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 Miguel Cifuentes

1. Objetivos del OVI

Objetivo general:

Exponer a los Estudiantes o usuarios en el siguiente formato los distintos conceptos básicos en seguridad informática y sus mecanismos de seguridad.

Objetivo específico 1:

Dar a conocer los estándares y normas en seguridad informática.

Objetivo específico 2:

Tipos de amenazas principales relacionadas a la seguridad informática.

Objetivo específico 3:

Conceptos e impacto en la red que se tiene al ser vulnerable al uso de seguridad informática.

2. **Contenido informativo del OVI por secciones**

Nombre de la sección que se creara en el OVI: Conceptos de Seguridad Informática.
2.1 Objetivo de la sección: (Registre a continuación el objetivo que tiene esta sección**)**
Se da a conocer a los estudiantes o usuarios conceptos que abarcan el tema relacionado en seguridad informática.
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, tamaño Letra 12 puntos **Imagen:** 74 kb – formato JPG ,73 kb – formato JPG ,22 kb –formato JPG, 77 kb – formato 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 día crecen los delitos informáticos, éstos aumentan debido a varios factores, como la debilidad o desprotección de algunos softwares y la desinformación que tienen los usuarios respecto al tema; Algunos conceptos importantes para tener en cuenta.

Hacker: persona con grandes conocimientos técnicos apasionada en detectar vulnerabilidades y es capaz de modificar, cambiar, borrar o sustraer información, hay distintas clases de Hackeo y no todos los Hacker son malos; algunos contratacan a los **Cracker** que no tienen Hacking ético y estos últimos buscan beneficio personal, en su mayoría económico.

Ataque DDOS: Es un tipo de ataque que busca que determinado sitio web quede sin posibilidad de seguir dando servicios a sus usuarios, esto lo realizan solicitando un numero de servicio superior al del servidor del sitio web Atacado.

Botnet : Es una red de equipos que se presta para enviar spam para ataques DDos ,o para alojar información y actividades ilegales.

Exploit: Es una pequeña secuencia de comando, que la aplican para robar información o instalar códigos maliciosos en sistemas que tienen cierta vulnerabilidad.

Phishing : termino que se utiliza por algunos ciberdelincuentes para estafar.

Ransomware : software malintesionado que Bloquea o encripta información de un equipo , este se detecta cuando aparece una placa informando que se debe pagar para volver Acceder ala información.

Keylogger : Especie de malware que se instala en el navegador para realizar capturas de pantalla o registro de teclado para luego enviarla al atacante de esta manera pueden acceder a claves personales.

Nombre de la sección que se creara en el OVI: impacto de las vulnerabilidades en la red al no poseer un mecanismo de seguridad.
2.1 Objetivo de la sección: (Registre a continuación el objetivo que tiene esta sección**)**
Los estudiantes o Usuarios Analizan la importancia de la seguridad informática en equipos y software y las consecuencias en la vulnerabilidad 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**)**
Imagen: 18,9 Kb– formato JPG ,10,1 Kb – formato JPG **Video:** 9,65 Mb – duración 3 min 42 segundos, **link :** **https://www.youtube.com/watch?v=nFQD7wD4eOY** **Autor:** Andalucía es digital.
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**)**

vulnerabilidades en seguridad informática: se puede definir como una debilidad presente en un sistema operativo o software que permite al atacante violar la confidencialidad, integridad, disponibilidad y control de acceso en sus sistemas, datos y aplicaciones.

Las vulnerabilidades son producto de un mal diseño de software y también puede ser producto de las limitaciones propias de la tecnología para la que fue diseñado.

Existen 4 tipos de clasificación de importancia.

- **Critica**: permite la propagación de amenazas sin ser necesaria la participación del usuario.
- **Importante:** pone en riesgo la confidencialidad, integridad y disponibilidad de datos de los usuarios y a la vez la integridad, disponibilidad de los recursos de procesamiento.
- **Moderada:** es la vulnerabilidad más sencilla de combatir ya que el riesgo que presenta se puede disminuir con medidas de configuraciones predeterminadas.
- **Baja**: esta es difícil de aprovechar por el atacante, su impacto es mínimo ya que no afecta una gran masa de usuarios.

Cada una de las calificaciones anteriores enumera peligrosas vulnerabilidades con un grado de daño peligroso en masa es decir en cantidad de usuarios en el caso de una red de empresas o de interes público hasta un usuario en específico.

- Es importante crear protocolos de seguridad para no ser víctimas de las vulnerabilidades prever, detener y recuperación. Desde la computadora personal se puede implementar un control de todo lo que hacemos, vemos, descargamos y páginas que investigamos con software puesto a disposición por los mismos sistemas operativos u otros hechos para ayudar a bloquear las vulnerabilidades de peligro, así mismo hay protocolos de seguridad bastante completos para proteger servidores y demás sistemas informáticos de empresas sitios de interes de la delincuencia informática.