

Universidad Nacional Abierta y a Distancia - UNAD - Vicerrectoría Académica y de Investigación - VIACI

Escuela: Ciencias Básicas Tecnología e Ingeniería

Programa: Ingeniería de Sistemas

Curso: Diseños de Sitios Web

Código: 301122

ACTIVIDAD FASE DE PLANEACION Y ANALISIS
CURSO DISEÑOS DE SITIOS WEB - COD. 301122

FORMATO GUION SITIO WEB DEL OVI

204039 Seguridad Informática

Diseñado Por: Duvan Alejandro Navas

A continuación se presenta el formato de Guion para el desarrollo de la actividad de la Fase de Planeación y Análisis, revise muy bien las instrucciones para que realice un correcto diligenciamiento del mismo.

Éxitos!!!

1. Objetivos del OVI (describa mediante el registro de 1 objetivo general y tres

Objetivo general:

Se diseña para los usuarios puedan conocer los conceptos básicos de seguridad informática.

Objetivo específico 1:

Que estándares se utilizan en la seguridad informática según esos conceptos básicos

Objetivo específico 2:

Normas que se emplean en la seguridad de redes

Objetivo específico 3:

Que impacto tiene en la red la seguridad informática sobre su uso

específicos para que se construye este OVI

2. Contenido informativo del OVI por secciones (Replique el siguiente cuadro de acuerdo al número de secciones que vaya a crear en el OVI)

Nombre de la sección que se creara en el OVI: descripción de cada concepto de seguridad informática

2.1 Objetivo de la sección: (Registre a continuación el objetivo que tiene esta sección)

Que el usuario conozca la descripción de cada concepto de seguridad informática para que las pueda emplear.

2.2 Recursos de consulta que usara en la sección: (coloque el nombre del material que usara para crear los contenidos de la sección y el enlace de descarga de los mismos sean estos Texto, Imágenes, Audios o Vídeos)

Texto: Verdana, 12 puntos

Imagen: tamaño 77kb, archivo jpg, tamaño 11kb, archivo jpg

2.3 Redacte un borrador del contenido de lectura en formato de texto que tendrá la sección: (Sea este la presentación de la sección, el contenido o ambos; redacte un borrador del texto que publicara como contenido en la sección coloque un subtítulo para identificar si corresponde a la presentación de la sección o el contenido de lectura de la sección)

Conceptos de seguridad informática

Cada ataque cibernético tiene su nombre y las familias de códigos maliciosos son numerosas. Entonces, dar un paso más en la materia, implica profundizar en algunos conceptos nuevos para los usuarios comunes.

Botnet. Es una red de equipos infectados por códigos maliciosos, controlados por un atacante. Cada sistema infectado (zombi) interpreta y ejecuta las órdenes emitidas. Los botnets suelen utilizarse para el envío de spam, el alojamiento de material ilegal o la realización de ataques de denegación de servicio distribuido (DDoS).

Exploit. Fragmento de código que permite a un atacante aprovechar una falla en el sistema (una vulnerabilidad crítica) para ganar control sobre él. Una vez que esto ocurre, es posible robar información o instalar otros códigos maliciosos.

Jackware. Es un tipo de código malicioso que intenta tomar el control de un dispositivo cuyo objetivo principal no es el procesamiento de datos ni la comunicación digital. Por ejemplo, un auto. El jackware es como una forma especializada de ransomware. Lo bueno es que se encuentra en su etapa teórica, aún no está libre.

Keylogger. Es un tipo de malware que registra las teclas pulsadas en un sistema para almacenarlas en un archivo o enviarlas a través de internet. Suele guardar contraseñas, números de tarjeta de crédito u otros datos sensibles. Hay versiones más complejas capaces de realizar capturas de pantalla cuando se registra un clic, haciendo que estrategias de seguridad como el uso del teclado virtual sean obsoletas.

