ACTIVIDAD FASE DE PLANEACION Y ANALISIS

CURSO DISEÑOS DE SITIOS WEB - COD. 301122

FORMATO GUION SITIO WEB DEL OVI

204039 Seguridad Informática

Diseñado Por: Gina Oliva Puerto E.

Cod: 1053608982

1. **Objetivos del OVI (**describa mediante el registro de 1 objetivo general y tres específicos para que se construye este OVI**)**

Objetivo general:

Dar a conocer de manera teórica y comprensiva, los conceptos básicos de la seguridad informática y la importancia de su uso, en sus diferentes escenarios, de manera que las personas entiendan y apliquen la seguridad en redes y la informática en general.

Objetivo específico 1:

Mostrar de manera clara, los estándares usados en la seguridad de redes.

Objetivo específico 2:

Ofrecer información de manera clara sobre las normas de la seguridad en las redes.

Objetivo específico 3:

Demostrar el impacto que tiene el buen uso de la seguridad informática, además de los riesgos a los que estamos expuestos en caso de no contar con un buen sistema de seguridad en cuanto a la protección de nuestros datos virtual mente.

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: Inicio- Significado de la seguridad informática.(Inicio)
2.1 Objetivo de la sección: (Registre a continuación el objetivo que tiene esta sección**)**
Presentar de manera clara y didáctica la importancia del uso de la seguridad informática y significado de la misma.
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: Arial 12 puntos, **Recuperado de: "Seguridad informática". En: Significados.com. Disponible en: https://www.significados.com/seguridad-informatica/** **Tomado de Infosegur (noviembre del 2013) https://infosegur.wordpress.com/category/1-conceptos-basicos-de-la-seguridad-informatica/** **Recuperado de: ¿Qué es la seguridad informática y cómo puede ayudarme?** Por: **Equipo de Expertos** **Universidad Internacional de Valencia (2018)** **https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/**

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

Es la disciplina que se encarga de proteger la integridad y privacidad de la información almacenada en un sistema informático, a pesar del avance de la tecnología, no se ha encontrado algo efectivo que pueda proteger nuestros datos de la inviolabilidad de un sistema.
La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.
La seguridad informática se caracteriza por la protección de datos y de comunicaciones en una red asegurando, en la medida de lo posible, los tres principios básicos son:

La integridad de los datos: la modificación de cualquier tipo de información debe ser conocido y autorizado por el autor o entidad.

La disponibilidad del sistema: la operación continua para mantener la productividad y la credibilidad de la empresa.

La confidencialidad: la divulgación de datos debe ser autorizada y los datos protegidos contra ataques que violen este principio.
La seguridad informática es una disciplina o rama de la Tecnología de la información, que estudia e implementa las amenazas y vulnerabilidades de los sistemas informáticos especialmente en la red como, por ejemplo, virus, gusanos, caballos de troya, ciber-ataques, ataques de invasión, robo de identidad, robo de datos, adivinación de contraseñas, intercepción de comunicaciones electrónicas, entre otros.

Nombre de la sección que se creara en el OVI: Conceptos Básicos de la seguridad Informática
2.1 Objetivo de la sección: (Registre a continuación el objetivo que tiene esta sección**)**
Presentar de manera clara y didáctica los conceptos básicos normas y estándares.
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:12 puntos; **Conceptos Básicos sobre Seguridad Informática;** tomado de **Youtube** Néstor Adrián Aguirre Publicado el 9 jul. 2017 recuperado de: **https://www.youtube.com/watch?v=JXDUKotmsWQ** **Security Hangout / Conceptos Básicos de la seguridad | DAIT – Seguridad informática;** tomado de **YouTube** por: Instituto de Ciberseguridad Publicado el 30 abr. 2016 **https://www.youtube.com/watch?v=JtEQDGA3WmY** **Conceptos fundamentales de seguridad informática - #02;** Tomado de **YouTube** por: **CURSOS PROFESIONALES** Publicado el 17 nov. 2017 **https://www.youtube.com/watch?v=87rBXGIBbUA** **Tomado de: Linkedin Learning Instructor José Dimas Luján Castillo(2017).** **https://es.linkedin.com/learning/fundamentos-de-la-seguridad-informatica/normas-o-estandares-en-seguridad-informatica**

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 Básicos de la seguridad Informática

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, por ejemplo.

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 (¿todo lleva a “Black Mirror”, la serie televisiva inglesa?). 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.

Sheila Berta (más conocida como @unapibageek o “Shey Winker”), especialista en seguridad informática, agrega algunos conceptos a la lista.

