“Evaluación de Riesgos”

UNIDAD III

PROFESOR: Sergio Ávila M.

MATERIA:

ADMINISTRACION. Y

SEGURIDAD DE REDES

11-10-2015

INSTITUTO TECNOLOGICO

"Compromiso a la innovación de la cultura"

"INSTITUTO TECNOLOGICO DE GUSTAVO A. MADERO"

PROFESOR: SERGIO AVILA M.

MATERIA: ADMINISTRACION Y SEGURIDAD DE REDES

INTEGRANTES:*Aguilar López Cristian David

*Galván León Víctor Manuel

*Guevara Moreno Raymundo

*Rodríguez Huerta Rubén

*Suarez Hernández Cecilia

CARRERA: TICS

UNIDAD III: EVALUACION DE RIESGOS

LUNES 12 DE OCTUBRE DEL 2015

Introducción:

En esta unidad veremos lo que es una Evaluación de Riesgos se mencionara que un riesgo ya esta evaluación nos permita saber cuáles son las principales vulnerabilidades de los activos de información y cuáles son las amenazas.

En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

Una amenaza en una Organización puede afectar la información y estás amenazas están relacionadas con el recurso humano, eventos naturales o fallas técnicas.

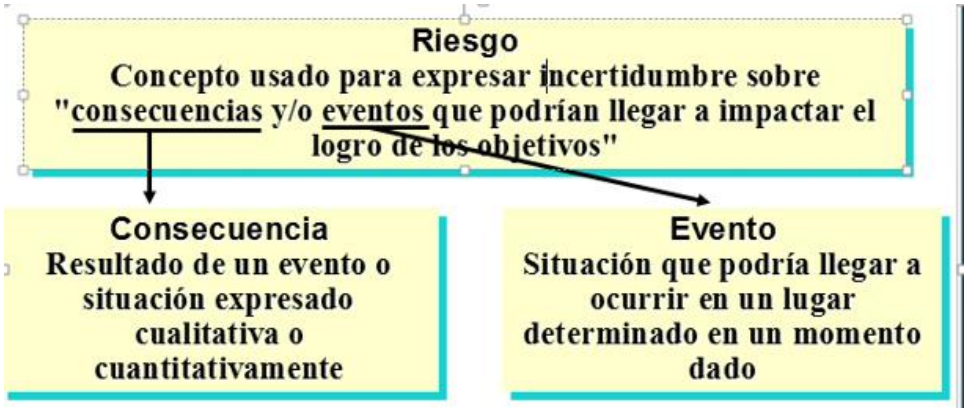
Algunos ejemplos pueden ser ataques informáticos externos, errores u omisiones del personal de la empresa, infecciones con malware, terremotos, tormentas eléctricas o sobrecargas en el fluido eléctrico.

Ahora, para que la empresa pueda tomar decisiones sobre cómo actuar ante los diferentes riesgos es necesario hacer una valoración para determinar cuáles son los más críticos para la empresa.

Es por eso la Importancia de La Evaluación de Riesgos para saber cómo mitigarla además de tener en cuenta el por qué están ocurriendo.

“3.4.Evaluación de Riesgos”

¿Qué es un Riesgo?



¿Qué es la Evaluación de Riesgos?

El análisis de riesgo también conocido como evaluación de riesgo es el estudio de las causas de las posibles amenazas, los daños y consecuencias que éstas puedan producir.

Evaluar riesgos es un proceso por el cual una organización identifica amenazas, evalúa el nivel de riesgo asociado con esas amenazas, y determina formas de evitar altos riesgos (high-risks hazards).

Una evaluación de riesgos debería ser llevada a cabo antes de que las políticas para el manejo de riesgos sean creadas, y antes de que un proyecto comience. Al evolucionar la naturaleza del trabajo de una organización, y al cambiar la situación política en la que actúan, las organizaciones deben re-evaluar riesgos, adoptar estrategias de atenuación y tomar medidas adecuadas.

Evaluar riesgos le permite a una organización asegurar que su personal este consciente de los riesgos, así como de las estrategias para prevenirlos o evitarlos. Las políticas para el manejo de riesgos también definen los roles y responsabilidades de la organización y de los individuos que componen el personal al responder a peligros reales y potenciales. También es importante que las organizaciones desarrollen estrategias para proteger a individuos vulnerables que se contacten buscando información o asesoramiento.

RIESGO → CONTROL → PRUEBA

Riesgo: Algo que puede o no suceder.

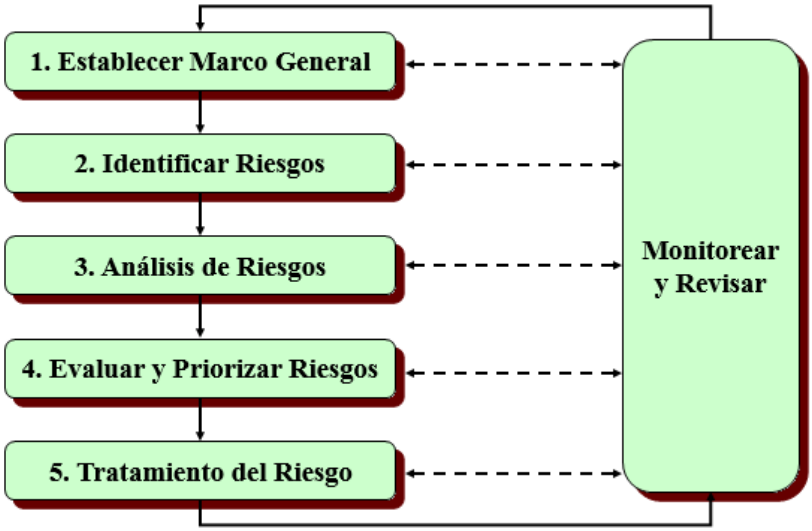
Control: Planteamiento de la solucion (idea).

Prueba: Ejecucion,aplicación.

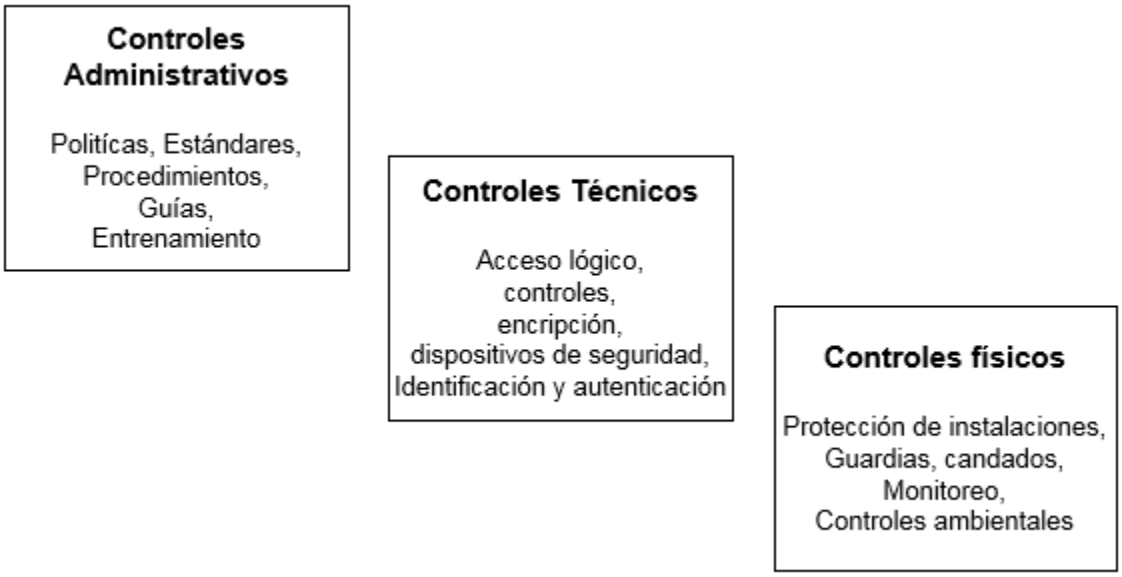
ISO/IEC 27001

• Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)

“Procesos de Evaluación de Riesgos”



“Controles en Seguridad”



“Técnicas para asegurar el sistema”

*Utilizar técnicas de desarrollo que cumplan con los criterios de seguridad al uso para todo el software

*Codificar la información: criptografía

*Contraseñas difíciles de averiguar

*Vigilancia de red

*Copias de seguridad

*Restringir el acceso

“3.4.1.Activos a Proteger”

Activos

Es todo aquello con valor para una organización y que necesita protección, en el ámbito informático pueden ser datos, infraestructura, hardware, software, personal, información, servicios.

Riesgo

Un riesgo es la posibilidad de que se presente algún daño o pérdida, esto es, la posibilidad de que se materialice una amenaza.

Aceptación del riesgo

Es la decisión de recibir, reconocer, tolerar o admitir un riesgo. Esta decisión se toma una vez que se han estudiado los diferentes escenarios posibles para una misma amenaza y se han aplicado todos los procedimientos posibles para contrarrestar sus efectos y probabilidad de que ocurra.

Análisis del riesgo

Uso sistemático de la información disponible para identificar las fuentes y para estimar la frecuencia de que determinados eventos no deseados pueden ocurrir y la magnitud de sus consecuencias.

Manejo del riesgo

Proceso de identificación, control y minimización o eliminación de riesgos de seguridad que pueden afectar a los sistemas de información, por un costo aceptable.

Amenaza

Una acción o situación potencial que tiene la posibilidad de causar daño.

Análisis cuantitativo

El análisis cuantitativo es una técnica de análisis que busca entender el comportamiento de las cosas por medio de modelos estadísticos y técnicas matemáticas para ello se encarga de asignar un valor numérico a las variables, e intenta replicar la realidad matemáticamente.

Análisis cualitativo

Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en términos subjetivos (Impacto Muy Alto, Alto, Medio, Bajo o Muy Bajo)

“3.4.2.Amenazas con las que se tiene que Proteger”

¿Qué es una amenaza informática?

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Las amenazas pueden ser causadas por:

***Usuarios:** causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobre dimensionados, no se les han restringido acciones innecesarias, etc.

***Programas maliciosos**: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica, un programa espía o spyware, en general conocidos como malware.

***Errores de programación:** La mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados como exploits por los crackers, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.

***Personal técnico interno:** técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.

***Fallos** electrónicos o lógicos de los sistemas informáticos en general.

***Catástrofes naturales**: rayos, terremotos, inundaciones, rayos cósmicos, etc.

Tipos de Amenazas

Amenazas por el origen: El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella y con esto, se puede hacer robo de información o alterar el funcionamiento de la red.

a) **Amenazas internas:** Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.
b) **Amenazas externas**: Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.
c) **Amenazas por el efecto:**

*Robo de información.
*Destrucción de información.
*Anulación del funcionamiento de los *sistemas o efectos que tiendan a ello.
*Suplantación de la identidad, publicidad *de datos personales o confidenciales, *cambio de información, venta de datos *personales, etc.
*Robo de dinero, estafas,...
*Amenazas por el medio utilizado

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

*Phishing.

*Ingeniería social.

*Caballo de Troya

*Denegación de servicio.

“3.4.3.Proteccion Legal”

La Seguridad Informática es uno de los elementos técnico-jurídico más vinculados a la era de la Información y por ende constituye una de las piedras angulares de toda realización informática que vaya a tener una incidencia social. Las disposiciones de Seguridad Informática son las que permiten contar con sistemas automatizados que cuenten con los requisitos de confidencialidad, integralidad y disponibilidad de la información digitalizada.

Por eso un régimen jurídico de Seguridad Informática debe contener las normas que establezcan.

-Las garantías para la confidencialidad.

-Disponibilidad e integridad de los sistemas informáticos.

- La información digitalizada tanto la que se guarda en soportes de almacenamiento y como la que circula por las redes.

-Programas, Datos e Información.

-Servicios de procesamientos de datos.

-Equipos e instalaciones de procesamiento electrónico de datos e información.

-Las principales debilidades y amenazas de los sistemas informáticos.

Por otra parte consideramos que la Seguridad Informática debe ser reconocida legalmente como medio de prevención de delitos en el entorno informático, por tal razón es necesario establecer las normas que rigen para el registro contable de los medios y recursos informáticos a proteger o medidas de seguridad informática, así como aquellas disposiciones que permitan delimitar el valor patrimonial de los activos protegidos.

No debe faltar en esta previsión legislativa las normas que fijen las medidas de Seguridad Informática que rigen para diversos ámbitos de aplicación:

*Administrativo y de organización

*Personal.

*Entorno físico.

*Sistemas electrónicos utilizados en telecomunicaciones.

*Equipos y programas de computación.

Especial relevancia tienen las normas para el reconocimiento y otorgamiento de las licencias de Seguridad y las Certificaciones de Seguridad Informática, ya que las certificaciones efectuadas hoy en día por las entidades autorizadas, si bien disponen de autorización para la actividad, la validez del documento electrónico, que se emiten, no dispone aún de un sistema integral de reconocimiento legal a diversas instancias, no solo judicial.

1) Violación de correspondencia electrónica:

a) el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido

b) El que se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; Aspectos Legales de la Seguridad Informática.

3) indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

4) Igual pena en caso interceptar o captar o captar comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. Aspectos Legales de la Seguridad Informática.

2) ACCESO ILEGÍTIMO A UN SISTEMA O DATO INFORMÁTICO

Será reprimido el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

(Art.153: 15 días a 6 meses).

Conclusión Cecilia:

Como vimos para que nuestra inofrmacion este confible,disponible e integra es necesario hacer una Evaluacion de Riesgos,como se menciono evaluación de riesgo identifica situaciones que podrían tener un impacto negativo en los procesos e intenta cuantificar su gravedad y probabilidad.

Ya que se tiene identificados los riesgos se tienen que mitigar asi mismo poner en practica medidas preventivas para que ese riesgo ocurra con menor frecuencia.

Como se menciono la Seguridad Informática debe ser reconocida legalmente como medio de prevención de delitos en el entorno informático.

Este tema nos servirá para un mejor funcionamiento de nuestra Organización.

Conclusión Víctor Manuel:

La Seguridad Informática es un aspecto muchas veces descuidado en nuestros sistemas, pero de vital importancia para el correcto funcionamiento de todos ellos.

Sería importante y muy relevante hacer hincapié en los siguientes conceptos:
Todo sistema es susceptible de ser atacado, por lo que conviene prevenir esos ataques.
Conocer las técnicas de ataque ayuda a defenderse más eficientemente.
De todas formas, como en la mayoría de los ámbitos de la seguridad, lo esencial sigue siendo la capacitación de los usuarios. Una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos de la mejor manera posible para evitar ataques o accidentes.
En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

Conclusión Cristian David:

En este tema de la Seguridad Informática pudimos observar que se tiene que cumplir ciertos módulos para poder sacar adelante el riesgo o amenaza que tenemos.

Se vio que hay ciertas técnicas para evitar riesgos informáticos con usuarios, así como también hay distintas amenazas informáticas con cierto objetivo.

Que son de suma importancia las Políticas de Seguridad para que nuestra Organización pueda tener menos amenazas.

Conclusión Rubén:

Existen diferentes tipos de ataques en Internet como virus, troyanos, dichos ataques pueden ser contrarrestados o eliminados pero hay un tipo de ataque, que no afecta directamente a los ordenadores, sino a sus usuarios, conocidos como “el eslabón más débil”. Dicho ataque es capaz de almacenar conseguir resultados similares a un ataque a través de la red, saltándose toda la infraestructura creada para combatir programas maliciosos. Además, es un ataque más eficiente, debido a que es más complejo de calcular y prever. Se pueden utilizar infinidad de influencias psicológicas para lograr que los ataques a un servidor sean lo más sencillo posible, ya que el usuario estaría inconscientemente dando autorización para que dicha inducción se vea finiquitada hasta el punto de accesos de administrador.

Conclusión Raymundo:

Es importante en toda organización contar con herramientas, que garanticen la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y que por medio de procedimientos de control se puede evaluar el desempeño del entorno informático la cual describe las políticas y medidas tomadas para su realización. Idealmente los objetivos y las políticas de administración de riesgos deben ser producto de las decisiones de los departamentos de seguridad informática en conjunto con el área jurídica de toda organización.

Bibliografía:

https://www.ifex.org/campaigns/risk_assessment/es/

http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap5.html