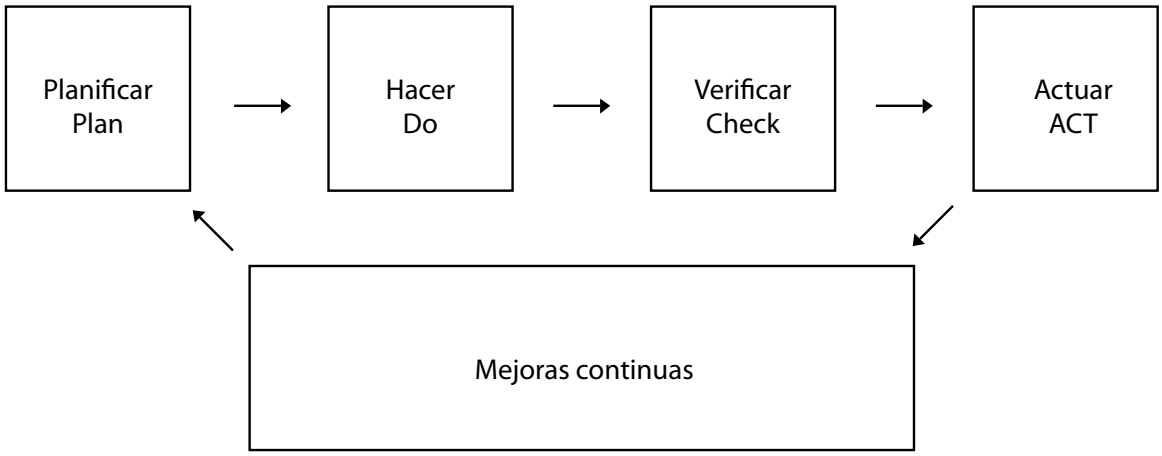


Figura 3
Fuente: Propia.

a. Planificar (Plan): consiste en establecer el contexto en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

b. Hacer (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

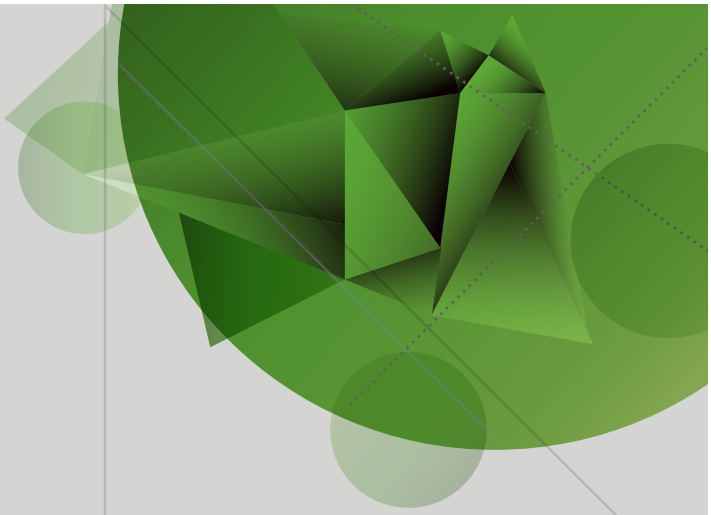
c. Verificar (Check): consiste en monitorear las actividades y hacer auditorías internas.

d. Actuar (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

2

Unidad 2

Ciclo de la seguridad informática



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

El ciclo de la seguridad informática nos permite contar con unas fases o pasos para conformar un sistema basado en la seguridad de la información y con la capacidad de poder llegar a determinar los riesgo o vulnerabilidades que se pueden presentar siendo cual sea el entorno donde nos encontremos, cada amenaza encontrada debe tener un tratamiento para ser mitigado y colocando los factores necesarios para que no se vuelva a presentar.

La protección de los sistemas de información y por lo general no elimina por completo la posibilidad de que estos bienes están dañados. Por lo tanto, los gerentes deben aplicar esas medidas de seguridad con los riesgos a niveles aceptables, contando el coste de las medidas a implementar, con el valor de los bienes a proteger y la cuantificación de las pérdidas que podrían derivarse de la aparición de cierto incidente de seguridad.

En todo caso, la seguridad informática requiere capacidad para gestionar los riesgos adecuadamente. Invertir en medidas de seguridad, las organizaciones pueden reducir la frecuencia y severidad de las pérdidas relacionadas con las violaciones de seguridad en sus sistemas. Por ejemplo, una empresa puede estimar que las pérdidas se sufren debido a la manipulación fraudulenta de su inventario de los sistemas informáticos, contables o de facturación. En este caso, algunas medidas para mejorar los controles de acceso se pueden reducir las pérdidas de manera significativa.

Imagen 1

Fuente: http://blog.infoempleo.com/a/estan-protegidas-nuestras-empresas/

U2

Metodología

Leer y entender el contenido plasmado sobre la cartilla, apoyarse en el documento de lecturas complementarias y auto investigación sobre los temas que serán vistos en esta semana. Tener como apoyo los recursos complementarios para la profundización del tema visto.

Conociendo cuales son los principios de la seguridad, nos apoyaremos en los ciclos de la seguridad, con la finalidad de poder conocer que abarca cada contexto y como se ejecutaría estos dos sistemas al momento de implementar la seguridad. Los conceptos que se verán a continuación son fundamentales e importantes para la seguridad en una organización o empresa.

Ciclo de la seguridad informática

Ciclo de vida de la seguridad informática

Se trata de un ciclo en el que la seguridad se mantiene en una organización, la forma en que un conjunto de pasos o fases, para la de mitigación del riesgo, amenaza o pérdida de información como activos principal de un negocio:

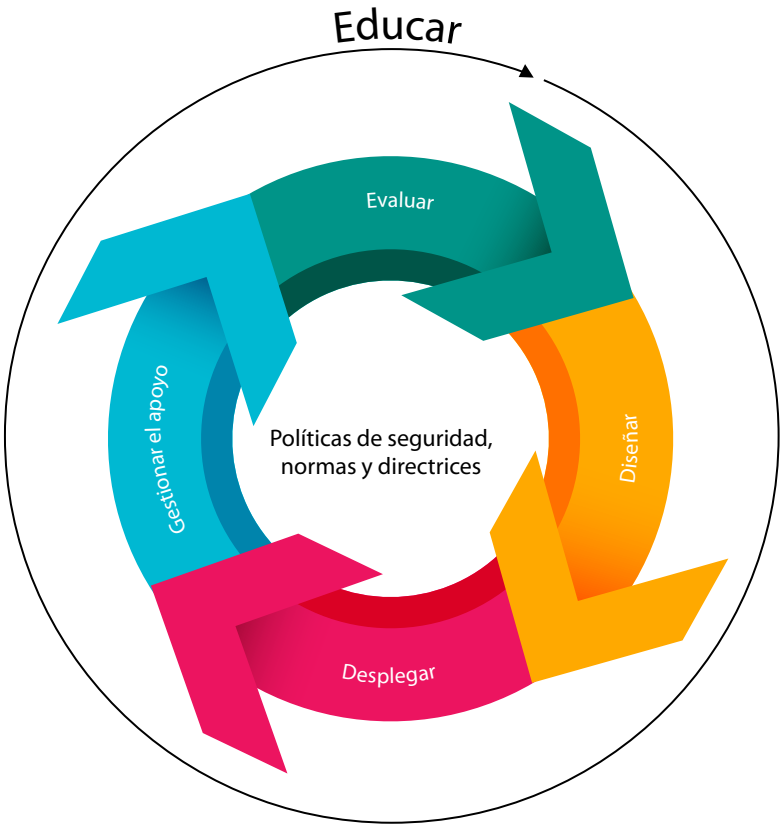


Figura 1
Fuente: Propia.

Evaluación (*Assess*)

Debe hacerse la primera referencia para evaluar, encontrar una metodología o una estrategia que le permite saber en qué estado está su seguridad, donde se puede determinar el estado de las vulnerabilidades según la evidencia encontrada, tales evaluaciones deben ser específicas como el núcleo de empresa o el entorno en el que se basa la organización. Sobre la base el objetivo es poder analizar, verificar que significa que cada vulnerabilidad encontrada, ver las prioridades para resolver, ver el estado actual es suficiente para la protección de la información protegida, con el fin de tener una visión general. También vemos que cruzará para todos los pasos, para comunicarse, para crear conciencia sobre la situación de los datos, y comunicarse en un lenguaje que sea comprensible para todos, en términos y lenguaje de los negocios.

Debilidades:

- Determinar el estado de la seguridad en dos áreas principales: técnica y no técnica.
- No técnica: evaluación de políticas.
- Técnica: evaluación de seguridad física, diseño de seguridad en redes, matriz de habilidades.

Otras áreas que se deben revisar:

- Seguridad exterior.
- Seguridad de la basura.
- Seguridad en el edificio.
- Passwords.
- Ingeniería social.
- Clasificación de los datos.
- Etc.

El análisis de riesgos nos permitirá:

Realizar acciones:

- Proactivas
- Reactivas

Administrar el riesgo:

- Identificar
- Analizar
- Evaluar
- Tratamiento a seguir

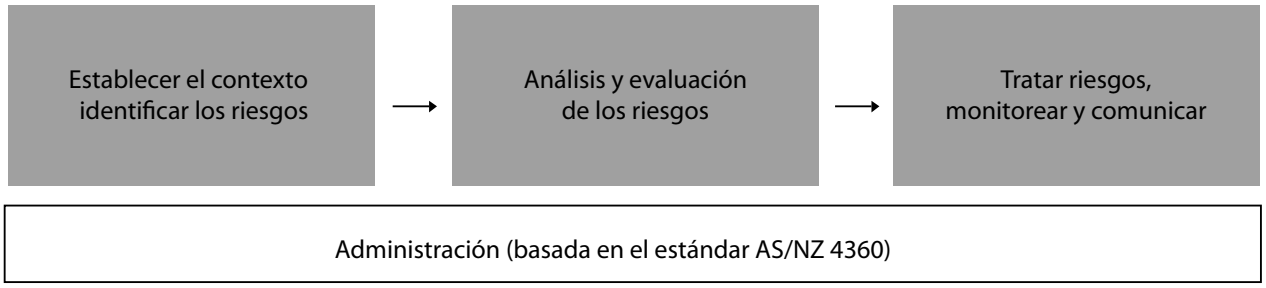


Figura 1
Fuente: Propia.

Diseño (*Dessing*)

Con la anterior evaluación, se debe diseñar una solución que corrige, los ataques y mitigar los puntos que se encuentran por encima, siendo coherentes con los criterios de prioridad y teniendo los recursos para implementar la solución, establecer parámetros que indican el éxito o el fracaso de la aplicación y establecer los pasos después de la implementación, tenga en cuenta cada criterio de evaluación, es decir, la forma en que se administra, quien controla a quien se le da, etc.

Todo este plan hecho debe realizarse en un horario, distribuido en tareas y los plazos de acuerdo a lo establecido (cronograma), la difusión de las acciones o los parámetros que fueron apeladas, la comunicación debe ser en términos de negocio y las métricas de éxito claro de no causar problemas con la aplicación expectativas.

Es importante tener en cuenta los siguientes métodos en el diseño de la aplicación:

¿Necesitamos políticas de seguridad?

Con el fin de determinar:

- ¿Empleados acezando internet?
- ¿Problemas con el uso de la red o el email?
- ¿Empleados utilizando información confidencial o privada?
- ¿Acceso remoto a la organización?
- ¿Dependencia de los recursos informáticos?

Políticas define que prácticas son o no son aceptadas.

¿Cómo concientizar?

- En persona, por escrito o través de la intranet.
- Reuniones por departamento.
- Publicar artículos, boletines, noticias.
- Crear un espacio virtual para sugerencias y comentarios.
- Enviar emails con mensajes de concientización.
- Pegar letreros en lugares estratégicos.
- Dar premios a empleados.
- Exámenes on-line.
- Crear eventos de seguridad informática.

Implementar (*Deploy*)

Fase donde instruye según la función en la implementación, que se ejecuta cada una de las actividades propuestas en el calendario inicial para la implementación de cada uno de los métodos de seguridad para que los sistemas sean más seguros.

Los cambios deben ser documentados, cada parámetro hecho, los problemas aún presentes, documentar la solución de éstos, la aplicación de medición basado en indicadores ya acordados, probar la implementación, hacer las pruebas de carga, establecer el nivel de éxito, en comparación con las métricas, evaluar el proceso de implementación en sí también.

