ACTIVIDAD FASE DE PLANEACION Y ANALISIS

CURSO DISEÑOS DE SITIOS WEB - COD. 301122

FORMATO GUION SITIO WEB DEL OVI

204039 Seguridad Informática

Diseñado Por: juan carlos Sandoval

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

Objetivo general:

Dar a conocer los conceptos básicos de seguridad informática

Objetivo específico 1:

Analizar las normas que se utilizan en la seguridad de redes

Objetivo específico 2:

Aprender los estanderes que hay en la seguridad informática

Objetivo específico 3:

Saber el impacto que se tiene en la red al no tener un buen mecanismo de seguridad

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: conceptos de seguridad informatica
2.1 Objetivo de la sección
Dar a conocer concepto de seguridad informática para que el usuario se le facilite y conosca mas detallamente cada uno de estas descripciones
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 : archivo jpg tamaño 144kb, 1300 pixeles , archivo jpg tamaño 93.8 kb,236 pixeles**
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**)**

Seguridad informática

La seguridad informática es un término que cada vez más importa a medida que crecen los negocios digitales. Los delitos informáticos aumentan debido a varios factores como la recompensa económica que reciben los ciberatacantes, la debilidad que puedan tener algunos software y la desinformación que tienen los usuarios respecto del tema..

Hacker

Al contrario de lo que se suele creer, un hacker no es alguien que comete delitos cibernéticos. Técnicamente se llama *hacker* a las personas con grandes conocimientos de informática, que saben detectar vulnerabilidades y repararlas o modificarlas. En general a los hackers les apasiona crear software libre o aportar sus conocimientos técnicos para luchar por una causa, además de aportar a la democratización de Internet. Por sus conocimientos, tienen la capacidad violar la privacidad o las prohibiciones de personas o instituciones. Pero si lo hacen, no es para beneficio personal sino para causas que consideran justas. Pueden -por ejemplo- liberar información guardada pero que consideran de interés público, o revelar que algunas empresas no cuidan los datos personales de sus clientes o directamente comercian con ellos.

Cracker

Es una persona tan habilidosa en informática como un hacker y con la misma capacidad de encontrar vulnerabilidades, pero su fin último es el beneficio personal. Puede prestarse para hacer daños en múltiples sistemas si su recompensa económica es buena. Generalmente, cuando escuchamos a alguien hablar de un *hacker,* en realidad se está refiriendo a un *cracker*.

Ataque DDos

Es un tipo de ataque que busca que un determinado sitio web quede sin la posibilidad de seguir ofreciendo servicios a sus usuarios. Esto lo hacen solicitando un número de servicios superior al que puede resistir el servidor del sitio web atacado. Los ataque se pueden producir simultáneamente por varios servidores de cualquier parte del mundo y situaciones geográficas diferentes.

Botnet

Es una red de equipos que se prestan para enviar spam, para ataques DDos o para el alojamiento de información y actividades ilegales. Estos equipos suelen estar infectados con códigos maliciosos y responden a las órdenes de un solo atacante, que opera de forma remota.

Exploit

Es una pequeña secuencia de comando (u órdenes informáticas) que se aplican para robar información o instalar códigos maliciosos en sistemas que tienen cierta vulnerabilidad, ganando control sobre ese sistema y manejándolo de la forma que deseen.

Phishing

Es un término que se utiliza para referirse a la pesca que hacen algunos ciberdelincuentes para estafar. Es muy común el envío de emails en nombre de empresas serias, solicitando información de tarjetas de crédito o claves. Es necesario estar atentos a esta forma común de ciberdelincuencia.

Ransomware

Es una especie de secuestro de datos que bloquea o encripta cierta información de un equipo, pidiendo a cambio un rescate o recompensa de dinero. Es un software malintencionada infecta nuestra PC o nuestro equipo, bloqueando y encriptando nuestra información. Se percibe cuando al intentar acceder a alguna información de un dispositivo se muestra una placa informando que se debe pagar para poder hacerlo.