Sednit. Es una banda cibercriminal que, al menos desde 2004, ha desarrollado ataques sofisticados capaces de evadir las medidas de

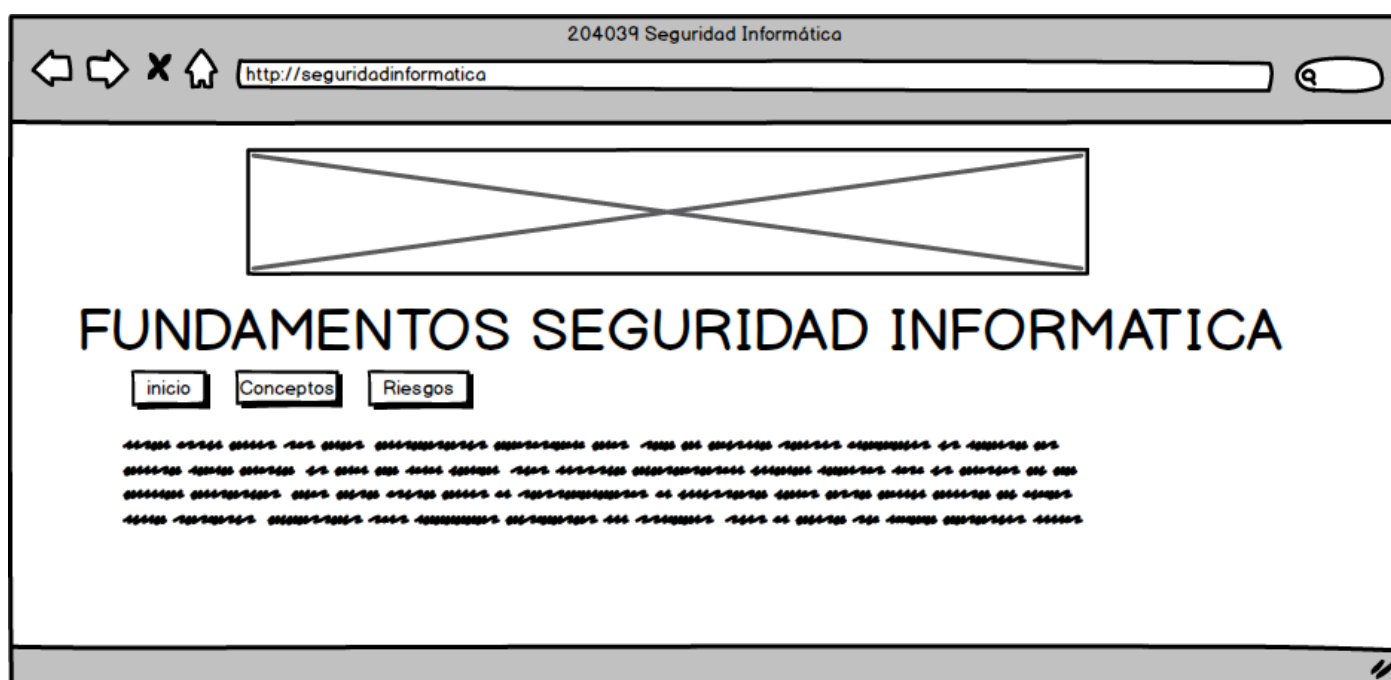
seguridad típicas de las redes corporativas. También es conocida como APT28, Fancy Bear, Pawn Storm o Sofacy. Según una investigación de ESET, algunos objetivos descubiertos en Latinoamérica son las embajadas pertenecientes a Brasil, Colombia y los Ministerios de Defensa en Argentina.