Los tipos de tecnologías que se implementan a un sistema de seguro:

Fuente: ISSA/BSA, 2003

	Implantado	Planeado
Antivirus	99%	0%
Firewalls	97%	1%
Filtros de email	74%	10%
IDS	62%	12%
Bloqueo de adjuntos	62%	3%
Filtro de Web sites	59%	5%
Análisis de Vulnerabilidades	43%	18%
Email encriptado	31%	15%

Cuadro 1
Fuente: ISSA/BSA 2003

Administración y soporte (*Mannage y support*)

Fase donde lo custodia la implementación, se trata de una mejora continua del proceso, por lo que se tiene que medir constantemente, hasta el mantenimiento y el apoyo, mediciones contra las métricas de apoyo y contra las métricas que pueden cotejar, y en constante comunicación, indicar el estado en que se encuentra y documentar nuevas debilidades encontradas.

Pasos a tener en cuenta:

- Observar las actividades normales y reaccionar ante incidentes.
- Monitoreo y alertas.
- Las respuestas se basan en el documento de Políticas de Seguridad definido.
- Forma en que se trata el incidente.
- Encontrar el problema y corregirlo.
- Prácticas forenses.
- Definir la responsabilidad y el causante del problema.

Como se realiza el manejo de incidentes, a nivel del sistema:

- Organización.
- Identificación.
- Encapsulamiento
- Erradicación.
- Recuperación.
- Lecciones aprendidas.

Mejora continua (*Continuous improvement*)

Después de terminar el ciclo completo, la fase de mejora continua determina los errores y las soluciones adoptadas para resolver los problemas o conflictos que se presentan en el sistema siempre debe existir.

Se debe continuar con todo el ciclo de vida como la ampliación de toda la organización. Se confirman las habilidades y la experiencia que se logran dentro del proceso.

Análisis de riesgo

A la hora de implementar un sistema de seguridad de la información de una organización debe tener en cuenta todos los elementos o activos que lo comprenden, analizar el nivel de vulnerabilidad de cada uno, con el fin de identificar y evaluar las posibles amenazas del impacto causaría un ataque contra el sistema.

"La cadena siempre se rompe por el eslabón más débil"

El personal y el equipo de seguridad serán responsables de analizar cuidadosamente cada uno de los elementos que lo conforman, a veces el abandono mínimo de un elemento débil en cuestión, ha producido fallos de seguridad importantes. Ellos se interrelacionan y a cualquier descuido puede causar errores inesperados en los efectos en cadena sobre la organización.

Para comenzar el análisis de un sistema de información que es proporcionar medidas de seguridad, debe tener en cuenta los siguientes elementos:

Activos: son los recursos que pertenecen al propio sistema de información o que están relacionados entre sí. La presencia de los activos en una organización u empresa facilitan el funcionamiento y la consecución de los objetivos. Al hacer el estudio de los activos existentes hay que tener en cuenta la relación que guardan entre ellos y la criticidad que ejercen: como afectarían en uno de ellos un daño ocurrido a otro.

Se pueden clasificar en los siguientes tipos de activos:

Datos: constituyen el núcleo de toda la organización, al punto que se tiende a considerar como el activo más valioso. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo. El funcionamiento de una empresa depende de sus datos, que pueden de todo tipo: económicos, fiscales, de recursos humanos clientes, proveedores, entre otros.

Software: constituido por el sistema operativo y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben, gestionan o transforman los datos para fines establecidos.

Hardware: se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacena los datos del sistema de información.

Redes: desde las redes locales de las misma organización hasta las metropolitanas o internet. Representa la vía de comunicación y trasmisión de los datos a distancia.

Soportes: los lugares donde la información quedara registrada y almacenada durante largos periodos o de forma permanente (DVD, CD, tarjetas de memoria, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).

Instalaciones: son los lugares donde se albergan los sistemas de información y de comunicaciones. Normalmente se trata de oficinas, despachos, locales, edificios o Datacenters.

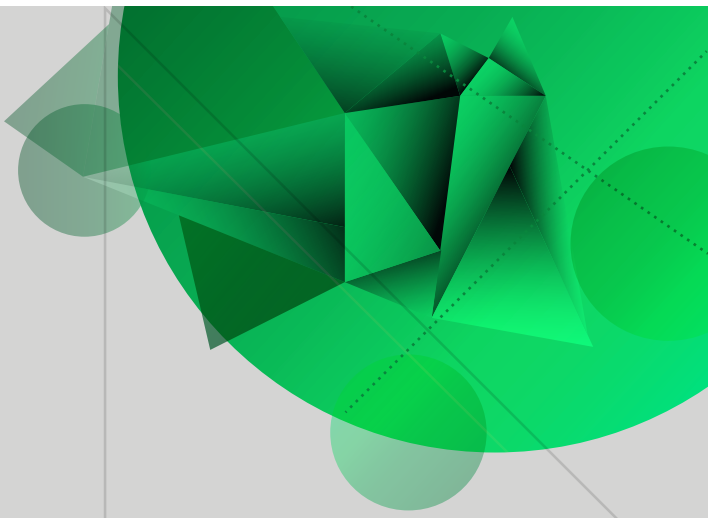
Personal: el conjunto de personas que interactúan con la información: administradores, programadores, usuarios internos y externos, y resto del personal de la empresa. Los estudian indican que los mayores riesgos de seguridad son intervención del factor humano que por fallos de tecnología.

Servicios: son los que ofrecen a clientes o usuarios, productos, servicios, sitios web, foros, correo electrónico y otros servicios de comunicaciones, información, seguridad, etc.

3

Unidad 3

Amenazas y sus tipos



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Los sistemas informáticos son vulnerables a muchas amenazas que pueden causar daño resultando en pérdidas significativas. El daño puede variar desde simples errores en el uso de aplicaciones de gestión que comprometen la integridad de los datos, hasta que todos los sistemas de inutilizables después de un desastre. Las pérdidas pueden ocurrir a partir de la actividad de la organización por parte de entidades externas (intrusos) para el acceso fraudulento por el acceso no autorizado, por el mal uso de los sistemas por los propios empleados, o la ocurrencia de contingencias generalmente destructivos.

Imagen 1
Fuente: http://2.bp.blogspot.com/-B02QJ29JK_o/UqocKKRskqI/AAAAAAAADfg/NoqEcDlJ3zA/s1600/seguridad-web.jpg

Los efectos de las diversas amenazas se pueden variar. Algunos pueden comprometer la integridad de la información o los sistemas, otros pueden degradar la disponibilidad de servicios y otros pueden estar relacionados con la confidencialidad de la información. En cualquier caso, la gestión adecuada de los riesgos debe implicar una profunda comprensión de las vulnerabilidades del sistema y las amenazas que pueden explotar. Las características de las organizaciones deberían influenciar en las medidas de seguridad que son más apropiadas y más eficientes en términos de costos, para contrarrestar las amenazas o incluso tolerar en ningún caso conocer sus implicaciones.

A continuación conoceremos la definición de una amenaza y los factores o tipos de amenazas que nos podemos encontrar en el ambiente laboral o ámbito personal, esto con la finalidad de poder determinar y que acción se pueda ejecutar para poder mitigar la amenaza.

U3 Metodología

Leer y entender el contenido plasmado sobre la cartilla, apoyarse en el documento de lecturas complementarias y auto investigación sobre los temas que serán vistos en esta semana. Tener como apoyo los recursos complementarios para la profundización del tema visto.

Entender que es una amenaza y por qué son consideras como fuentes potenciales al momento de incluir un riesgo en una organización que pueden desencadenarse en cualquier ámbito laboral y las consecuencias que esto llevarían. Conoceremos los diferentes tipos y factores de amenazas que pueden existir en un entorno, con el fin de determinar sus tipos de impactos que pueden ocasionar y el ámbito donde se puede generar.

Amenazas y sus tipos

Amenazas

En los sistemas de información, *amenaza* significa la presencia de uno o más factores (personas, máquinas o eventos) que tienen capacidades, lo que le causa daños al sistema aprovechando su vulnerabilidad. Hay diferentes tipos de amenazas de las cuales el sistema debe ser protegido físicamente como lo son los apagones, fallos de hardware o riesgos ambientales a errores intencionales o no intencionales de los usuarios, la entrada de malware (virus, troyanos, gusanos) o el robo, destrucción o modificación de información.

Criminalidad (común y política)

· Allanamiento, sabotaje, robo/hurto, fraude, espionaje, virus, entre otras.

Sucesos de origen físico

· Incendio, inundación, sismo, polvo, sobrecarga eléctrica, falta de corriente, entre otras.

Negligencia y decisiones institucionales

· Falta de reglas, falta de capacitación, no cifrar datos críticos, mal manejo de contraseñas, entre otras.

Cuadro 1
Fuente: Propia.

Dependiendo del tipo de alteración, daño o intervención que podrían producir sobre la información, las amenazas se clasifican en cuatro grupos:

a. **De interrupción:** el objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, la destrucción de componentes físicos como el disco duro, bloqueando el acceso a los datos, o el corte o la saturación de los canales de comunicación.
b. **De interceptación:** gente, programas o equipos no autorizados pueden acceder a un recurso determinado en un sistema y capturar información de la organización confidencial, como datos, programas o la identidad de las personas.
c. **De modificación:** gente, software o hardware no autorizado no sólo acceder a los programas y datos de un sistema de información, sino también realizarían modificaciones. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada.
d. **De fabricación:** a añadir información falsa en toda la información del sistema.

Según su origen las amenazas se clasifican en:

a. **Accidentales:** accidentes meteorológicos, incendios, inundaciones, fallas de equipos, redes, sistemas operativos o software, errores humanos.
b. **Intencionadas:** estos siempre se deben a la acción humana, tales como la introducción de malware -malware- (aunque esto entra en el sistema por algún procedimiento automático, su origen es siempre humano), la piratería (a menudo se produce después de la introducción de malware en el equipo), robos. Las amenazas intencionales pueden originarse fuera de la organización o incluso el mismo personal de la compañía.

Tipos de amenazas

Factor humano

Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en que se inviertan más recursos para controlar y contrarrestar sus efectos. Cubre actos maliciosos, el incumplimiento de las medidas de seguridad que resulten de actos negligentes o falta de controles adecuados.

Tipos de amenazas humanas

Los actos humanos que pueden afectar la seguridad de un sistema son variados, entre los más comunes e importantes están:

- Curiosos: estas son personas que entran a los sistemas (a veces accidentalmente) que no están autorizadas, motivados por la curiosidad, impugnadas por lo personal, o por el deseo de aprender o averiguar.

  Por lo general, este tipo de intrusiones no tiene las habilidades necesarias para lograr el daño, pero no se debe pasar por alto sin tomar las precauciones necesarias. Aunque afirma que no tienen mala intención, su única intrusión representa una amenaza peligrosa, ya que puede causar daño no intencionado o exponer la estructura y el sistema de seguridad.

- Intrusos remunerados: este tipo de atacante es responsable de penetrar los sistemas a cambio de pago. Aunque es menos común, en realidad son muy peligrosos, ya que hay personas que poseen el conocimiento, la experiencia y las herramientas necesarias para penetrar el sistema, incuso en aquellos que tienen un alto nivel de seguridad.
- Personal enterado: son las personas que han autorizado el acceso o conocen la estructura del sistema de cierta organización. Por lo general, es el personal interno de una empresa o de un ex empleado, sus motivaciones van de venganza y retribución monetarias de organizaciones rivales.
- Terroristas: pretenden causar daño para diferentes propósitos, tales proselitistas o religiosas.
- Robo: se refiere a la extracción física de la información a través de las unidades secundarias de almacenamiento (disquetes, CD, cintas, etc.), el robo físico de los componentes de hardware del sistema e incluso el robo también se considera como el uso de equipos para diferentes actividades a las que se asignan en la organización.
- Sabotaje: es reducir la funcionalidad del sistema a través de acciones deliberadas para dañar el equipo, el logro de la interrupción de los servicios e incluso la destrucción completa del sistema. Puede ser perpetrada por personal interno o adversarios externos.
- Fraude: estas actividades no están dirigidas principalmente a la destrucción del sistema, si no utilizar los recursos que se manejan con fines de lucro sin relación con los objetivos de la organización.

  Aunque los responsables del fraude son identificados y arrestados, este tipo de actividad comúnmente tratada con la máxima discreción para no hacer publicidad, ya que da una mala imagen a la organización involucrada.
- Ingeniería social: en el campo de la ingeniería social de la seguridad informática es la práctica de obtener información confidencial mediante la manipulación de usuarios legítimos que tienen ellos para revelar información sensible o violar las políticas de seguridad típicas.

  Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, en lugar de explotar agujeros de seguridad en los sistemas informáticos. Se conviene en general que *"los usuarios son el eslabón más débil"* en materia de seguridad; este es el principio que rige la ingeniería social.

Imagen 2
Fuente: https://mariaalmejof304.files.wordpress.com/2011/04/new1.jpg

Hardware

La amenaza viene dada por fallas físicas presentadas en los elementos de hardware que componen el sistema informático. Estos defectos físicos pueden ser defectos o mal diseño de los equipos de fabricación, pero también puede ser el resultado de un mal uso y la negligencia en el mantenimiento.

Tipos de amenazas de hardware

- Mal diseño: cuando los componentes de hardware del sistema no son apropiados y no cumplen con los requisitos necesarios, es decir, la parte del módulo no fue adecuadamente diseñado para trabajar en el sistema.
- Errores de fabricación: cuando las piezas de hardware se adquieren con defectos de fabricación y luego fallan al intentar utilizar. Aunque la calidad de los componentes de hardware es la responsabilidad del fabricante, la organización que adquiere la más afectada por este tipo de amenazas.
- Suministro de energía: variaciones de tensión dañan los dispositivos, por lo que es necesario verificar que las instalaciones de suministro de energía operan dentro de los parámetros requeridos. También debe garantizarse que tales instalaciones proporcionan los voltajes necesarios para el funcionamiento de un dispositivo, ya que hay componentes de hardware que necesitan ser energizado a ciertos niveles de tensión especificados por los fabricantes, de lo contrario su vida se acortará.
- Desgaste: el uso constante de hardware se considera desgaste normal, con el tiempo esto reduce el óptimo funcionamiento del dispositivo para seguir con su actividad normal.
- Descuido y mal uso: todos los componentes deben ser utilizados dentro de los parámetros establecidos por los fabricantes, lo que incluye tiempos de uso, plazos y procedimientos para el mantenimiento y almacenamiento. El incumplimiento de estas prácticas provoca un mayor desgaste que se traduce en la vida prematura y la reducción de las averías de los recursos.

Imagen 3

Fuente: http://garciaanarosa.blogspot.com.co/2012/11/mantenimiento-preventivo-y-correctivo.html

Red de datos

Esta amenaza es cuando la red de comunicación no está disponible para su uso, este puede ser causado por un ataque deliberado por un intruso o un error físico o lógico del sistema. Las dos principales amenazas encontradas en una red de datos son, la falta de disponibilidad de la red, y la información de la lógica de extracción a través del mismo.

Tipos:

- Topología seleccionada: la topología es la disposición física en la que los nodos de una red de ordenadores o servidores se conectan, cada uno tiene una serie de ventajas y desventajas están conectados. Dependiendo del alcance y de recursos compartidos de red puede ser más conveniente para seleccionar una topología sobre otro, pero hay que señalar que las desventajas de cada arquitectura no sólo la comunicación limitada, incluso puede salir de la red fuera de servicio.

  Por ejemplo, en una red de anillo se produce por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa por la recogida y la entrega de paquetes de información, por lo que cualquier pérdida de datos debido a las colisiones se evitan, pero si se pierde la comunicación en algún nodo, se pierde entonces la comunicación alrededor del anillo.

- Sistema operativo: aunque el modelo OSI permite la comunicación entre ordenadores con diferentes sistemas operativos.

  Cada sistema operativo también tiene un nivel diferente de protección que los hace más susceptibles a los ataques que otros, y desde allí el atacante puede tomar acciones en contra de otros sistemas operativos con mayor seguridad. Este último punto se considera más de una vulnerabilidad de amenaza.

- Incumplimiento de las normas de instalación de la red: la instalación del cableado físico de redes de datos, debe seguir ciertas reglas y normas de diseño también conocido como cableado estructurado.

  Cableado estructurado corresponde a un conjunto de normas internacionales en el tendido de cables en el interior de un edificio con el propósito de implementar una red de área local, es el sistema colectivo de cables, tuberías, accesorios, etiquetas, espacios y otros dispositivos se debe instalar para establecer una infraestructura de red en un edificio, para ello hay que tener en cuenta las limitaciones de diseño impuestas por la red de tecnología de área local que se aplicará:

  - La segmentación del tráfico de red.
  - La longitud máxima de cada segmento de red.
  - La presencia de interferencias electromagnéticas.
  - La necesidad de redes locales virtuales.

Sin tener en cuenta estos puntos puede dar lugar a defectos de diseño que causan problemas de transmisión de datos, el funcionamiento o falta de disponibilidad de recursos de la red.

Imagen 4
Fuente: http://52.1.175.72/portal/sites/all/themes/argo/assets/img/home/misionvision.png

Software

Amenazas de software incluyen posibles defectos en el software del sistema operativo, el software desarrollado mal, mal diseñado o mal implementado, además existe uso de software malicioso que plantea una amenaza directa a un sistema.

Tipos:

- Software de desarrollo: es un tipo de software personalizado, puede ser creado para atacar a todo un sistema o aprovechar algunas de sus características para violar su seguridad.
- Software de aplicación: este software no fue creado específicamente para llevar a cabo los ataques, pero tiene propiedades que pueden ser utilizados maliciosamente para atacar un sistema.
- Código malicioso: es cualquier software que entra en un sistema informático sin invitación y tratar de romper las reglas, esto incluye troyanos, virus, gusanos, bombas lógicas y otras amenazas programadas.
- Virus: este tipo de código malicioso tiene como principal característica la capacidad de replicarse a sí mismo utilizando los recursos del sistema infectado, extendiendo su infección rápidamente.
- Troyanos: este tipo de código se presenta oculto en otros programas de aplicación aparentemente inofensivos, más tarde volvió discretamente perjudiciales cumplimiento de su propósito.
- Los troyanos son programas destructivos que representan al usuario como si fueran oportunidades beneficiosas
- Gusanos: es muy similar al virus, con la diferencia de que ellos aprovechan más recursos de los sistemas infectados, atacando a los diferentes programas y luego se duplica a ser redistribuido.
- Errores de programación y diseño: software creado para cumplir un papel dentro de la organización (por ejemplo un sistema de transacciones financieras, sistema de nómina, sistemas operativos, etc.) también pueden causar la pérdida o modificación de información. Esto ocurre cuando el software en cuestión no cumple con los estándares de seguridad requeridos, ya que nunca fue diseñado para apoyar a una organización. Los errores de programación y fracasos que pueden tener software de aplicación general también suponen una amenaza.

Imagen 5
Fuente: https://vulnerabilityteam.files.wordpress.com/2009/08/tiritas.png?w=614

Desastres naturales

Son eventos que tienen sus raíces en las fuerzas de la naturaleza. Estos desastres no sólo afectan a la información contenida en los sistemas, sino también representan una amenaza para la integridad de todo el sistema (infraestructura, instalación, componentes, equipos, etc.) pueden salir del sistema, incluso en un estado de interoperabilidad permanente. Estas amenazas también incluye la falta de preparación.

Tipos:

Entre los tipos de desastres naturales que amenazan a un sistema de información, tenemos inundaciones, terremotos, incendios, huracanes, tormentas, etc. Donde causan cortocircuitos, destrucción total o parcial de los equipos informáticos o alteraciones físicas de los pueblos, causando que ya no sea adecuada para albergar los equipos informáticos.

Por lo que es necesario tener en cuenta la ubicación geográfica en la que se llevara a cabo la instalación de los equipos de computación, los centro de servicio, centro de cómputo, etc., y hacer un estudio para determinar las amenazas que, probablemente, para evitar convertirse en víctimas de estos.

Imagen 6
Fuente: http://www.ultimasnoticiasbolivia.com/wp-content/uploads/2013/04/arde.jpg

Adicionalmente cuenta la importancia del cableado, no sólo en las redes de red de datos sino en toda la electricidad y el abastecimiento de agua que indirectamente podrían causar un desastre de este tipo y los daños de información de la organización.

Ejemplo

Este ejemplo se dio en el 2005 sobre el tipo de amenazas internas:

Un desarrollador, quien perdió su trabajo en el sector de TI, por reducción de personal en la empresa, expreso su descontento justo antes de las festividades de Navidad lanzando un ataque en la red de informática de su antigua empresa, tres semanas después de su despido, el usuario utilizo su usuario y contraseña de uno de sus antiguos compañeros, para obtener acceso a la red corporativa y así modificar varias páginas web de la empresa, reemplazando algunos textos por imágenes pornográficas, también a cada uno de los clientes un mensaje por correo electrónico advirtiendo que la página de la empresa había sido Hackeada. Cada correo electrónico contenía los nombres de usuario y contraseña para el acceso por la página web. Se inició una investigación por lo sucedido pero no se logró identificar el empleado que realizo esta serie de actividades. Un mes y Medio después, volvió a ingresar a la red corporativa de manera remota, donde ejecuto unos scripts para desactivar todas las contraseñas de red y modifico 4000 registros de precios para adulterar la información de los productos. Al final este ex empleador fue identificado y procesado.

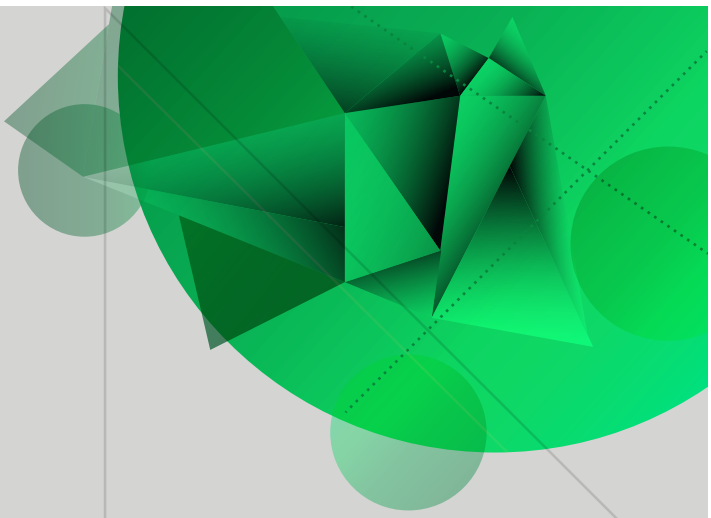
Según el ejemplo anterior identificar:

1. Qué tipo de amenaza encerraría la acción efectuada.
2. Qué factores influyeron para poder perpetuar cada uno de los ataques.
3. Si fuera usted el responsable de la seguridad que acciones tomaría para haber prevenido este tipo de ataques.

3

Unidad 3

Vulnerabilidades, tipos y factores



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Sobre esta cartilla trataremos cada uno de los temas relacionados a las vulnerabilidades teniendo en cuenta que es el primer factor importante al momento de detectar una amenaza o riesgo en una organización en sus sistemas informáticos. Muchas de las organizaciones hoy en día no se focalizan en cómo se encuentra su conformada su infraestructura, suponiendo que está estable solo porque sus aplicaciones están funcionando correctamente.

Toda la infraestructura o el sistema deben actualizarse de manera continua y con períodos de revisión con el fin de prevenir cualquier tipo de ataques o los riesgos causados por los sistemas vulnerables, donde la causa principal son los parches obsoletos o desactualización continua sobre las aplicaciones, en cada uno de los medios de comunicación que hacen en el campo tecnológico.

Los errores humanos al utilizar los sistemas pueden comprometer la integridad de la información manejada por la organización. Incluso las aplicaciones más sofisticadas están libres de este tipo de problemas, que pueden reducirse con paramentos de seguridad estrictos sobre la integridad de los datos y la formación adecuada del personal.

Imagen 1
Fuente: http://definicion.com.mx/imagenes/vulneralidad.jpg

A menudo errores simples pueden comprometer la integridad no sólo de los datos, también pueden causar la aparición de nuevas vulnerabilidades en los sistemas. Este tipo de amenaza es aún más relevante en las empresas que participan en el nuevo sector de las tecnologías, el desarrollo de sistemas y, a menudo interconectados entre varias organizaciones ejecutoras. Un error de programación sencilla en la administración o la falta de formación necesaria para evaluar las implicaciones de seguridad de especial enfoque de desarrollo, puede causar vulnerabilidades que afectan a los sistemas de las organizaciones no sólo de los usuarios, sino también a las empresas que desarrollan que podía ver muy desfavorecido en su imagen corporativa.

U3

Metodología

Leer y entender el contenido plasmado sobre la cartilla, apoyarse en el documento de lecturas complementarias y auto investigación sobre los temas que serán vistos en esta semana. Tener como apoyo los recursos complementarios para la profundización del tema visto.

Importante tener en cuenta que "siendo los sistemas informáticos los medios que nos permiten la comunicación, el almacenamiento y el tratado de la información, es relevante que cada sistema esté protegido y actualizado para así evitar cualquier tipo de vulnerabilidad existente".

U3

Desarrollo temático

Vulnerabilidades, tipos y factores

Vulnerabilidades

Dependiendo del enfoque de seguridad de la computadora, un sistema informático está expuesto al peligro por dos factores: amenazas y vulnerabilidades.

Las vulnerabilidades son el otro factor que pone en peligro la seguridad de un sistema, en general se cree que una vulnerabilidad es una debilidad en un sistema y si bien no es una definición incorrecta, tampoco expresa plenamente lo que es una vulnerabilidad.

Una vulnerabilidad de software es un elemento de un sistema informático que puede ser explotado por un atacante para violar la seguridad, también pueden causar daño por sí mismos sin ser un ataque deliberado.

