OVI PARA DISEÑAR UN OBJETO VIRTUAL DE INFORMACIÓN – OVI

Objetivo General

Realizar un OVI relacionado el tema de Seguridad Informática" con el fin de implementar una página web en su primera etapa que es la "Fase de Diseño".

Sección de texto	Sección de imágenes
SEGURIDAD INFORMATICA Definimos la seguridad de información como la protección de ventajas de información de la revelación no autorizada, de la modificación, o de la destrucción, o accidental o intencional, o la incapacidad para procesar es a información. La seguridad de la red, se compone de esas medidas toma das para proteger una red del acceso no autorizado, interferencia accidental o intencionada con operaciones normales, o con la destrucción, inclusive la protección de facilidades físicas, del software, y de la seguridad del personal.	Video: https://www.youtube.com/watch?v=lskwU3kw29o

Sección de texto	Sección de imágenes
¿Por qué requiere atención especial la seguridad en el Web? •Internet es una red de dos sentidos. Así como hace posible que los servidores Web divulguen información a millones de usuarios, permite a los hackers, crackers, criminales y otros "chicos malos" irrumpir en las mismas computadoras donde se ejecutan los servidores Web. •Las empresas, instituciones y los gobiernos utilizan cada vez más el Word Wide Web para distribuir información importante y realizar transacciones comerciales. Al violar servidores Web se pueden dañar reputaciones y perder dinero. •Aunque el Web es fácil de utilizar, los servidores son piezas de software extremadamente complicadas y tienen diversas fallas de seguridad potenciales. •Es mucho más onerosa y tardada la recuperación de un incidente de seguridad que implementar medidas preventivas.	http://www.dragonjar.org/wp-content/uploads/2011/02/SeguridadWeb.jpg  https://inusual.com/wp-content/uploads/2014/05/shutterstock_165303932.jpg  https://www.frogx3.com/wp-

¿Por qué preocuparse sobre la seguridad en el Web?

Los servidores son un blanco atractivo para los trasgresores por varias razones:

Publicidad. Los servidores web son la cara que las organizaciones presentan al público y al mundo electrónico. Un ataque exitoso a alguno de ellos es acto público que puede ser visto en unas horas por cientos de miles de personas.

Comercio. Muchos servidores web están relacionados con el comercio y el dinero. De esta forma, los servidores web se han convertido en repositorios de información financiera confidencial, lo cual los convierte en un blanco atractivo para los atacantes.

Información confidencial. Para las organizaciones, la tecnología del Web se ha convertido en una forma de distribuir información con gran sencillez, tanto internamente, a sus propios miembros, como de manera externa, a sus socios en todo el mundo. Esta información confidencial es un blanco atractivo para sus competidores y enemigos.

Acceso a las redes. Al ser utilizados por personas tanto dentro como fuera de las organizaciones, los servidores web sirven efectivamente como puente entre la red interna de la organización y las redes externas. Su posición privilegiada en cuanto a las conexiones de red los convierte en un blanco ideal para ser atacados, ya que un servidor web violado puede emplearse como base para atacar desde ahí a las computadoras de una organización.

Extensibilidad de los servidores. Debido a su naturaleza, los servidores estan diseñados para ser extensibles, lo cual hace posible conectarlos con bases de datos, sistemas heredados y otros programas que se ejecutan en la red de una organización.

content/uploads/2015/03/seguridad-internet-shutterstock-1.jpg

https://diarioti.com/wp-content/uploads/2016/11/shutterstock_193331816_wk1003mike-https.jpg

Interrupción del servicio. Como la tecnología del Web se basa en la familia de protocolos TCP/IP, está sujeta a interrupciones del servicio: ya sea accidental o intencionalmente por medio de ataques de negación del servicio. Las personas que utilizan dicha tecnologías en estar enteradas de sus fallas y prepararse para interrupciones importantes del servicio. **Soporte complicado**. Los navegadores necesitan servicios internos, como DNS (Servicio de nombres de Dominio, Domain Name Service) y el enrutamiento del protocolo IP (Protocolo Interne, Internet Protocol) para funcionar bien. La robustez y confiabilidad de tales servicios pueden ser desconocidas y vulnerables a errores de programación, accidentes y subversión, la subversión de un servicio de más bajo nivel puede causar problemas también a los navegadores.	

Sección de texto	Sección de imágenes
Objetivos de la Seguridad. Seguridad informática es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de una entidad. **Integridad**. Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizas o accidentales, como información de censo o sistemas de transacciones financieras.	http://www.danysoft.com/wp-content/uploads/2014/06/1501-seguridad-sistemas-web-1030x1030.jpg

Disponibilidad. Se refiere a la continuidad operativa de la entidad, la pérdida de disponibilidad puede implicar, la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.

Confidencialidad. Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede resultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada Estos aspectos además de lidiar con el riesgo que representan los atacantes remotos, se ven amenazados también por los riesgos por desastres naturales, empleados desleales, virus y sabotaje, entre otros.

Metodología para la definición de una estrategia de seguridad

La figura explica una metodología para definir una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales, y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque.

Metodología de estrategias de seguridad [Miguel, 1998]

Predecir posibles ataques y analizar riesgos.