Ataque DDoS. La sigla significa Distributed Denial of Service y la mejor forma de entender de qué se trata es analizando la definición en términos. Una denegación de servicio implica que un determinado servicio (web u otro) quede completamente fuera de disponibilidad para sus usuarios. El ataque de Denegación de Servicio busca, mediante diversas técnicas, lograr eso: dejar un servicio imposible de utilizar. Este ataque puede ser realizado por más de un equipo atacante a la vez, y es ahí cuando la Denegación de Servicio pasa a ser Distribuida, simplemente porque las técnicas de ataque se llevan a cabo desde lugares geográficamente diferentes. En el caso de un servicio web, el ataque DDoS más frecuente es que múltiples equipos soliciten recursos a ese sitio continuamente, de manera que el servidor que está detrás, no dé abasto con las peticiones y sufra un colapso.

Cracker. Es algo así como un hacker con malas intenciones. El cracker utiliza sus conocimientos en seguridad informática con fines negativos, de un modo u otro perjudica a un tercero. Hay hackers que utilizan sus conocimientos para defender y otros, como los crackers, lo hacen para atacar en beneficio propio (generalmente económico).

Nombre de la sección que se creara en el OVI: Impacto en la red al no tener un buen mecanismo de seguridad
2.1 Objetivo de la sección: (Registre a continuación el objetivo que tiene esta sección)
El usuario analice cual es el impacto en la red que causa no tener un buen mecanismo de seguridad.
2.2 Recursos de consulta que usara en la sección: (coloque el nombre del material que usara para crear los contenidos de la sección y el enlace de descarga de los mismos sean estos Texto, Imágenes, Audios o Vídeos)
Texto: verdana, 12 puntos Imagen: tamaño Video: Duracion 2:19 link https://www.youtube.com/watch?v=T41zBYg3M_s , tamaño 12,2 MB
2.3 Redacte un borrador del contenido de lectura en formato de texto que tendrá la sección: (Sea este la presentación de la sección, el contenido o ambos; redacte un borrador del texto que publicara como contenido en la sección coloque un subtítulo para identificar si corresponde a la presentación de la sección o el contenido de lectura de la sección)

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.



204039 Seguridad Informática

[←](#)
[→](#)
[X](#)
[↑](#)

FUNDAMENTOS SEGURIDAD INFORMATICA

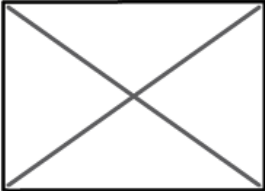
inicio

conceptos

Riesgos

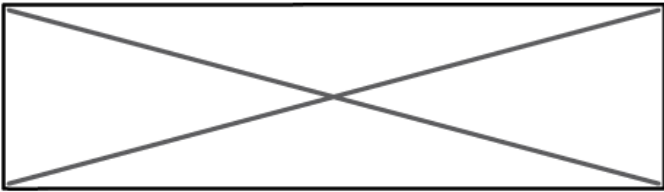
Conceptos de seguridad informatica

La seguridad informática es el conjunto de medidas y acciones que se toman para proteger la información y los recursos de un sistema informático contra amenazas y riesgos. Estas medidas pueden ser técnicas, organizativas o humanas, y su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información.



La seguridad informática es el conjunto de medidas y acciones que se toman para proteger la información y los recursos de un sistema informático contra amenazas y riesgos. Estas medidas pueden ser técnicas, organizativas o humanas, y su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información.

La seguridad informática es el conjunto de medidas y acciones que se toman para proteger la información y los recursos de un sistema informático contra amenazas y riesgos. Estas medidas pueden ser técnicas, organizativas o humanas, y su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información.



La seguridad informática es el conjunto de medidas y acciones que se toman para proteger la información y los recursos de un sistema informático contra amenazas y riesgos. Estas medidas pueden ser técnicas, organizativas o humanas, y su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información.

La seguridad informática es el conjunto de medidas y acciones que se toman para proteger la información y los recursos de un sistema informático contra amenazas y riesgos. Estas medidas pueden ser técnicas, organizativas o humanas, y su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información.

La seguridad informática es el conjunto de medidas y acciones que se toman para proteger la información y los recursos de un sistema informático contra amenazas y riesgos. Estas medidas pueden ser técnicas, organizativas o humanas, y su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información.