Las vulnerabilidades fueron consideradas un elemento interno del sistema, por lo que corresponde a los administradores y usuarios de detectar, evaluarlos y reducirlos.

Tipos de vulnerabilidades

Las vulnerabilidades son el resultado de errores de programación (bugs), fallas en el diseño del sistema, incluidas en las limitaciones tecnológicas pueden ser explotadas por atacantes.

Vulnerabilidades físicas

Debilidades en orden físico son las presentes en los entornos en la que la información se almacena o manipula.

Ejemplo de este tipo de vulnerabilidad se pueden distinguir: instalaciones inadecuadas espacio de trabajo, la falta de recursos en los puestos de trabajo; disposición desordenada de los cables de alimentación y de red, la falta de identificación de personas y locales, entre otros.

Estas debilidades al ser explotadas por amenazas, afectan directamente a los principios básicos de la seguridad de la información, especialmente la disponibilidad.

Vulnerabilidades naturales

Debilidades naturales son los relacionados con las condiciones de la naturaleza que puedan poner en riesgo la información. A menudo, la humedad, el polvo y la contaminación pueden causar daños a los bienes.

Por lo tanto, deben ser protegidos para garantizar sus funciones. La probabilidad de exposición a los peligros naturales es crucial en la elección e instalación de un entorno. Deberán tener especial cuidado con el local, según el tipo de riesgo natural que puede ocurrir en una región geográfica particular.

Ejemplo: los peligros naturales más comunes pueden incluir entornos de fuego sin protección, cerca de los ríos que podrían causar inundaciones en la infraestructura, locales que no pueden resistirse a las manifestaciones de la naturaleza, como terremotos, tsunamis, huracanes, etc.

Vulnerabilidades de hardware

Imagen 2
Fuente: http://static.wixstatic.com/media/d1a2d2_13add2b23d4d334d39a420a59d0f1381.jpg_1024

Posibles defectos de fabricación o la configuración de los equipos de la empresa que permitiría el ataque o alteración de la misma. Hay muchos elementos que representan debilidades de hardware. Entre ellos podemos mencionar: la falta de actualizaciones de acuerdo con las directrices de los fabricantes en los programas que se utilizan, y el mantenimiento inadecuado de los equipos.

Por lo tanto, trata de evaluar la seguridad informática: si el hardware utilizado es de tamaño adecuadamente sus funciones. Si usted tiene suficiente almacenamiento, el procesamiento y la velocidad. Ejemplo: la falta de copias de seguridad de configuración o equipos de contingencia podría representar una vulnerabilidad de sistemas de la empresa.

Vulnerabilidades de software

Los puntos débiles que se producen las aplicaciones permiten el acceso no autorizado a sistemas informáticos, incluso sin el conocimiento de un usuario o administrador de red. Debilidades de software relacionados pueden ser proporcionados por varias amenazas ya conocidas. Entre ellas están:

Una configuración incorrecta e instalación de programas informáticos, que pueden llevar a un mal uso de los recursos por usuarios maliciosos. A veces, la libertad de uso implica un mayor riesgo.

Ejemplo: lectores de correo electrónico que permiten la ejecución de código malicioso, editores de texto que permiten la ejecución de los virus de macro, etc. Estas deficiencias ponen en riesgo la seguridad de los entornos tecnológicos

Las aplicaciones son elementos que realizan la lectura de la información y permitir al usuario el acceso a esos datos en medios electrónicos, por lo tanto, se convierten en el blanco preferido de las amenazas de los agentes causantes. Ejemplo: También pueden tener software de aplicación utilizado para la edición de texto e imagen, para automatizar procesos y permitir la lectura de la información de una persona o empresa, como las páginas de los navegadores de Internet.

Los sistemas operativos como Microsoft ® Windows ® y UNIX ®, que proporcionan la interfaz para configurar y organizar un entorno tecnológico. Estos son el blanco de los ataques, porque a través de ellas se pueden hacer cualquier alteración de la estructura de una computadora o red. Ejemplo: Estas aplicaciones son vulnerables a varias acciones que afectan a la seguridad, como la instalación incorrecta y la configuración, sin actualización, programación insegura etc.

Imagen 3
Fuente: http://static.wixstatic.com/media/d1a2d2_13add2b23d4d334d39a420a59d0f1381.jpg_1024

Vulnerabilidades de medios de almacenaje

Los medios de almacenamiento son medios físicos o magnéticos utilizados para almacenar información. Los tipos o medios de almacenamiento de información que están expuestos son: disquetes, CDs, discos duros de los servidores y bases de datos, así como lo que se registra en el papel.

Si los medios de comunicación que almacenan información no se utilizan correctamente, el contenido de los mismos puede ser vulnerables a una serie de factores que pueden afectar la integridad, disponibilidad y confidencialidad de la información. Ejemplo: medios de almacenamiento pueden ser afectadas por los puntos débiles que se pueden dañar o incluso dejarlos inservibles. Estas debilidades son: período de validez y defecto de fabricación, mal uso, ubicación de almacenamiento poco saludable de la humedad, el magnetismo o estática, moho, etc.

Imagen 4
Fuente: http://static0.bigstockphoto.com/thumbs/0/0/2/small2/20037182.jpg

Vulnerabilidades de comunicación

Este tipo de debilidad se extiende a toda la información que transita por la red. Donde quiera que la información se transite, ya sea a través de cable, satélite, fibra óptica u ondas de radio, tiene que haber seguridad. Los Datos que viajan es un aspecto crucial al momento de aplicar la seguridad de la información.

Hay un gran intercambio de información a través de los medios de comunicación que rompen las barreras físicas tales como teléfono, Internet, WAP, fax, télex, etc. Por lo tanto, estos medios deben ser tratados con la seguridad adecuada para el propósito de prevenir: cualquier ruptura en la comunicación hace que la información queda disponible para los usuarios, o por el contrario, estar a disposición de cualquier persona que no tenga derechos de acceso.

La información se altera en su estado original, afectando su integridad. Por lo tanto, la seguridad de la información también se asocia con el desempeño de los equipos involucrados en la comunicación, ya que les importa: la calidad del medio ambiente que se preparó para el tránsito, el procesamiento, el almacenamiento y lectura de información.

Imagen 5
Fuente: http://www.muycomputerpro.com/wp-content/uploads/2012/03/WiFi.jpg

Vulnerabilidades humanas

Esta categoría de vulnerabilidad está relacionada con el daño que puede hacer las personas a la información y el entorno tecnológico que soporta. Debilidades humanas también pueden ser intencional o no. Muchas veces, los errores y accidentes que ponen en peligro la seguridad de la información se producen en entornos institucionales. La mayor vulnerabilidad es la falta de medidas de seguridad adecuadas para ser adoptada por cada elemento constituyente, principalmente miembros internos de la empresa. Dos debilidades humanas, por su grado de frecuencia son: la falta de formación específica para la ejecución de las actividades relacionadas con las funciones de cada uno, la falta de conciencia sobre la seguridad a la rutina diarias de sus actividades, errores, omisiones, etc. insatisfacción.

En cuanto a las vulnerabilidades humanas de fuentes externas, podemos considerar a todos aquellos que se pueden explorar por amenazas como el vandalismo, el fraude, la invasión, etc.

Imagen 6
Fuente: http://www.hubsante.org/sites/default/files/styles/image_full_810x239/public/culture_numerique.png?itok=YpvpRxLZ

"El riesgo es el producto de la ocurrencia de la amenaza y su consecuencia"

Factores de la vulnerabilidad

Se trata de un conjunto de factores que permite a las personas para identificar, ya sea mayor o menor la probabilidad de estar expuestos a un desastre de este conjunto de elementos, pero todos ellos tienen una estrecha relación o vínculo que no se presenta de una manera aislada.

Los factores más importantes de la vulnerabilidad son:

Factores físicos: están relacionados a condiciones específicas y la ubicación de los asentamientos humanos y las condiciones de producción de la infraestructura.

Entre las condiciones específicas de estos asentamientos pueden ejemplificar: el uso de técnicas y materiales de construcción resistentes a los terremotos. Un factor de vulnerabilidad es la ubicación de los asentamientos humanos en las laderas. En los volcanes de la falda de las zonas costeras que experimentan inundaciones y terremotos faltas.

Factores ambientales o ecológicos: son las que se relacionan en la manera de cómo una comunidad utiliza elementos insostenibles de su entorno, lo que debilita la capacidad de los ecosistemas para absorber sin riesgos naturales de lesiones. Por ejemplo: la deforestación de una ladera.

Factores económicos: la ausencia o la disponibilidad limitada de recursos económicos de los miembros de una localidad, como el mal uso de los recursos disponibles para la gestión de riesgos adecuada un ejemplo a señalar es la pobreza, que se conoce como una de las principales causas de la vulnerabilidad.

Factores sociales: se refiere a un conjunto de relaciones, comportamientos, creencias, formas de organización y el modus operandi de las localidades e instituciones que sitúan en una menor vulnerabilidad más o entre estos están:

Factores políticos: la baja capacidad del sector para tomar decisiones o para influir en las autoridades locales o nacionales sobre cuestiones que los afecten, también puede relacionarse con la gestión y negociación con los agentes externos que pueden afectar a sus condiciones positivas o negativas y la falta de alianzas para influir a sus decisiones territoriales.

Factores Educativos: el contenido y los métodos de enseñanza son percibidos como un concepto socioeconómico aislada población, la educación de calidad debe tener en cuenta el comportamiento de aprendizaje que permitan a las amenazas de cara, prevenir y actuar adecuadamente en situaciones de desastre puede ser un ejemplo ausencia de contenidos educativos relacionados con la gestión del riesgo en los planes de estudio.

Factores ideológicos y culturales: se refiere al concepto y prejuicios que los hombres y las mujeres tienen sobre el mundo y la vista de cómo se interpretan los fenómenos, esto incluye en la prevención de este tipo son las creencias sobre el origen de la catástrofe debe ver con la voluntad o por Dios.

Factores organizativos: el grado en que las comunidades se organizan articuladas y con una visión clara de su vulnerabilidad y por lo tanto amenaza con ser su respuesta a un desastre, una ciudad que tiene un plan para la gestión de riesgos en el lugar esta menos expuesta al impacto de un desastre.

Factores Institucionales: significa que las instituciones tienen estrategia eficaz y eficiente para la gestión de riesgos con el fin de actuar adecuadamente; una ciudad donde las instituciones funcionan de manera coordinada en el marco del enfoque de gestión del riesgo se reducirá el impacto que puede producirse un suceso como un terremoto, tormenta tropical y otros.

Para el análisis de este conjunto de factores de vulnerabilidad, se debe contar que pueden influir directa o indirectamente en el caso de que esto tiene un mayor o menor impacto en su localidad.

Ejemplos

- Microsoft Windows, el sistema operativo de los sistemas más utilizados conectados a Internet, contiene múltiples vulnerabilidades graves. El más utilizado son en IIS, MS-SQL Internet Explorer, y los servicios de servicios de archivos y mensajes del sistema operativo de procesamiento.
- Una vulnerabilidad en IIS, se detalla en el Microsoft Security Bulletin MS01-033, es una de las vulnerabilidades de Windows más utilizados. Durante años enteros, un gran número de gusanos de red se han escrito para usar esta vulnerabilidad, incluyendo 'CodeRed'. CodeRed se detectó por primera vez el 17 de julio de 2001, y se cree que infectar a más de 300.000 artefactos. Interrumpió un gran número de empresas y causó enormes pérdidas financieras en todo el mundo. Aunque Microsoft ha creado un parche para la vulnerabilidad, junto con el Boletín MS01-033 de seguridad, algunas versiones de que el gusano CodeRed aún están difundiendo en todo el internet.
- El gusano de red *spida* detecta prácticamente un año después CodeRed aparecía, utilizó una exposición de MS-SQL Server para extenderse. Algunas instalaciones omitidas del servidor MS-SQL no tiene una cuenta de contraseña del sistema 'SA'. Esto permitió que cualquier persona con acceso a la red para el sistema ejecuta las instrucciones. Mediante el uso de esta exposición, el gusano configura la cuenta "Invitado" para permitir que los archivos compartidos abiertos y descargado para orientar el acceso al sistema. Luego utiliza el mismo MS-SQL no la contraseña, vaya a cuenta del 'SA' para lanzar una copia remota de sí mismo, extendiendo así la infección.
- Gusano *slammer* red detectada a finales de enero de 2003, utilizó una aún más directa para infectar el servidor en los sistemas Windows con el método de MS-SQL: una vulnerabilidad de desbordamiento de búfer en un subrutinas servidor UDP manejo de paquetes. Como era relativamente pequeño-376 bytes - y utilizado UDO, un protocolo diseñado para la rápida transmisión de datos, *slammer* propagación de una manera casi increíble. Se estima *slammer* tarda sólo 15 minutos distribuidos en todo el mundo, infectando alrededor de 75.000 hosts.

  Estos tres gusanos notables basan en vulnerabilidades de software y las exposiciones de varias versiones de Microsoft Windows. Sin embargo, el gusano Lovesan detectó el 11 de agosto de 2003, utiliza un error de búfer desbordamiento mucho más grave en un componente de Windows para propagarse. Esta vulnerabilidad se detalla en el Microsoft Security Bulletin MS03-026.
- Sasser, que apareció a principios de mayo de 2003, utiliza otra vulnerabilidad componente vegetal, esta vez en el servicio de subsistema de autoridad local (LSASS). Información sobre la vulnerabilidad fue publicada en el Boletín de Seguridad MS04-011 Microsoft. El Sasser se propagó rápidamente, e infectó millones de ordenadores en todo el mundo, lo

que representa un costo enorme para las empresas. Muchas organizaciones e instituciones se vieron obligadas a suspender sus operaciones debido a interrupciones en la red causadas por el gusano.

Sin excepción todos los sistemas operativos contienen vulnerabilidades y exposiciones que pueden ser el blanco de los hackers y creadores de virus. Aunque vulnerabilidades de Windows reciben la mayor publicidad debido a la cantidad de dispositivos que funcionan con Windows, Unix tiene sus propias debilidades.

- Durante años, una de las exposiciones más populares en el mundo Unix ha utilizado el servicio de *finger.* Este servicio permite a alguien fuera de una red para ver qué usuarios están conectados a ciertos equipos o ubicación desde la que los usuarios tienen acceso.

  El servicio de *finger* es útil, pero también expone una gran cantidad de información que puede ser utilizada por los piratas informáticos. Esto demuestra que podemos aprender algunas cosas interesantes sobre la máquina remota utilizando el servicio de dedo: tres usuarios conectados, pero dos de ellos han permanecido por más de dos días, mientras que el otro equipo ha estado fuera durante 22 minutos. Los nombres de los usuarios conectados que muestran el servicio dedo se pueden utilizar para tratar de hacer combinaciones de usuario / contraseña. Esto puede poner en peligro el sistema, sobre todo si los usuarios utilizan los nombres como contraseñas, una práctica relativamente común.

  El servicio de los *finger* no sólo expone información importante sobre el servidor host; pero ha sido el blanco de muchas hazañas, como el famoso gusano de red escrito por Robert Morris Jr. que fue lanzado el 2 de noviembre de 1988. Por ello, las más modernas distribuciones de Unix han este servicio, desactivado por defecto.

- El programa *sendmail,* originalmente escrito por Eric Allman, también es otro destino popular para los piratas informáticos. 'Sendmail' fue desarrollado para manejar la transferencia de mensajes de correo electrónico a través de Internet. Debido al gran número de sistemas operativos y configuraciones de hardware, el *sendmail* se convirtió en un programa extremadamente complejo, que tiene un largo y notorio historial de vulnerabilidades graves. El gusano Morris utilizó un 'sendmail' explotar una vulnerabilidad y 'dedo' a extenderse.

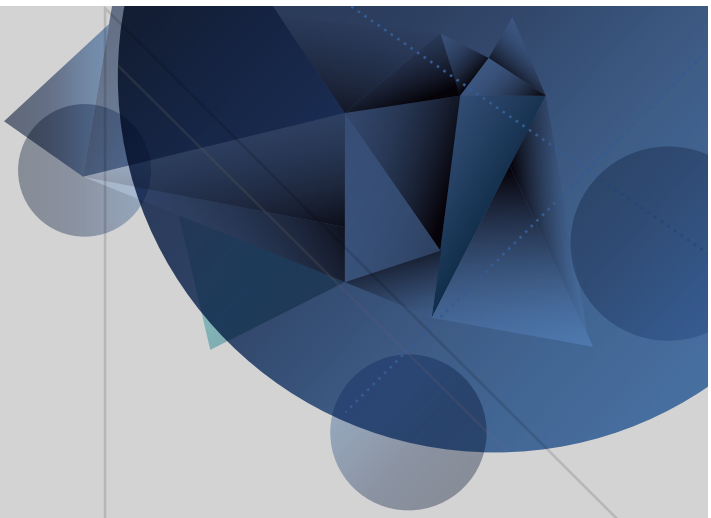
  Hay muchas otras hazañas populares en el mundo de Unix que se dirigen a los paquetes de software como SSH, Apache, WU-FTPD, BIND, IMAP / POP3, varias partes del kernel, etc.

Los *exploits*, vulnerabilidades e incidentes mencionados anteriormente destacado un hecho importante. Aunque el número de sistemas que ejecutan IIS, MS-SQL u otros paquetes de software específicos se puede contar en cientos de miles de personas, el número total de sistemas que ejecutan Windows es de alrededor de varios cientos de millones. Si todos estos artefactos fueron blancos de un gusano o un hacker usando una herramienta de hacking automatizada, podría poner en grave riesgo la estructura interna y la estabilidad de internet.

4

Unidad 4

Métodos y técnicas de intrusión



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Una técnica de intrusión es un conjunto de actividades que tienen por objetivo violar la seguridad de un sistema informático. Estas técnicas no solo deben ser conocidas por los atacantes, es imprescindible que sean conocidas por todos aquellos profesionales de las tecnologías de información a fin de proteger y resguardar los sistemas y medios de información de manera veráz y oportuna.

Sobre esta cartilla conoceremos los diferentes tipos de ataques o métodos de intrusión que se pueden deliberar en la seguridad informática, teniendo en cuenta que el objetivo es poder causar daño o robo de información para fines lucrativos o para difamar una organización. Para este capitulo nos enfocaremos a los ataques que son provocados deliberadamente.

Los autores de las intrusiones pueden ser internos y externos a la organización. Es notable observar que muchos estudios sobre el fraude y el robo a través de tecnología de la información están de acuerdo en que la mayor parte de las actividades fraudulentas son realizadas por personas vinculadas a la propia organización, pueden ser causados con acceso a los sistemas y la información no controlada, los ex empleados con conocimiento de ambos sistemas y las medidas de seguridad interna o personas vinculadas de alguna manera a la organización y disfrutan de ciertos privilegios que a menudo se esconden debajo de aparentes relaciones con la empresa.

Imagen 1
Fuente: http://www.livinghometech.co.uk/images/control4-7inwalltouchscreen-hand.jpg

Las intrusiones a menudo generan daño económico significativo, pero en cualquier caso, causan sensación importante de vulnerabilidad en toda la organización, que se agrava si no es posible identificar a los autores de los ataques, las técnicas utilizadas para cometerlos u objetivos perseguidos.

La definición de un ataque es simple; teniendo en cuenta que una amenaza se define como un sistema de información de la condición (persona, máquina, acontecimiento o idea) que, dada la oportunidad, podría dar lugar a una violación de la seguridad (confidencialidad, integridad, el medio ambiente disponibilidad debe ocurrir o uso legítimo), un ataque es nada más que la realización de una amenaza.

U4

Metodología

Entender y conocer las diferentes técnicas que existen en un ambiente global con la finalidad de poder obtener información de una organización o de una persona para infringir daños monetarios o sociales, cada ataque es dirigido a personas en especial o sistemas informáticos que podrían alterar su entorno. Muchas de las organizaciones o personas por el desconocimiento no están pendientes de este tipo de ataques y de esta forma son atacados fácilmente, sin contar con un sistema de seguridad acorde para poder proteger o reguardar su información.

U4

Desarrollo temático

Métodos y técnicas de intrusión

Reconocimiento y obtención de información

Leer y entender el contenido plasmado sobre la cartilla, apoyarse en el documento de lecturas complementarias y auto investigación sobre los temas que será visto en esta semana. Tener como apoyo los recursos complementarios para la profundización del tema visto.

Bases de datos públicas

Una de las razones de las vulnerabilidades de bases de datos son tan extendidas es el hecho de que la mayoría de las bases que existen se han programado para dar dinamismo a las páginas sin tener que preocuparse por las implicaciones de seguridad.

El programador de base de datos quien publica en la web, a menudo no sabe que un fallo de seguridad puede poner en peligro todo el servidor que aloja la página. Y los administradores de servidores web que ofrecen servicios a sus clientes, pueden hacer poco para detenerlo porque es un muy extenso trabajo para supervisar todas las acciones de los usuarios de uno en uno.

Web

La World Wide Web es un sistema de documentos de hipertexto e hipermedia (Los documentos pueden bifurcar o ejecutar cuando se le solicite) vinculados y accesible a través de la red informática internet.

Esta realización se puede proporcionar para ocultar código malicioso en las páginas Web, los cuales son ejecutados por usuarios sin mayor parte del tiempo nos damos cuenta, la exposición de la seguridad del sistema. Por otra parte, el Internet es un gran control de dicha red y la regulación es casi imposible, por lo que su uso implica la constante exposición a los distintos tipos de amenazas y la seguridad recae en todos y cada uno de sus miembros.

DNS

El DNS (*Domain Name Service*) es un sistema de nomenclatura para traducir nombres de dominio a direcciones IP y viceversa. Aunque internet sólo funciona en base a direcciones IP, DNS permite a los seres humanos utilizamos nombres de dominio que son bastante simples para recordar.

Los diferentes ataques por DNS se basan principalmente en el robo de identidad, tomar la identidad de otro elemento para realizar ciertas acciones perjudiciales, como los usuarios de interceptación que quieren acceder a determinados recursos en línea re direccionar su petición a cualquier otro sitio.

Keyloggers

Keyloggers son un tipo de software responsable de registrar todas las actividades del teclado de los equipos informáticos sin el conocimiento del usuario; por lo general se utilizan para los obtener paswords de acceso autorizado.

Los *keyloggers* también pueden ser utilizados para la seguridad informática, ya que permiten hacer un seguimiento de lo que hacen los usuarios cuando utilizan el equipo.

Por ejemplo, pueden usarse para determinar qué acciones un usuario realizó durante una sesión de trabajo para interpretar las secuencias introducidas por teclado. Tales acciones pueden revelar si el usuario introdujo una cuenta que no pertenezca o información importante del sistema modificado.

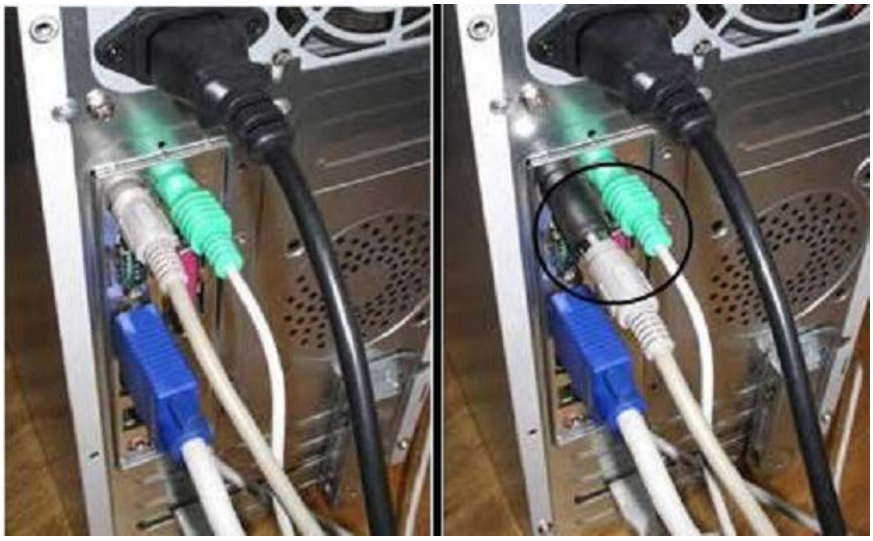


Imagen 2
Fuente: http://s.glbimg.com/po/tt/f/original/2012/10/08/kyelogger02.jpg

Aunque menos comunes, los keyloggers también pueden ser dispositivos de hardware conectados al puerto del teclado.

Ingeniería social

La ingeniería social es la práctica de obtener información confidencial mediante la manipulación de usuarios legítimos. Un ingeniero social comúnmente usar el teléfono o Internet para engañar a la gente y llevarla a revelar las políticas de seguridad sensibles o violar información típica. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, en lugar de explotar agujeros de seguridad en los sistemas informáticos. Se conviene en general que "los usuarios son el eslabón más débil" en materia de seguridad; este es el principio que rige la ingeniería social.

Otros

Jamming o flooding: este tipo de ataques saturan los recursos del sistema. Por ejemplo, un atacante puede consumir todo el espacio de memoria o disco disponible y enviar tráfico a la red para que nadie más pueda usarlo.

Packet sniffing: muchas redes son vulnerables a las *eavesdropping* (literalmente traducido como " escuchar secretamente "), que consiste en la intercepción pasiva del tráfico de red (sin cambios). En internet esto se hace mediante analizadores de paquetes o sniffers, que son programas que monitorean los paquetes de red que están dirigidos a la computadora donde están instalados. El sniffer se puede colocar en una estación de trabajo conectada a equipos de red tal como un router o una puerta de enlace a internet, y esto se puede hacer por alguien con acceso legítimo, o por un intruso que entró a través de otros canales.