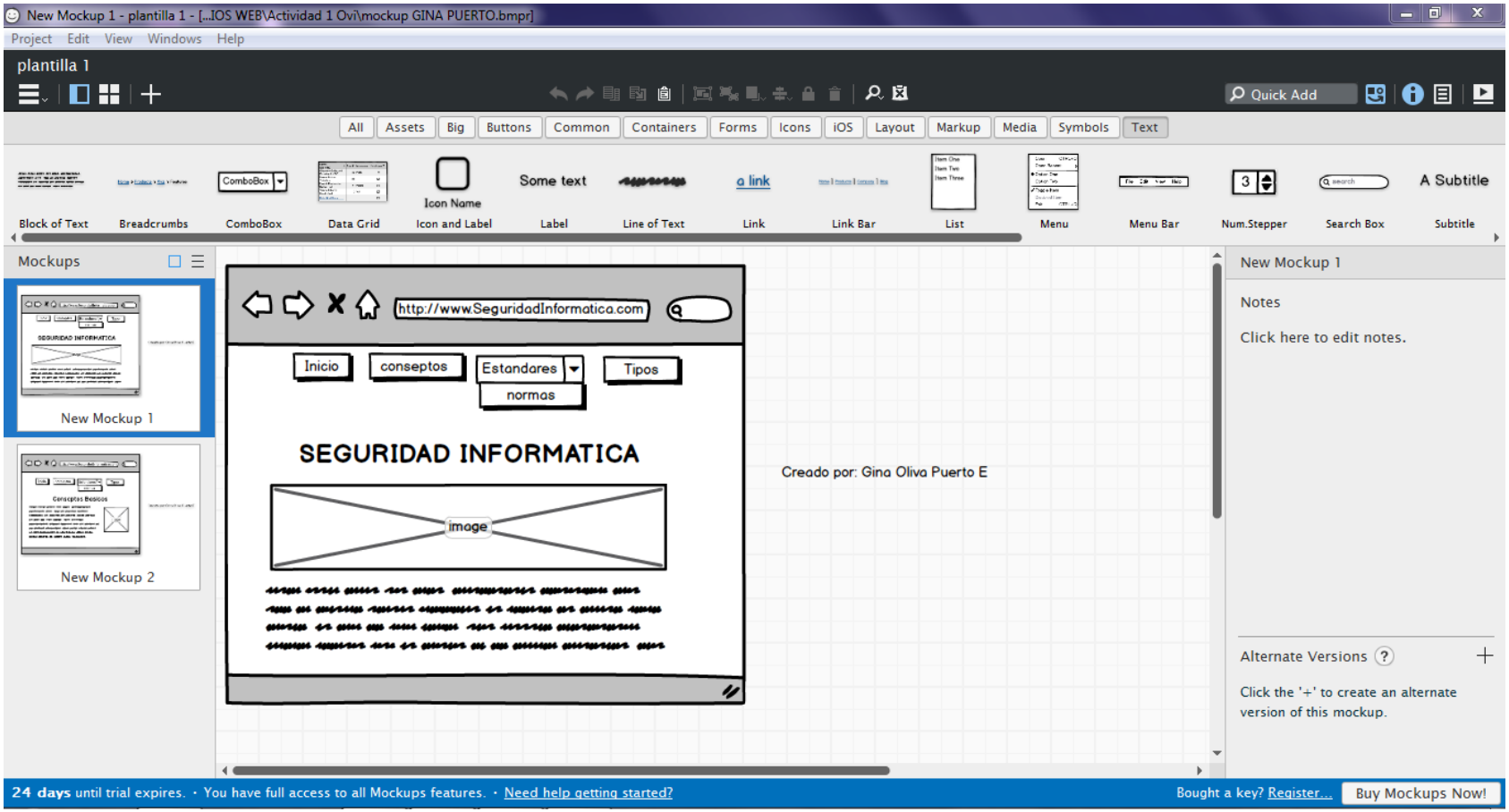
Ataque DDoS. La sigla significa Distributed Denial of Service y la mejor forma de entender de qué se trata es analizando la definición en términos. Una denegación de servicio (Denial of Service) implica que un determinado servicio (web u otro) quede completamente fuera de disponibilidad para sus usuarios. 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 (Distributed), simplemente

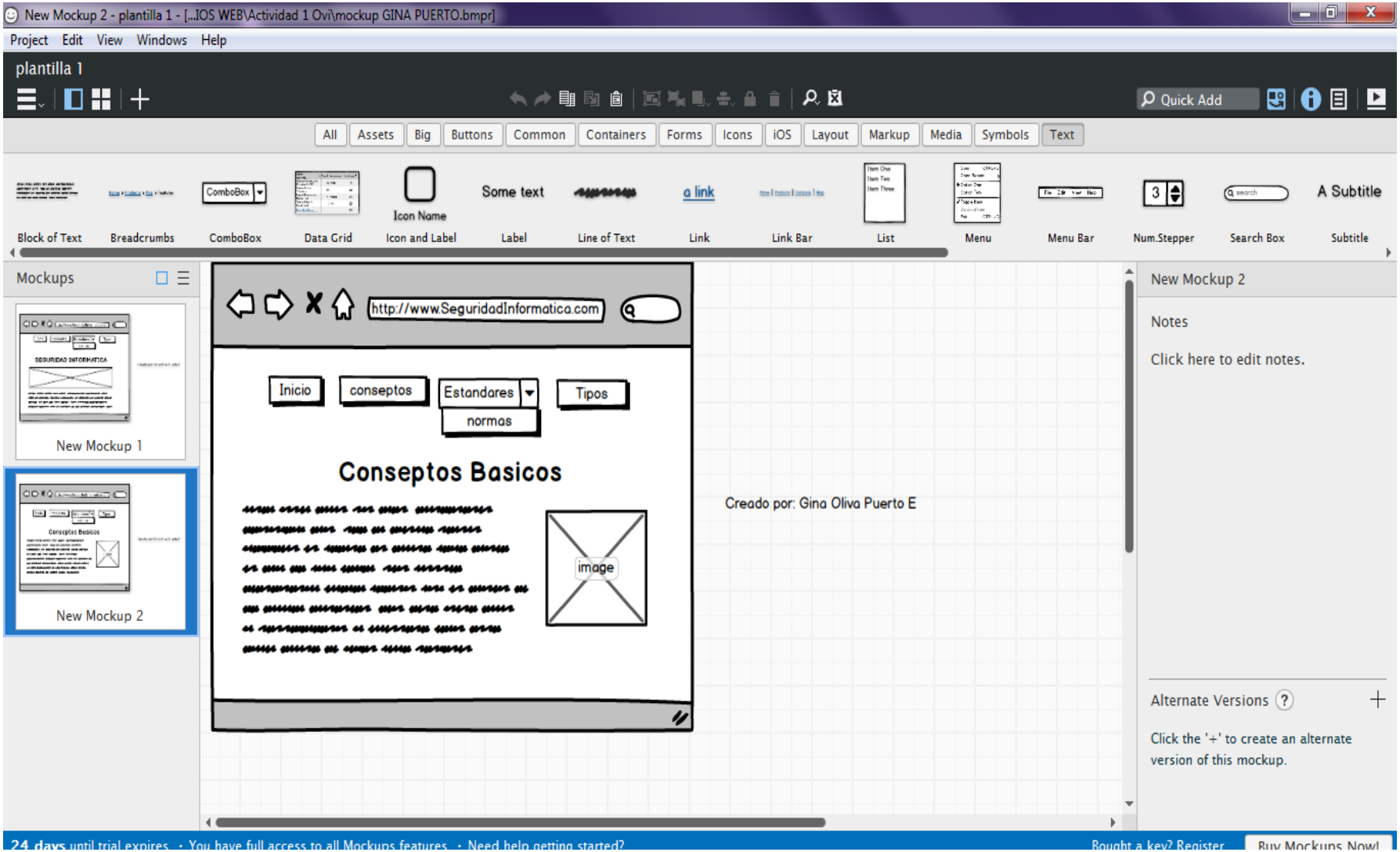
porque las técnicas de ataque se llevan a cabo desde lugares geográficamente diferentes. En el caso de un servicio web, el ataque DDoS más frecuente es que múltiples equipos soliciten recursos a ese sitio continuamente, de manera que el servidor que está detrás, no dé abasto con las peticiones y sufra 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).

Tomado de: https://www.lanacion.com.ar/1970660-7-conceptos-basicos-de-seguridad-informatica-que-deberias-saber

DISEÑO DE MOCKUP




New Mockup 2 - plantilla 1 - [...IOS WEB\Actividad 1 Ovi\mockup GINA PUERTO.bmpr]
Project Edit View Windows Help
plantilla 1
Quick Add
All Assets Big Buttons Common Containers Forms Icons iOS Layout Markup Media Symbols Text
Block of Text Breadcrumbs ComboBox Data Grid Icon and Label Label Line of Text Link Link Bar List Menu Menu Bar Num.Stepper Search Box Subtitle
Some text
a link
Icon Name
A Subtitle
Mockups
New Mockup 1
New Mockup 2
http://www.SeguridadInformatica.com
Inicio
conseptos
Estandares
normas
Tipos
Conseptos Basicos
image
Creado por: Gina Oliva Puerto E
New Mockup 2
Notes
Click here to edit notes.
Alternate Versions
Click the '+' to create an alternate version of this mockup.
24 days until trial expires · You have full access to all Mockups features · Need help getting started?
Bought a key? Register
Buy Mockups Now!