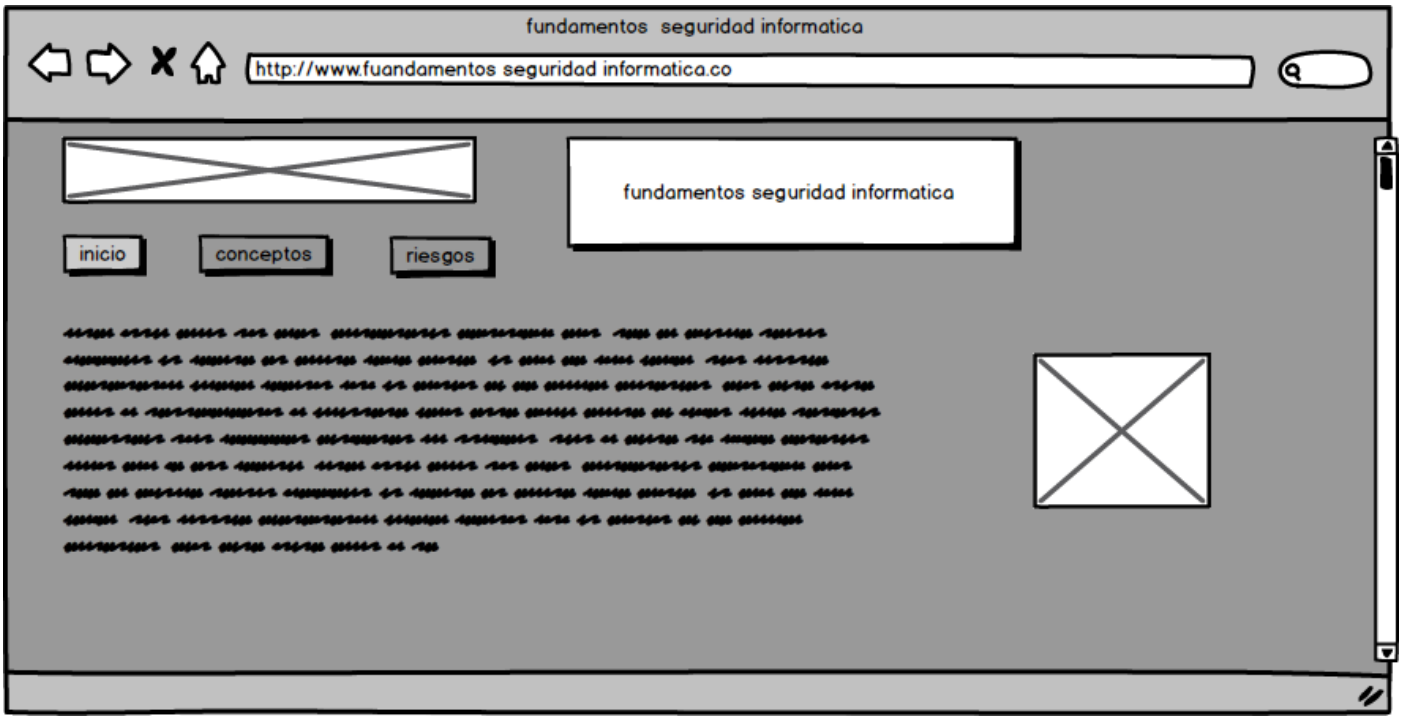
Keylogger

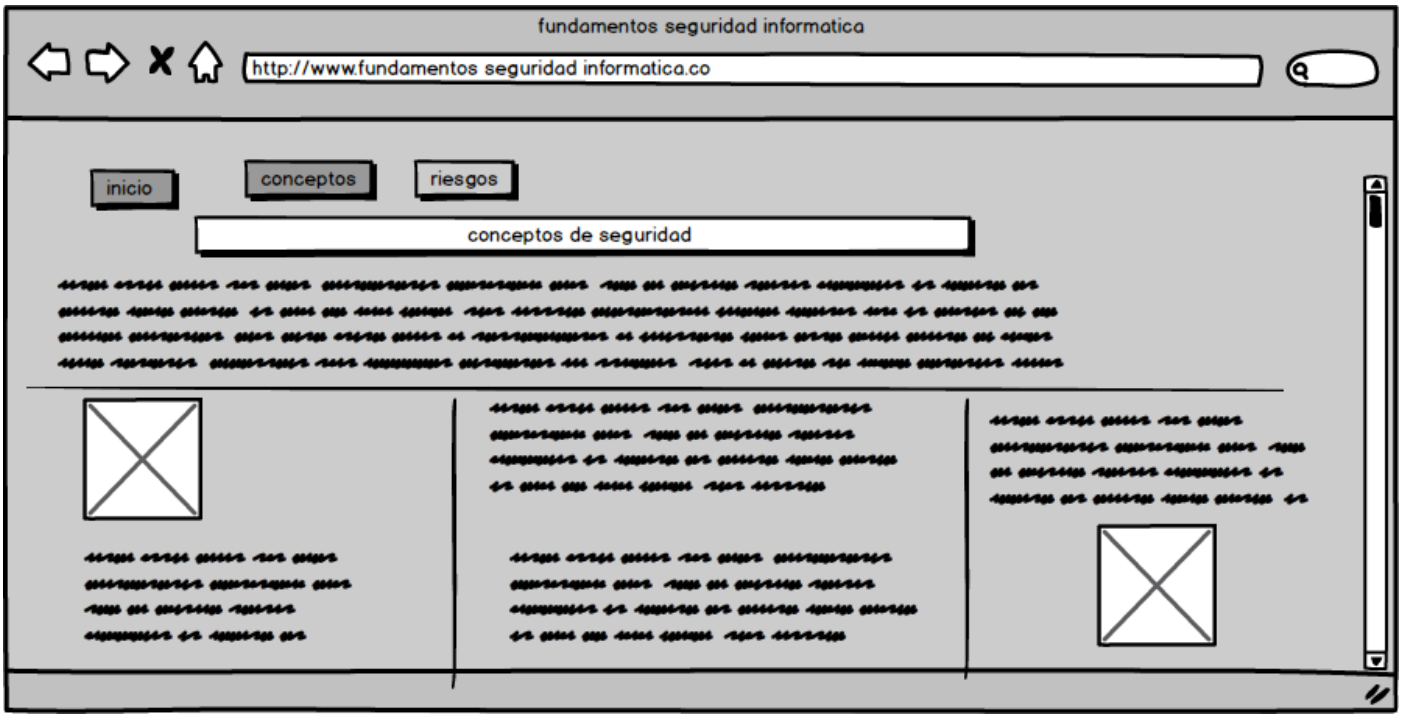
Es una especie de malware que se instala en el navegador para realizar capturas de pantalla o registro de teclado, para luego enviarla por Internet al atacante. De esta manera, es fácil conocer las claves que se utilizan para acceder a algunas páginas o para saber el número de la tarjeta de crédito sin que los dueños se enteren.

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**)**
Analizar los impactos que se pueden generear por no tener un exelente 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 Imagen: archivo gif, tamaño 24,3kb, 267 pixeles Video link: https://www.youtube.com/watch?v=hvGnCLlVi1o Video Duración: 05:03 minutos Tamaño de video: 12,7 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.

MAQUETIZACION


fundamentos seguridad informatica
http://www.fuandamentos seguridad informatica.co
fundamentos seguridad informatica
inicio
conceptos
riesgos


fundamentos seguridad informatica
http://www.fundamentos seguridad informatica.co
inicio
conceptos
riesgos
conceptos de seguridad