Snooping y downloading: los ataques de esta categoría tienen el mismo objetivo que el *sniffing,* obtener la información sin modificaciones. Sin embargo, los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otros datos guardados, actuando en la mayoría de los casos, una descarga, es decir, un proceso de descarga de la información a su propia computadora.

Tamppering o data diddling: esta categoría se refiere a la modificación no autorizada de datos o software instalado en un sistema, incluyendo la eliminación de archivos. Estos ataques son particularmente graves cuando se realiza dado que ha obtenido derechos gerente o supervisor, con la capacidad de ejecutar cualquier comando y así alterar o borrar cualquier información que puede incluso resultar en el sistema total más bajo deliberadamente.

Identificación de vulnerabilidades

Las vulnerabilidades son aspectos del sistema que son utilizados por los atacantes para romper la seguridad. Es difícil de detectar un ataque usando una vulnerabilidad porque el atacante se aprovecha de una característica del sistema operativo (puede ser de hardware, software o sistema de la misma organización) en lugar de llevar a cabo un ataque por la fuerza utilizando medios externos.

Identificar las vulnerabilidades en el sistema es una actividad importante para ambos lados, el atacante y el defensor; No se puede eliminar una entrada de la vulnerabilidad de su existencia es desconocida.

Ataques a redes telefónicas

El hecho de que las nuevas redes de telefonía corporativa están conectados a redes de datos corporativos que los hace un blanco atractivo para los atacantes, que pueden utilizar como una puerta de entrada a los sistemas de información. A partir de ahí, pueden robar información corporativa, escuchar las conversaciones y crear confusión en el sistema debido a la ignorancia del origen del ataque.

La forma principal de amenaza de ataque y las redes telefónicas, es la intercepción de información, sino también la instalación de terminales no autorizados es un problema importante en este medio.

También incluso casos actuales donde el servicio no está disponible, ya sea debido a una saturación del medio de transmisión o incluso daños a la infraestructura.

Barrido de puertos

La exploración de barrido o puerto es comprobar qué puertos están disponibles para ser explorado dentro de uno o varios equipos de una red. Por sí mismo, el escaneo de puertos es una actividad normal que se utiliza a menudo para mejorar los servicios de seguridad y rendimiento de la red, pero también puede convertirse en una actividad perjudicial, ya que se puede utilizar para buscar puntos de acceso vulnerables para forzar la conexión.

Hay casos en que el sistema tiene varios puertos abiertos y son desconocidos por el oficial de seguridad, y por lo tanto estos puertos no se supervisan y los datos pueden fluir a través de ellos sin ningún tipo de control de seguridad, por lo que es una vulnerabilidad del sistema.

Esto puede deberse a una mala configuración de sistemas (por ejemplo, cortafuegos) de seguridad que pueden dejar muchos puertos abiertos por defecto, y el Firewall de administradores de revisar cuidadosamente la configuración se olvide de comprobar todos los puertos disponibles.

Identificación de *Firewalls*

Un *firewall* es un dispositivo de seguridad que filtra los paquetes de datos a partir de una serie de reglas y criterios definidos por un administrador de red. Este dispositivo puede ser una máquina diseñada y construida específicamente para esta función, pero también puede ser un software que se instala en un ordenador conectado a la red a través del cual los datos se filtran antes de ser distribuido a los demás equipos de la red. Cada equipo puede tener un firewall de software instalado para un solo filtro.

Los atacantes pueden saltar de un *firewall* mediante puertos abiertos que se aprovechan del sistema. Un método común para descubrir los puertos vulnerables está enviando una serie de paquetes de datos defectuosos (por ejemplo, dirigida a una red IP inexistente), que cuando se filtra, el *firewall* interceptará y no permitir su enrutamiento, pero si no se está filtrando el puerto, después se dejó para aprobar el paquete y no puede enrutar correctamente, el cortafuegos enviará un mensaje de error ICMP (*Internet Control Message Protocol*) que indica que el paquete no se filtró. Usted puede crear un esquema para indicar los puertos que no se está filtrando a partir de los mensajes de error que se generan por este proceso.

Identificación de Sistemas Operativos / OS *Fingerprinting*

Fingerprinting OS es el proceso para identificar el sistema operativo de un usuario remoto a través de una red, esta identificación se basa en las características que diferencian cada uno de los otros sistemas: diferentes implementaciones de la pila TCP / IP, diferentes comportamientos para los paquetes que envían que tienen una particular, la forma, las diferentes respuestas dependiendo del protocolo utilizado (TCP, ICMP, ARP), etc.

El objetivo de esta técnica no se limita a identificar el sistema operativo remoto, también se puede obtener información sobre cómo funciona en el caso de un sistema personalizado que no se pueden encontrar en una lista de compras.

El *fingerprinting* tiene aplicaciones beneficiosas para la seguridad informática, pero como la mayoría de estos recursos, también se puede utilizar para un ataque, con la identificación de un sistema operativo a distancia, uno de los primeros pasos a seguir para un ataque.

Vulnerabilidades en el Software

Las vulnerabilidades en el software pueden ser defectos en la programación, configuración, análisis, diseño o ejecución y pueden ocurrir en los programas de seguridad, navegadores de Internet, administradores de bases de datos, número de solicitud y el mismo sistema operativo.

Un atacante puede usar estas vulnerabilidades para introducirse a un sistema dependiendo de su función, el software y las herramientas con las que cuenta, por lo que cada caso es diferente, pero una forma común de avanzar es reunir primero toda la información posible sobre el sistema de destino.

Métodos de Identificación

Hay dos métodos de *fingerprinting* clasificados como activo y pasivo.

Fingerprinting activo: se basa en el análisis de la respuesta del servidor que desea comprobar cuando se le envía ciertos paquetes TCP y UDP.

El *fingerprinting* activo tiene la ventaja de que se puede experimentar diferentes tipos de paquetes para forzar el envío de diferentes respuestas del sistema, esto da una gama más amplia de resultados cuando se están analizando, que son muy útiles en la determinación de las características del sistema.

Su principal desventaja es que es fácil de detectar e interceptar por los dispositivos de seguridad (por ejemplo cortafuegos) implementado en la red donde se analiza el sistema. Como se ha mencionado, el tipo de pruebas que se realizan en el sistema analizado por este método, es para enviar paquetes y analizar las respuestas.

Fingerprinting pasivo: *fingerprinting* pasivo se basa en la captura de paquetes de datos desde un sistema remoto, a diferencia del *fingerprinting* activo donde se envían los paquetes.

Esta captura de paquetes se logra a través de programas llamados sniffers, que son programas que registran las actividades y tramas de datos hacia y desde un ordenador conectado a una red.

Con base en los paquetes capturados de un *sniffer,* se puede determinar el sistema operativo del sistema remoto. Como en el caso de la identificación activa, pasiva se basa en el principio de que todas las direcciones IP

proporcionan información sobre las características del sistema operativo. Analizando los paquetes capturados y la identificación de estas diferencias puede determinar el sistema operativo de la máquina remota.

Técnicas de intrusión y ataques

Control de accesos

El control de acceso requiere no sólo la capacidad de identificar, pero también asociarlo con la apertura y cierre de puertas, permitir o denegar el acceso en función de las limitaciones de tiempo, área o sector dentro de una empresa o institución de acceso. Los controles de acceso incluyen el uso de personal de seguridad, dispositivos de acceso electrónico y la verificación, cerraduras manuales y electrónicos, y la implementación de políticas de seguridad y las normas entre el mismo personal.

Una intrusión a las instalaciones físicas se da generalmente por los empleados que saben y tienen acceso directo a las instalaciones, en casos muy raros puede ser perpetuado por personas sin relación alguna, como ladrones, espías y terroristas.

Imagen 3
Fuente: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/img/DSI_22.jpg

Configuración de servicios y servidores

Hay muchos casos en que los riesgos pueden reducirse simplemente para verificar la configuración de todos los servicios que forman parte de un sistema.

Todos los servicios vienen con una configuración estándar que puede proporcionar una instalación rápida y facilidad de uso, pero no es el más adecuado para satisfacer las necesidades de seguridad. Muchas veces un servicio mal configurado se convierte en una grave vulnerabilidad a ser explotadas por atacantes. Así que cuando se implanta un servicio o dispositivo dentro de una red, es necesario llevar a cabo una configuración personalizada que cumpla con las políticas de seguridad, el mantenimiento de un equilibrio entre la funcionalidad del sistema y seguridad.

Software

Los atacantes pueden explotar diferentes vulnerabilidades de software (errores de programación, mal diseño, mala configuración, etc.) para penetrar en una red o sistema, pero también hay software sin ser necesariamente malicioso, puede utilizarse para violar la seguridad. En el mercado existen numerosas aplicaciones que se crearon para ayudar en la mejora continua de los sistemas de gestión de seguridad y facilitar la conectividad de una red, pero también son herramientas utilizadas en el acceso no autorizado a los sistemas.

Ejemplos más concretos son Nmap, un software que permite escanear puertos TCP y UDP o *Netslumber,* una aplicación que funciona de forma continua del espectro radioeléctrico para redes inalámbricas disponibles.

También hay software a medida, creado por los mismos atacantes con el fin de ayudar a penetrar en los sistemas de seguridad.

Robo de identidad

Este tipo de ataque tiene lugar cuando el atacante se hace pasar por otro usuario, con el fin de obtener acceso a la red, obtener privilegios de usuario superiores o realizar transacciones financieras fraudulentas.

El atacante podría robar la identidad directamente a través de los equipos informáticos de la víctima, para obtener el código de usuario y contraseña, o falsificar identificaciones electrónicas y digitales.

Una variante del robo de identidad es el robo de sesión, como su nombre indica, es secuestrar la sesión iniciada por otro usuario, teniendo acceso a todos los recursos que la víctima tenga acceso.

También suplantar una dirección IP es el robo de identidad, haciéndose pasar por equipo de cómputo en el otro. Este tipo de suplantación es posible cambiar manualmente la configuración de red del ordenador.

Imagen 4
Fuente: http://actualidadradio.com/media/2016/03/RoboDeIdentidad.jpg

La mayoría de las personas no saben que han sido víctimas de robo de identidad hasta que se reflejan misteriosos cobros en su crédito facturas.

SQL *Injection*

Este error surgió con el boom de las aplicaciones Web que utilizan bases de datos. Se produce cuando se introducen los datos suministrados por el usuario como parte de una consulta SQL. Inyección SQL se produce cuando se inserta o "inyectada" Un código "invasor" SQL dentro de otro código SQL para alterar su funcionamiento normal.

Cuando se ejecuta esta base de datos de consulta, el código SQL también inyectado se ejecuta y podría hacer un número de cosas, tales como registros de insertar, modificar o eliminar datos, el acceso autorizado e incluso ejecutar código malicioso en el equipo.

Virus y gusanos

Un virus es código escrito con la intención expresa de replicarse. Un virus se une a un programa y luego intenta propagarse de un ordenador a otro. Un verdadero virus no se propaga sin intervención humana, alguien tiene que compartir un archivo o enviar un correo electrónico para propagarse.

Un gusano, como un virus, está diseñado para copiarse a sí mismo de un ordenador a otro, pero lo hace de forma automática. En primer lugar, toma el control de características en

el equipo que puede transportar archivos o información. Una vez que un gusano se encuentra en su sistema, puede viajar solo. El gran peligro de los gusanos es su capacidad para replicarse en grandes números. Por ejemplo, un gusano podría enviar copias de sí mismo a todo el mundo en el email de la libreta de direcciones. Un gusano puede consumir memoria o ancho de banda de la red, lo que puede provocar que un equipo se bloquee.

Ataques a contraseñas

Un ataque a la contraseña es cualquier acción para obtener, modificar o eliminar las contraseñas de un sistema informático. Estos ataques pueden ser perpetrados con mayor facilidad si los usuarios autorizados utilizan contraseñas débiles, es decir, limitada por un número y tipo de caracteres contraseñas, también consideró contraseña débil cuando las palabras enteras (o deformaciones simples) se usan contenidos en un idioma.

En general, se recomienda el uso de combinaciones aleatorias de caracteres para formar una contraseña segura, con la desventaja de que la mayoría de los usuarios no pueden recordar estas contraseñas y contraseñas generalmente registradas en otros medios de comunicación (como un archivo de texto o una nota de papel) donde pueden extraviarla o pueden ser revisados por otros usuarios.

Sniffing

Sniffing es un ataque pasivo donde un usuario no autorizado se dedica a hacer el seguimiento de todos los paquetes de información que circulan en la red con un sniffer. El tráfico de las redes inalámbricas puede ser espiado más fácilmente que una red convencional, ya que sólo una tarjeta de red y un ordenador para iniciar la interceptación de datos, independientemente de si están encriptados o no es necesario.

El análisis de tráfico, en este tipo de ataque pasivo el atacante necesita para obtener la información que desea a través de un examen detallado de los patrones de tráfico: a qué hora determinados equipos están encendidos, la cantidad de tráfico que usted envía, por cuánto tiempo, etc.

Suplantación o enmascaramiento

Este tipo de ataque activo es obtener direcciones válidas por varios sniffer y el tráfico de análisis para saber a qué hora se conecte a hacerse pasar por un usuario de la red atacada, así que cuando llegue el momento el atacante se hace cargo de la dirección del verdadero usuario y las identifica de entrada de red como verdadera, puede acceder a la información dentro de la red.

Otra forma es instalar puntos ilegítimos suplantación u/o acceso hostil (puntos de acceso) para engañar a la red autorizada para conectarse a este punto de acceso en lugar de la red a la que pertenecen los usuarios.

Denegación de servicio

Este método de ataque es donde la red atacante se ocupa de diversos tipos de interferencia, hasta muchos errores en la velocidad de transmisión cae abruptamente red o cesan ocurren operaciones. Cuando los ataques de corta vida es muy difícil de defender en contra de ellos, ya que sólo es posible detectar el momento de actuar.

Caballos de Troya

Son aparentemente inofensivos programas, con una función o utilidad particular, pero

contienen códigos ocultos para ejecutar diferentes acciones sobre el pc del usuario. Tienen que ver con el malware, que puede robar información confidencial de un equipo infectado, mientras que pasar por programas o servicios inofensivos.

Ejemplos

Ingeniera social:

En un estudio del caso, *hadnagy* describe cómo fue contratado como auditor para acceder a los servidores de una compañía de impresión y los vendedores de la competencia detrás de los procesos. En una reunión telefónica con su socio de negocios *hadnagy*, el director general le informó que "sería casi imposible de hackear" porque "cuidaba sus secretos con su vida."

"Era el tipo que nunca se enamoraría de esto", dijo *hadnagy*. "Pensé que alguien probablemente llamar y pedir la contraseña que estaba listo para un enfoque táctico de este tipo".

Después de alguna recopilación de información, *hadnagy* encontraría la ubicación de los servidores, direcciones IP, direcciones de correo electrónico, números de teléfono, direcciones físicas, servidores de correo, nombres de empleados, títulos y más. Pero el premio más grande fue cuando *hadnagy* descubierto que el CEO tenía un miembro de la familia que habían luchado contra el cáncer y estaba vivo. Como resultado, él estaba interesado e involucrado en la recaudación de fondos y la investigación del cáncer. A través de Facebook, también fue capaz de obtener otros detalles personales sobre el presidente, como su restaurante y equipamiento deportivo favorito.

Armado con la información, que estaba listo para atacar. Llamó al director general y se hizo pasar por una recaudación de fondos para el cáncer, de la caridad con la que el director general había intentado en el pasado. Él le informó que estaban ofreciendo un sorteo para las donaciones y los premios incluyen entradas para un partido jugado por su equipo favorito, así como los certificados de regalo de varios restaurantes, entre ellos su lugar favorito.

El CEO mordió el anzuelo, y accedió a que *hadnagy* le enviara un PDF con más información sobre la campaña de recaudación de fondos. Incluso consiguió el CEO de decirle que era la versión de Adobe Reader que llevaba porque, como le dijo el CEO "Quiero asegurarme de que estoy enviando un archivo PDF que se puede leer". Poco después de enviar el archivo PDF, el CEO de la abrió, la instalación de un programa malicioso que permite el acceso *hadnagy* a su máquina.

Cuando *hadnagy* y su compañero informaron a la empresa sobre el éxito de la violación al director general del equipo, el CEO estaba comprensiblemente enojado, añadió *hadnagy*.

Sentí que era injusto que usamos algo, pero así es como funciona el mundo", dijo *hadnagy*. "Un hacker malicioso no lo pensaría dos veces antes de utilizar esa información en contra de ellos".

Deducción 1: no hay información independientemente de su personal o emocional, que está fuera de los límites de un ingeniero social que busca hacer daño

Deducción 2: a menudo, la persona que piensa que es más seguro es el que tiene la mayor vulnerabilidad. Un consultor de se-

guridad dijo recientemente a los ejecutivos de las OSC son los blancos más fáciles de ingeniería social.

Ataques sin intención:

Un experto en seguridad informática advirtió que las aeronaves que incorpora el servicio de internet de pasajeros que ofrecen algunas aerolíneas podría ser la puerta de entrada para los hackers tomar el control de la aeronave.

Los viajes en avión cada vez tratan de ser cómodo para los viajeros que ofrecen no sólo comodidad sino también diversos servicios para ayudar a hacer el viaje más agradable. Pero en la búsqueda de esa mejora, podrían estar dejando fuera algunos problemas de seguridad. Al menos eso es lo que dijeron Chris Roberts, experto en seguridad informática en los aviones.

Según este especialista, algunas líneas aéreas utilizan la misma red para ofrecer conectividad Wi-Fi para los pasajeros y para sus sistemas de navegación. Así que deja abierta la posibilidad de que un hacker puede acceder a toda la información contenida dentro de la aeronave.

La advertencia de Roberts produjo en medio de una gran controversia como lo hizo a través de su cuenta de Twitter durante un vuelo. El mensaje fue enviado a la experta, "estoy en un 737/800 permite ver Cuadro-IFE-ICE-SATCOM? ¿Deberíamos empezar a jugar con mensajes EICAS?" PASS oxígeno "a alguien :)"?.

Su mensaje ha sido interceptado por la Oficina Federal de Investigaciones de los Estados Unidos decidió retrasar durante unas horas a Roberts para pedir explicaciones. Además, se le prohibió volar con esa aerolínea por vida.

Este altercado, lo que obligó al FBI a enviar una advertencia dirigida a las aerolíneas que les exigen estar atentos a cualquier comportamiento sospechoso que puede tener sus pasajeros en todos aquellos que tratan de utilizar cables para conectar sus dispositivos.

Para lograr la paz, los agentes de la agencia de investigación de Estados Unidos aclararon que no se muestra que la aeronave puede ser hackeado, pero necesitan mientras trabajan para lograr la paz. "A pesar de lo que los medios dicen que es teórico y no ha sido probada, publicidad en los medios asociados a estos casos puede animar a otros a utilizar los métodos descritos intrusión. Trate de obtener acceso no autorizado a las redes de un avión comercial es un delito federal que" explicaron.

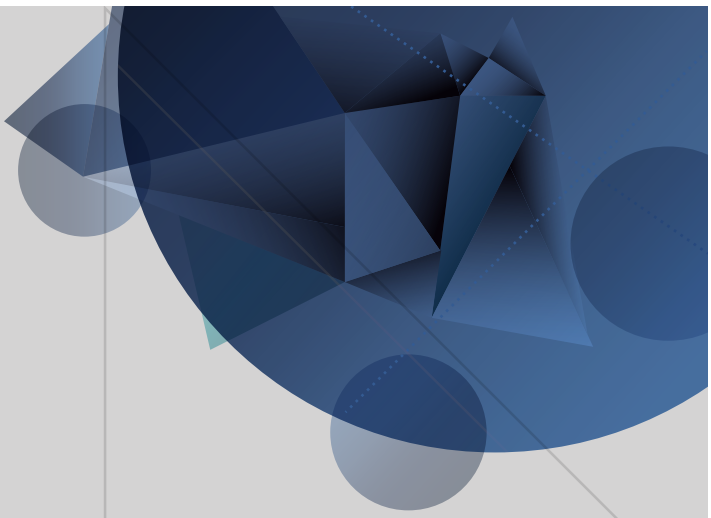
Con respecto a Roberts, hace años que estaba trabajando en la mejora de los sistemas de seguridad de la aeronave y al parecer, la razón por la que envió ese mensaje en Twitter iba a ser cansado para alertar a las compañías aéreas en sus vulnerabilidades y que no hacen nada al respecto.

La realidad es que hasta el momento ningún caso de ataques informáticos en los sistemas de control de la aeronave, pero, a raíz de una denuncia presentada por Roberts, las aerolíneas se vieron obligados a resolver cualquier tipo de debilidad en las barreras de seguridad.

4

Unidad 4

Política de seguridad en una compañía



Fundamentos de seguridad informática

Autor: Carlos Arturo Avenía Delgado

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Sobre esta cartilla conoceremos unos de los principios al momento de fomentar las seguridad informática en un organización, teniendo en cuenta que toda organización debe cumplir con unos estándares y normas establecidas, según su visión y misión, es por ello que deben contar con una política de seguridad aprobada por la parte gerencial y trasmitida al personal interno o externo que labore o tenga un vínculo con la empresa, con el fin conservar las mejores prácticas dentro de la compañía y en pro de sobreguarda la información.

Las políticas de seguridad de una organización son las normas y procedimientos internos que deben seguir los miembros de la organización para cumplir con los requisitos de seguridad que desean preservar. Debe describir la criticidad de los sistemas de información y las funciones de cada puesto de trabajo y los mecanismos de acceso a los sistemas, herramientas, documentación y cualquier otro componente del sistema de información. A menudo al desglosar las políticas de seguridad en procedimientos detallados para cada componente del sistema de forma individual, así que por ejemplo, puede crear documentos que describen las políticas de tratamiento de correos electrónicos, las políticas de uso de internet, copias de seguridad, virus de tratamiento y otra lógica maliciosa, las políticas de formación para la seguridad del personal, etc.

Los directivos de cualquier organización deben considerar la seguridad de la información como una parte integral de las estrategias corporativas y tácticas. Una vez incorporada la importancia de los sistemas para lograr uno de los objetivos y los riesgos que pueden significar la pérdida de la integridad de su información, falta de disponibilidad de los sistemas o de la violación de la confidencialidad de su información pueda surgir con mayor rigor otras medidas para atender a los objetivos de negocio de la compañía. Emergiendo desde el aspecto estratégico de la información y los sistemas corporativos, dos herramientas son a menudo generan gestión no es menos importante: las políticas de seguridad y el plan de contingencia.

Imagen 1
Fuente: Propia.

Cabe señalar que las políticas de seguridad deben emanar de la estrategia corporativa y que deben documentar todos los miembros del personal. Por su parte, el plan de contingencia se describe los procedimientos a seguir por la aparición de eventualidades significativas que podrían plantear serias consecuencias para la organización. Debe estar detallado cada uno de los pasos, por ejemplo en caso de destrucción total de los sistemas de inundación, incendio, etc. menudo la simple preparación del plan descubrir defectos en los sistemas que pueden ser aliviados con relativa facilidad. Por ejemplo, es posible que ninguna copia de seguridad de la información crucial para la compañía sigan siendo lugares físicamente seguros, o por lo menos distante para la ubicación de los sistemas susceptibles a los sitios de daño.

U4 Metodología

Leer y entender el contenido plasmado sobre la cartilla, apoyarse en el documento de lecturas complementarias y auto investigación sobre los temas que será visto en esta semana. Tener como apoyo los recursos complementarios para la profundización del tema visto.

U4

Desarrollo temático

Política de seguridad en una compañía

Políticas de seguridad informática

Las políticas son una serie de instrucciones documentadas que indica cómo se realizan algunos procesos dentro de una organización, también describió cómo tratar un problema o una situación específica.

Las políticas pueden ser vistas como un conjunto de características de una organización como leyes obligatorias, y están dirigidas al personal donde se proporcionan instrucciones generales, mientras que las normas indican requisitos técnicos específicos. Las normas, por ejemplo, pueden definir el número de bits de la clave secreta requerida en un algoritmo de cifrado. Por otro lado, las políticas simplemente definen la necesidad de un proceso de encriptación autorizado cuando la información confidencial se envía a través público, tales como las redes de internet.

Abordar el tema de la seguridad, una política de seguridad es un conjunto de reglas y prácticas que rigen la forma en que para gestionar, proteger y distribuir los recursos en una organización para llevar a cabo los objetivos de seguridad de la misma.

Objetivo de una política de seguridad

El propósito de una política de seguridad es la implementación de una serie de leyes, reglas, normas y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, ya su vez puede ser entendida y ejecutada por todos los miembros de la organización los que van destinados.

Misión, visión y objetivos de la organización

La misión, visión y objetivos varían mucho de una organización a otra, esto es normal si tenemos en cuenta que una organización es diferente de otra en sus actividades y todos los elementos que lo componen (elementos humanos, recursos materiales, infraestructura).

Rápidamente se definen los conceptos de misión, visión y organización.