La primera fase de la metodología esquematizada en la figura, es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques que reparar el daño que han causado.

Para cada tipo de amenaza

Considere todas las amenazas posibles que causan ataques en los sistemas. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales.

Para cada tipo de método de ataque

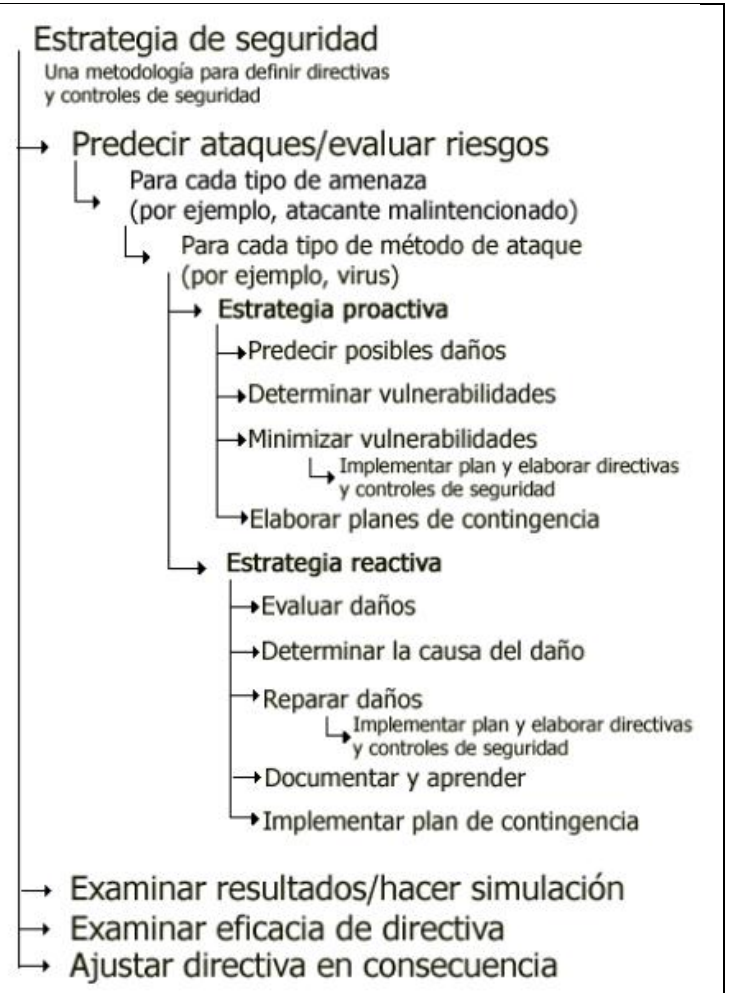
Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles.

Estrategia proactiva.

La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables.

Determinar el daño posible que puede causar un ataque.

Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, utilice un entorno de prueba o de laboratorio



para clarificar los daños que provocan los diferentes tipos de ataques. **Determinar los puntos vulnerables o las debilidades que pueden explotar los ataques** Si se pueden descubrir los puntos vulnerables que explota un ataque específico, se pueden modificar las directivas y los controles de seguridad actuales o implementar otras nuevas para reducir estos puntos vulnerables. **Reducir los puntos vulnerables y debilidades que puede explotar un posible ataque**. La reducción de los puntos vulnerables y las debilidades del sistema de seguridad que se determinaron en la evaluación anterior es el primer paso para desarrollar directivas y controles de seguridad eficaces. **Elaborar planes de contingencia.** Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. **Estrategia reactiva.** La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. **Evaluar el daño.** Determine el daño causado durante el ataque. Esto debe hacerse lo antes	

posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que puedan proseguir las operaciones comerciales y la productividad normales. **Determinar la causa del daño.** Para determinar la causa del daño, es necesario saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Revise los registros del sistema, los registros de auditoría y las pistas de auditoría. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados. **Reparar el daño.** Es muy importante que el daño se repare lo antes posible para restaurar las operaciones comerciales normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización (que se tratan en el documento acerca del diseño de la seguridad) deben cubrir la estrategia de restauración. **Documentar y aprender.** Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño	

Implementar un plan de contingencia. Si ya existe algún plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones comerciales. Si no hay ningún plan de contingencia, desarrolle un plan apropiado basado de la documentación del paso anterior. **Revisar el resultado y hacer simulaciones.** Tras el ataque o tras defenderse de él, revise su resultado con respecto al sistema. La revisión debe incluir la pérdida de productividad, la pérdida de datos o de hardware, y el tiempo que se tarda en recuperarlos. **Revisar la eficacia de las directivas.** Si hay directivas para defenderse de un ataque que se ha producido, hay que revisar y comprobar su eficacia. Si no hay directivas, se deben redactar para aminorar o impedir ataques futuros. **Ajustar las directivas en consecuencia.** Si la eficacia de la directiva no llega al estándar, hay que ajustarla en consecuencia. Las actualizaciones de las directivas debe realizarlas el personal directivo relevante, los responsables de seguridad, los administradores y el equipo de respuesta a incidentes.	

TOMADO DE http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf