

DISEÑO DE SITIOS WEB

FASE DE DISEÑO

PAULA ANDREA FERNANDEZ CÓDIGO:

ADRIANA MARIA VARGAS CÓDIGO: 52840872

KARINA SANDOVAL CAMELO CÓDIGO: 52999611

JAQUELINA ARDILA CÓDIGO: 52963562

LUZ MARIELA TRIANA CÓDIGO: 52801060

GRUPO: 301122_56

PRESENTADO A

JOSUE IGNACIO OCHOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

MARZO 2017

INTRODUCCIÓN

Para poder crear un proyecto, ya sea un OVI (objeto virtual de aprendizaje), un sitio web, una página o cualquier otro tipo de proyecto, se necesita primero planear lo que se va a hacer, cómo se va a hacer y porqué se va a hacer. El diseño no empieza cuando empezamos a implementar nuestro sitio, el diseño empieza cuando nos sentamos a pensar en lo que vamos a hacer, definir el objetivo del por qué estamos creando ese sitio, como lo vamos a mostrar, y que vamos a incluir.

Este trabajo colaborativo es la consolidación del planeamiento de nuestro OVI, nuestro grupo ha escogido el tema de “seguridad informática” y hemos diseñado el contenido según la temática; también hemos llegado a un acuerdo de cómo mostrar dicha información, teniendo en cuenta los planeamientos y la identidad institucional de nuestra universidad.

OBJETIVOS


- Poner en práctica habilidades de planificación y organización, orientadas al diseño de nuestro OVI (Objeto Virtual de aprendizaje)
- Escoger la temática a trabajar para nuestro OVI (Objeto Virtual de Información).
- Plantear el objetivo de nuestro sitio.
- Escoger el contenido
- Establecer la Estructura del sitio, según los lineamientos de la institución

OVI PARA DISEÑAR UN OBJETO VIRTUAL DE INFORMACIÓN – OVI

SEGURIDAD INFORMÁTICA


Objetivo General

Definir el concepto de seguridad informática, objetivos, impacto que se tiene en la red al no tener un buen mecanismo de seguridad e igualmente amenazas, riesgos y maneras de prevenir o disminuir dichas amenazas y riesgos.


Sección de texto	Sección de imágenes
<p>¿QUÉ ES SEGURIDAD INFORMÁTICA?</p> <p>La seguridad informática pretende identificar las amenazas y reducir los riesgos al detectar las vulnerabilidades acabando o minimizando así el impacto o efecto nocivo que se pueda causar.</p> <p>La seguridad informática no es un producto, es un proceso. Sirve para garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la</p>	

<p>información contenida en ellos, así como de las redes privadas y sus recursos. Se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas.</p> <p>Referencias consultadas e información tomada de :</p> <p>http://seguridadinformatica-zequieltgarcia.blogspot.com.co/2012/08/para-que-sirve-la-seguridad-informatica.htmlhttps://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica</p> <p>http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008</p> <p>http://www.monografias.com/trabajos81/seguridad-en-redes/seguridad-en-redes2.shtml</p>	<p>http://agenciadenoticias.unal.edu.co/detalle/article/plan-de-seguridad-informatica-para-empresas-kpo.html</p>
--	--

--	--

Sección de texto	Sección de imágenes
<p>OBJETIVOS DE LA SEGURIDAD INFORMÁTICA:</p> <p>El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable.</p> <p>El objetivo secundario de la seguridad informática. Consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total.</p> <p>Referencias consultadas e información tomada de :</p> <p>http://seguridadinformatica-zequielgarcia.blogspot.com.co/2012/08/para-que-sirve-la-seguridad-informatica.html</p> <p>https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica</p> <p>http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008</p> <p>http://www.monografias.com/trabajos81/seguridad-en-redes/seguridad-en-redes2.shtml</p>	 <p>http://www.uhcl.edu/cyber-security-institute</p>

--	--

Sección de texto	Sección de imágenes
<p style="text-align: center;">AMENAZAS INFORMÁTICAS</p> <p>Adware: programas que se instalan en los equipos para descargar y mostrar publicidad como ventanas emergentes cuando accede a internet e inclusive sin necesidad de acceder a él. Generalmente no daña el equipo pero si usa sus recursos para ejecutarse.</p> <p>Ataque día cero: un ataque dirigido a una aplicación o sistema que busca la ejecución de malware, gracias al conocimiento de las vulnerabilidades del sistema y para el cual aún no se ha desarrollado ningún parche de seguridad.</p> <p>Backdoor o puerta trasera: forma de entrar a un sistema evitando todos los sistemas de seguridad y sin conocimiento del propietario del sistema.</p> <p>Botnets: o zombis, es un conjunto de equipos infectados, los cuales son controlados por un ciberdelicuentes de manera remota para utilizar sus recursos.</p> <p>Caballos de Troya o troyanos: Este es un programa que se instala en la computadora y permite que usuarios externos accedan a él,</p>	 <p>Tipos de virus:</p> <p>http://princimaticos.blogspot.com.co/2010/11/virus-informaticos-computadora.html</p>

con el fin de robar información o controlar la maquina huésped. El troyano a diferencia del virus no corrompe ningún archivo, su objetivo es solo lograr el control de la máquina

Gusanos: Este es un tipo de virus que posee la habilidad de duplicarse a sí mismo. Este tipo de amenaza afecta la red como por ejemplo al consumir ancho de banda. Ya que se empiezan a duplicar sin restricción, consumen los recursos del sistema, colocando el sistema lento y hasta evitando que los programas se ejecuten correctamente o por completo.

Hackers: Informáticos altamente capacitados que usan sus conocimientos de manera intencional para robar datos o causar daños a los sistemas.

Malware: códigos diseñados para alterar el funcionamiento normal de un sistema informático corrompiendo o dañando archivos.

Phishing: Llegan mediante correos o páginas web, simulando ser páginas o mensajes auténticos, con el fin que el usuario se confíe y entregue datos personales o confidenciales. Ejemplo: cuando llega una página de un banco solicitando llenar un formulario para actualizar datos.

Ransomware: Es un programa que bloquea los dispositivos solicitando a su víctima un rescate para volver a tener acceso a su información.

Scam: estafas a través de medios electrónicos, muy parecido al phishing, con el objetivo claro de engañar para obtener ganancias.

Spywares: Estos programas espías buscan recopilar información de una empresa o usuario. Esta información recopilada puede ser usada desde fines publicitarios, reconociendo los hábitos de los usuarios, hasta ser usada para robar datos de los usuarios como claves de cuentas o información crítica de una empresa.

Virus informáticos: programas que se copian de forma automática y puede ejecutarse a sí mismos para alterar el funcionamiento normal del equipo, infectando o corrompiendo los archivos de la computadora. Pueden llegar a generar molestias como publicidad o bromas, hasta destruir intencionalmente la información del equipo o bloquear las redes informáticas afectando el tránsito de información.

Roberto8. 11Julio2008. Tipos de amenazas informáticas.

Wordpress. Disponible en:

<https://windsofthesky.wordpress.com/2008/07/11/tipos-de-amenazas-informaticas/>.

Oceano-IT.2014.amenazas más comunes en la actualidad.

Disponible en: <http://www.oceano-it.es/news-individual/369/amenazas-informaticas-mas-comunes-en-la-actualidad>

<p>Luzardo Ivan. 30 noviembre de 2010. Conozca las amenazas informáticas más comunes. Enter.co Disponible en:</p> <p>http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/</p> <p>Myers Lysa. 25 febrero 2015. ¿Qué es un 0-day? Explicando términos de seguridad. Welivesecurity. Disponible en:</p> <p>http://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/</p>	
--	--

Sección de texto	Sección de imágenes
<p>IMPACTO QUE SE TIENE EN LA RED AL NO TENER UN BUEN MECANISMO DE SEGURIDAD.</p> <p>El no tener una buena seguridad en la red implica que se Pueden causar daños o pérdidas financieras o administrativas a una empresa u organización, un hacker puede acceder fácilmente a la red interna .Esto habilitaría a un atacante sofisticado, leer y posiblemente filtrar correo</p>	

y documentos confidenciales; equipos basura, generando información; y más. Por no mencionar que entonces utilice su red y recursos para volverse e iniciar el ataque a otros sitios, que cuando sean descubiertos le apuntarán a usted y a su empresa, no al hacker.

Las amenazas, como ya hemos mencionado, consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma.


Una vulnerabilidad es alguna característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza, intencional o accidentalmente. Las vulnerabilidades pueden provenir de muchas fuentes, desde el diseño o implementación de los sistemas, los procedimientos de seguridad, los controles internos, etcétera; se trata en general de protecciones inadecuadas o insuficientes, tanto físicas como lógicas, procedimentales o legales de alguno de los recursos informáticos. Las vulnerabilidades al ser explotadas resultan en fisuras en la seguridad con potenciales impactos nocivos para la organización.


Referencias consultadas e información tomada de :



https://cdn.pixabay.com/photo/2014/08/25/09/26/monster-426995_960_720.jpg

<p>-http://seguridadinformatica-zequieltgarcia.blogspot.com.co/2012/08/para-que-sirve-la-seguridad-informatica.html</p> <p>- https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica</p> <p>- http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008</p> <p>-http://www.monografias.com/trabajos81/seguridad-en-redes/seguridad-en-redes2.shtml</p>	
---	--

Sección de texto	Sección de imágenes
<p>HERRAMIENTAS QUE PUEDEN AYUDAR A MEJORAR LA SEGURIDAD INFORMATICA</p> <p>✓ Sensibilización a usuarios de los riesgos de la seguridad informática, como son los peligros de ingresar a páginas no confiables, descargar o instalar programas no autorizados.</p>	

<ul style="list-style-type: none"> ✓ Copias de seguridad periódicas de la información más sensible, en lo posible automáticas con herramientas especializadas para ello. ✓ Actualizaciones de los sistemas operativos y antivirus de los computadores y servidores. Antivirus como Kaspersky, Panda, Microsoft, Avast, AVG, Avira, entre otros son de gran ayuda. ✓ Restricciones de instalaciones de programas a usuarios. ✓ Políticas de navegación a internet a usuarios. ✓ Controles de seguridad de acceso a Datacenters o cuartos de telecomunicaciones. ✓ El uso de hardware y equipos de seguridad apropiados que ayuden a mitigar ataques, marcas reconocidas en el mercado tales como Fortinet, Cisco, SonicWall, WatchGuard se han especializado en seguridad informática. 	<p>https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcTDL65u_nH54PNG0doj5ZQehQx86rVIdbpBsqg7oBco2pnZfwyIoQ</p>  <p>https://icybersecurity.files.wordpress.com/2014/05/cursos-seguridad-informatica-online.jpg?w=300&h=254</p>
---	--

✓ Personal idóneo en el área de tecnología y en constante capacitación acerca de problemas de seguridad informática

✓ Capacitación Constante a colaboradores acerca de los riesgos que pueden estar expuesto al no hacer un uso adecuado de herramientas como internet; importante la creación de políticas de seguridad informática.

[CCM Benchmark. \(s.f.\). Introducción a la seguridad informática. Recuperado de http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica](http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica)

Galeano, J., & Alzate, C. (2013). Protocolo de Políticas de Seguridad Informática para las Universidades de Risaralda.

Recuperado de

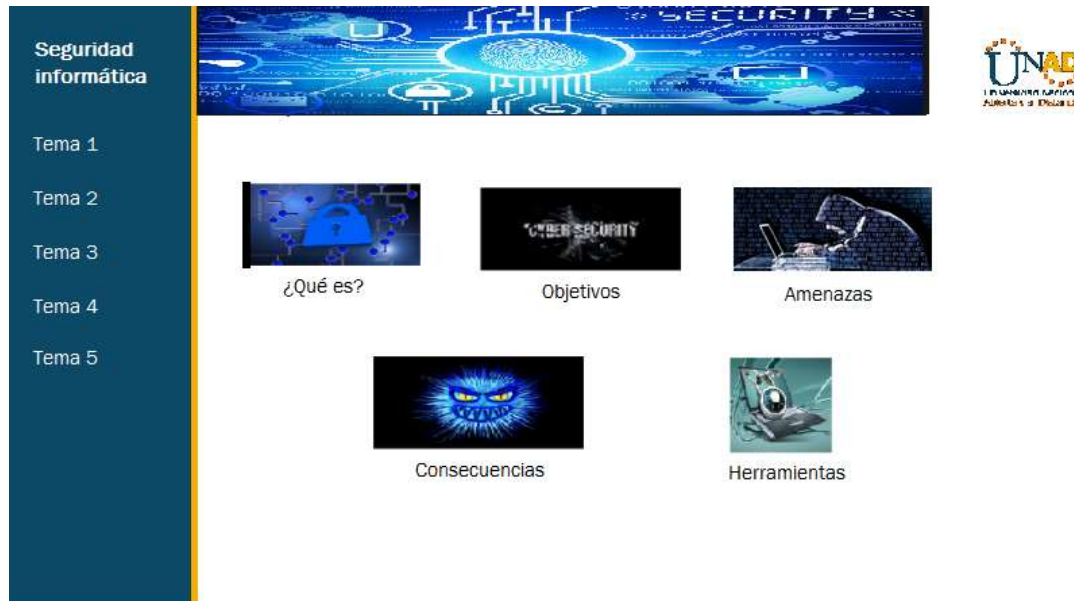
<http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1>

GlobalGate. (2013). Fortinet. Recuperado de

<http://fortinet.globalgate.com.ar/ver.php/mod/contenido/identificador/26/ Porque%20Fortinet>

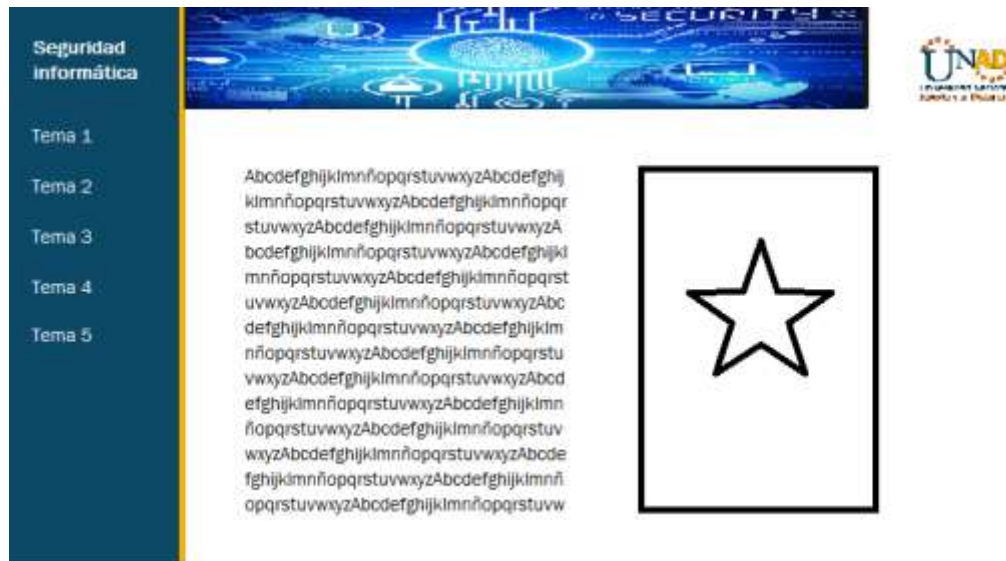
MÁQUETAS Y ENLACES DE HERRAMIENTA DE MAQUETACIÓN

INDEX



Herramienta de maquetación: <https://wireframe.cc/z6es1x>

CONTENIDO



Herramienta de maquetación: <https://wireframe.cc/dts5ea>

CONCLUSIONES

Para poder realizar un proyecto, necesitamos tener claro con qué objetivo lo vamos a hacer, planear que contenido vamos a utilizar y como se va a mostrar.

Una buena planificación, nos permitirá que nuestro proyecto cumpla con las expectativas deseadas.

Los diagramas o herramientas de maquetación son una gran ayuda para tener una idea general de cómo se va a ver nuestro sitio, y así poder hacer los cambios que se consideran pertinentes.

BILBIOGRAFÍA

Voutssas,J.(2010). Preservación documental digital y seguridad informática. Centro Universitario de Investigaciones Bibliotecológicas de la UNAM. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

(2015). Seguridad informática. Recuperado de https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Escobedo Rojas, A,(2010).Metodología de estudios. Recuperado de <http://www.monografias.com/trabajos81/seguridad-en-redes/seguridad-en-redes2.shtml>
[CCM Benchmark. \(s.f.\). Introducción a la seguridad informática. Recuperado de](http://www.monografias.com/trabajos81/seguridad-en-redes/seguridad-en-redes2.shtml)
<http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica>

Galeano, J., & Alzate, C. (2013). Protocolo de Políticas de Seguridad Informática para las Universidades de Risaralda. Recuperado de <http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1>

GlobalGate. (2013). Fortinet. Recuperado de <http://fortinet.globalgate.com.ar/ver.php/mod/contenido/identificador/26/Porque%20Fortinet>

Roberto8. (11 Julio2008). Tipos de amenazas informáticas. Wordpress. Disponible en: [https://windsofthesky.wordpress.com/2008/07/11/tipos-de-amenazas-informaticas/.](https://windsofthesky.wordpress.com/2008/07/11/tipos-de-amenazas-informaticas/)

Oceano-IT. (2014) .Amenazas más comunes en la actualidad. Disponible en: <http://www.oceano-it.es/news-individual/369/amenazas-informaticas-mas-comunes-en-la-actualidad>

Luzardo Ivan. (30 noviembre de 2010). Conozca las amenazas informáticas más comunes.

Enter.co Disponible en: <http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/>

Myers Lysa. 25 febrero 2015. ¿Qué es un 0-day? Explicando términos de seguridad.

Welivesecurity. [Disponible en: http://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/](http://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/)

Imágenes tomadas de :

https://cdn.pixabay.com/photo/2014/08/25/09/26/monster-426995_960_720.jpg

<https://iicybersecurity.files.wordpress.com/2014/05/curso-seguridad-informatica-online.jpg?w=300&h=254>

<https://encrypted->

[tbn2.gstatic.com/images?q=tbn:ANd9GcTDL65u_nH54PNG0doj5ZQehQx86rVIdbpBsqq7oBco2pnZfwyIoQ](https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcTDL65u_nH54PNG0doj5ZQehQx86rVIdbpBsqq7oBco2pnZfwyIoQ)

http://4.bp.blogspot.com/_P25k12LwnX8/TOK_u60AoXI/AAAAAAAAAEE/i9kgFLG_bIQ/s400/TiposDeVirus.jpg

<http://agenciadenoticias.unal.edu.co/detalle/article/plan-de-seguridad-informatica-para-empresas-kpo.html>

<http://www.uhcl.edu/cyber-security-institute>