Misión: la misma organización puede tener varias misiones que son actividades objetivas y específicas realizadas. Las misiones también destinados a satisfacer las necesidades de la organización. La misión está influido en ciertos momentos por parte de algunos elementos como la historia de la organización, las preferencias de gestión y / o propietarios, los factores externos o ambientales, los recursos disponibles y sus capacidades distintivas

Visión: es la imagen idealizada de lo que usted desea crear. Esta idea debe estar bien definida, como todas las actividades de la organización se centrarán para lograr esta visión.

Objetivos: son actividades específicas diseñadas para cumplir con las metas reales, alcanzables y asequibles. Se puede decir que un objetivo es el resultado que debe alcanzarse al final de cada operación. Así, es importante tener en cuenta la misión, la visión y la meta de ser de la empresa, para llevar a cabo un estudio sobre la base de estos para identificar el conjunto de las políticas de seguridad para garantizar la seguridad de la información, confidencialidad y disponibilidad.

Principios fundamentales de las políticas de seguridad

Son las ideas principales de las que se han diseñado políticas de seguridad.

Los principios fundamentales son: la responsabilidad individual, la autorización, privilegios mínimos, separación de obligaciones, la auditoría y la redundancia.

Auditoría

Todas las actividades, los resultados, las personas que participan en ellos y los recursos necesarios, deben ser controlados desde el principio hay que hacer después del proceso.

También es importante considerar que una auditoría informática busca verificar que las actividades realizadas y las herramientas instaladas y la configuración del esquema de seguridad coherente a cabo y si es conveniente para la seguridad requerida por la empresa.

Políticas para la confidencialidad

Desde el primer capítulo de esta investigación, se mencionó la necesidad de mantener el control sobre quién puede acceder a la información (documentos, ya sea por escrito o electrónico) no siempre quiere que la información a disposición de cualquier persona que quiera obtener.

Por lo tanto, hay políticas de confidencialidad, responsables de establecer la relación entre la clasificación del documento y la posición (nivel jerárquico dentro de la organización) requiere una persona para acceder a dicha información.

Políticas para la integridad

La política de integridad está orientado principalmente a preservar la integridad antes de la confidencialidad, esto ha sido sobre todo porque en muchas aplicaciones comerciales en el mundo real es más importante para mantener la integridad de los datos, ya que se utilizan para implementar actividades automatizadas, incluso mientras que en otros entornos que no es, como en las áreas de gobierno o militares.

Publicación y difusión de las políticas de seguridad

Como todos los documentos creados por una organización, debe decidir correctamente qué grupos se dirigen hacia las políticas de seguridad, por lo que significa que van a dar a conocer, si quiere que otros grupos puedan conocer.

El principal objetivo de la publicación y difusión es que el público objetivo entiende lo que son las políticas y crear conciencia acerca de su importancia a través de charlas y talleres para este propósito.

Procedimientos y planes de contingencia

Sólo cuando una organización se da cuenta de la importancia de la seguridad de su información, incluyendo sus recursos tecnológicos, es cuando se empieza a diseñar y establecer las medidas de seguridad que tienen como objetivo protegerlo de diversas situaciones perjudiciales.

Aunque la prevención de estos desastres es vital, no puede descuidar la eventualidad casi inevitable que suceda, sino que también tiene que formular y establecer un conjunto de procedimientos para hacer frente a los problemas y luego restablecer el funcionamiento normal de la zona afectada.

Procedimientos preventivos

Cubre todos los procedimientos antes que se materializa una amenaza, su propósito es evitar la materialización.

Los procedimientos preventivos pueden variar según el tipo de actividades de la organización, los recursos que tienen a su disposición, que es lo que desea proteger, que trabaja en las instalaciones y el uso de la tecnología.

Las actividades que se realizan en este punto son las siguientes:

- Copia de seguridad de bases de datos y otros documentos de información necesaria para la organización.

- La instalación de dispositivos de seguridad tales como cerraduras, alarmas, puertas electrónicas, cámaras de seguridad, protección de software para equipos de computación, entre otros.
- Inspeccionar y mantener un registro constante del rendimiento y el estado de los recursos informáticos, la infraestructura y las condiciones de construcción.
- Establecer servicios de seguridad, tales como líneas directas, extintores de incendios, construcción de carreteras de emergencia (entrada y salida), plantas de energía de emergencia, etc.
- Establecer un centro de servicio alternativo que cuenta con los recursos necesarios para continuar con las operaciones de la organización hasta el momento en que el centro de trabajo normal puede ser utilizado en condiciones normales.
- La capacitación del personal en el uso adecuado de la tecnología de la información en su adecuada ejecución de sus tareas y la implementación de los procedimientos de emergencia.

Procedimientos correctivos

Procedimientos de acciones correctivas están dirigidas a contrarrestar en lo posible los daños causados por un desastre, ataque u otra situación desfavorable y restablecer el funcionamiento normal de la operación del centro afectado.

Como procedimientos preventivos pueden variar en función de los recursos disponibles, sino que también varía en función de los daños para contrarrestar las emergencias porque no todos requieren el uso de todos los procedimientos de corrección definidos por la organización.

Planes de contingencia

El plan de contingencia es la herramienta de gestión para el manejo de Tecnologías de la Información y las Comunicaciones TIC.

Este plan contiene las medidas técnicas, humanos y organizativos para garantizar la continuidad de las operaciones de una institución en caso de desastres y catástrofes como incendios, terremotos, inundaciones, etc., pero también contiene medidas para hacer frente a los daños causados por el robo, sabotaje e incluso los ataques terroristas.

El plan de contingencia es un requisito previo para un requisito rápida y eficaz respuesta de emergencia. Sin una planificación de contingencia antes te vas a perder mucho tiempo en los primeros días de una emergencia.

Objetivos y características de un plan de contingencias

Los principales puntos que deben cumplir con un plan de contingencia son:

- Reducir el riesgo de un desastre.
- Establecer los procedimientos necesarios para enfrentar y hacer frente a los acontecimientos negativos que se producen.
- Aminorar los efectos negativos de un desastre, una vez ocurrido.
- Asegurar la continuidad de las operaciones de la organización.
- Restablecer el funcionamiento normal de las zonas afectadas por el desastre.
- Dar a conocer el personal del plan de contingencia involucrados.

Para lograr estos objetivos, es necesario diseñar e implementar un conjunto de procedimientos adaptados a las necesidades y los recursos disponibles para permitir una respuesta oportuna y precisa todos los acontecimientos negativos que la organización enfrenta.

Estos procedimientos deben basarse en los resultados de un análisis preliminar de riesgos y el establecimiento de prioridades.

Fases del plan de contingencia

Un plan de contingencia se divide en fases, lo que facilita el monitoreo del desempeño del plan, así como el apoyo para la detección y la implementación de mejoras, ya que cada fase se centra en una serie de aspectos específicos y posibles cambios se aplicarán a partir de la fase apropiada sin cambiando a lo largo de todo el plan.

Las fases se pueden dividir en análisis y diseño, desarrollo, pruebas y mantenimiento.

Análisis y diseño: **e**n esta fase las funciones de la organización pueden considerarse como crítica y se les da un orden jerárquico de prioridad según se identifican.

Se define y las amenazas a que están expuestos las funciones críticas y el impacto de un desastre en las funciones al materializarse y si se documentan los análisis.

Los niveles mínimos aceptables de servicio para cada problema planteado también se definen.

Las posibles soluciones se identifican y evalúan una relación de costo / beneficio para cada propuesta alternativa

Desarrollo de un plan de contingencias: en esta fase la documentación plan, el contenido mínimo se creará:

- Objetivo del plan.
- Modo de ejecución.
- Tiempo de duración.
- Costes estimados.
- Recursos necesarios.
- Evento a partir del cual se pondrá en marcha el plan.
- Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.

Es necesario que el plan sea revisado por los responsables de las áreas involucradas. Del mismo modo hay que tener en cuenta las posibles consecuencias legales que puedan derivarse de las actividades contempladas en el mismo.

Pruebas y mantenimiento: se base en realizar las pruebas pertinentes para tratar de evaluar el impacto real de un posible problema en los escenarios establecidos en la etapa de diseño. Las pruebas no deben tratar de comprobar si un plan funciona, y no deben centrarse en los problemas y la búsqueda de fallas en el plan con el fin de corregirlos. Es necesario documentar cada una de las pruebas realizadas para su respectiva aprobación de las partes implicadas.

En la fase de mantenimiento se corrigen los errores que se hayan encontrado durante las pruebas, pero también se revisan todos los elementos estén preparados para poner en acción el plan de contingencia con sus óptimas funciones, para su uso en cualquier momento para contrarrestar un desastre. De lo contrario, deben ser reparados o reemplazados.

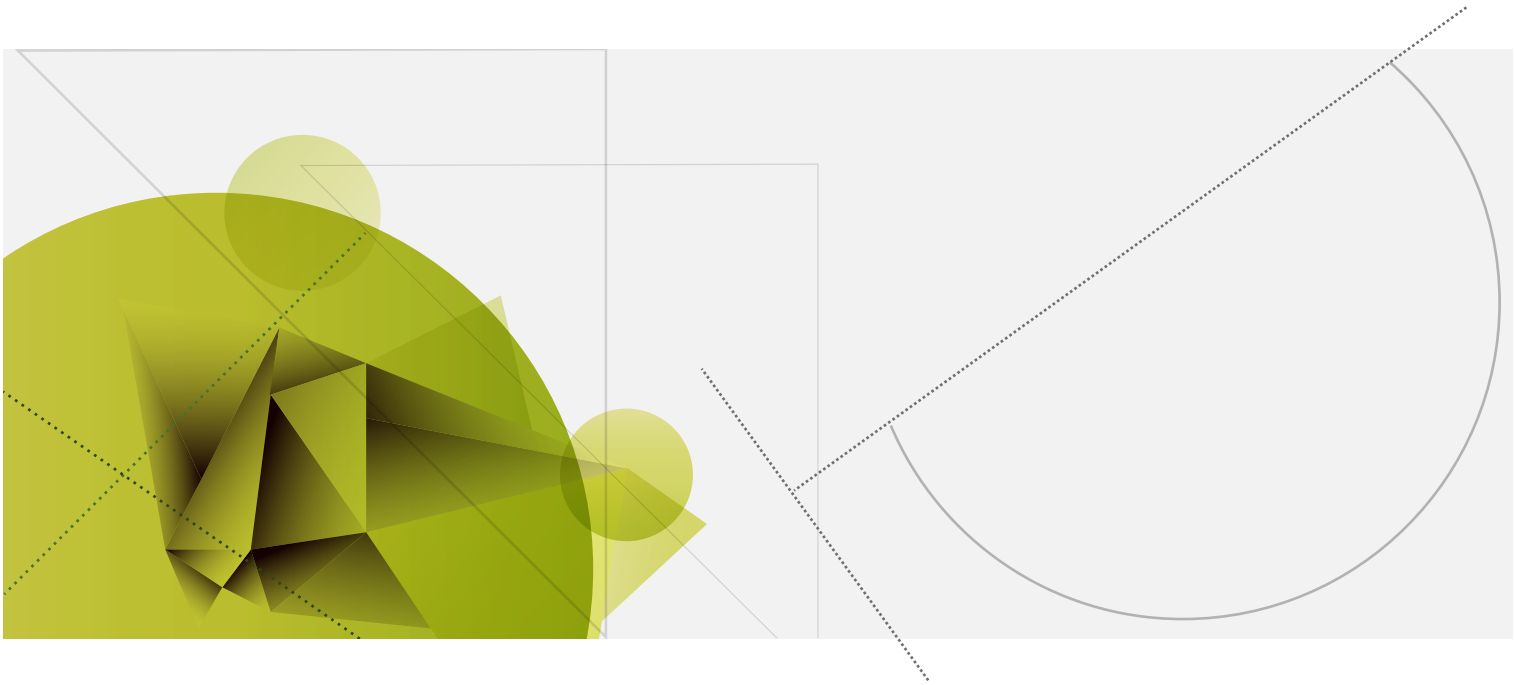
Algunas de las actividades realizadas en esta fase son:

- Verificar la disponibilidad de los colaboradores incluidos en la lista del plan de contingencia.
- Verificar los procedimientos que se emplearan para almacenar y recuperar los datos (backup).
- Comprobar el correcto funcionamiento del disco extraíble, y del software encargado de realizar dicho backup.
- Realizar simulacros, capacitando al personal en el uso de los procedimientos indicados en el plan de contingencia para la medición de su efectividad.

Bibliografia

- Aureliomavisoy. (2015). Historia de la seguridad informática.
- López, A. (2010). Seguridad informática. España: Editex S.A.
- Matamala, M. (2012), Fundamentos de seguridad.
- Muñoz, A. & Ramió, J. (2006). Cifrado de las comunicaciones digitales de la cifra clásica al algoritmo RSA.
- Santana, C. (2012). Seguridad informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?

Esta obra se terminó de editar en el mes de noviembre
Tipografá Myriad Pro 12 puntos
Bogotá D.C,-Colombia.



AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO