Seguridad Informática - 2º SMR
Tema 1: Conceptos básicos de Seguridad Informática

1.1.1. Busca en Internet tres noticia sobre vulneración de la seguridad de algún sistema informático

- Rector de UES pide a Fiscalía investigar vulneración de sistema informático, El rector afirmó que los delincuentes vulneraron los sistemas virtuales de seguridad y se metieron a la web de la Biblioteca de la UES, vieron en pantalla un registro de notas y creyeron que lo habían modificado; lo cierto fue que no hubo tal modificación. “De ahí que garantizamos y le damos certeza a nuestros estudiantes que no hubo tal modificación en sus notas”, afirmó Arias. Sin embargo, varios estudiantes intentaron verificar sus notas el domingo, y todas las materias les aparecían aprobadas con 6.90.

- Hackean páginas web de la Universidad de El Salvador y cambian a 6.90 las notas de los alumnos, el vicerrector académico dijo que están a la espera del informe técnico del análisis del incidente pero adelantó que existe respaldo de todos los archivos de seguridad, particularmente de las notas de todos los estudiantes. El equipo del DTI realiza estudios y análisis respectivos para restablecer el sistema y de encontrar indicios de vulneración de la datos de la comunidad universitaria se interpondrá la denuncia ante la Fiscalía General de la República (FGR), ya que esta información es un bien público.

- Desde hace tiempo WhatsApp tiene una web en la que va anunciando las actualizaciones que realiza, así como las vulnerabilidades que se han detectado y lo que han supuesto. Este ejercicio de transparencia de la compañía ayuda a hacerse una idea sobre los problemas a los que se enfrenta cualquier aplicación de este tipo. En su última actualización ha enumerado seis vulnerabilidades detectadas, de las cuales cinco fueron solucionadas el mismo día y la última se tardó algo más de tiempo.

1.3.1. Asocia los distintos mecanismos de seguridad expuestos en el tema con los objetivos de la seguridad informática.

- Hardware: Disponibilidad, no repudio
- Software: Autenticación, integridad, confidencialidad

1.3.2. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:

a) mesa No Segura
b) caseta No Segura
c) c8m4r2nes Segura
d) tu primer apellido No Segura
e) pr0mer1s& Segura
f) tu nombre No Segura

1.3.3. Escribe una contraseña muy segura y di por qué es muy segura.

Ka9sÑalsdoÀsk313a-als280231Hjk.$

Es una contraseña segura por que tiene muchos caracteres, tiene mayúsculas, minúsculas, números y signos, y no tiene referencia a nada en concreto.

1.3.4. Al poner la contraseña de la pregunta anterior, ¿te aseguras al 100% de que nadie va a poder hacer uso de ella (robártela)?

No me aseguro puesto que existen programas que descifran contraseñas de todas las posibilidades que pueden existir con todos los caracteres.

1.4.1. Describe los medios de seguridad física y lógica que hay en el aula.

Una infraestructura física, solo podemos entrar los usuarios que tengamos acceso a dichos ordenadores, no repudio, no tiene disponibilidad puesto que cuando se apaga el equipo se borran los datos de dichos equipos, tampoco tienen autenticación puesto que se inician automáticamente sin necesidad de usuario y contraseña.

1.4.2. De cada uno de los elementos expuestos a continuación, indica a qué dos tipos de seguridad están asociados (activa y lógica, activa y física, pasiva y lógica o pasiva y física)

a) Ventilador de un equipo informático

Activa y Física

b) Detector de incendios

Activa y Física

c) Detector de movimientos

Activa y Física

d) Cámara de seguridad

Activa y Física

e) Cortafuegos

Activa y Lógica

f) SAI

Pasiva y Física

g) Control de acceso mediante el iris del ojo.

Activa y Lógica

h) Contraseña para acceder a un equipo

Activa y Lógica

i) Control de acceso a un edificio

Activa y Lógica

1.4.3. Evalúa qué medias de seguridad activa y pasiva tienes en torno a tu ordenador personal.

Una Copia de seguridad, Antivirus, Contraseña.

1.6.1. Analiza la noticia buscada sobre ataques informáticos e indica el tipo de ataque y atacante del que se trata.

En la noticia que puse de ataques informáticas de la universidad que cambiaron las notas a 6,90 se considera crackers al ser hacker y hacer daño u obtener un beneficio por ello.

1.7.1. Analiza que pautas de protección no cumple el sistema que tienes en tu casa.

Redactar y revisar regularmente los planes de actuación ante catástrofes.

Gestionar y revisar los logs del sistema.

1.9.1. Vamos a crear una empresa de comercio electrónico y vamos a pedir en el registro de los clientes sus datos personales además de sus gustos para enviarles publicidad sobre los temas seleccionados. Indica los pasos a seguir antes, durante y después de la obtención de los datos de los clientes para cumplir la normativa de la LOPD.

El nivel de seguridad sería básico ya que piden sus datos personales y gustos, los pasos serian:

Debe existir un documento donde estén reflejadas las funciones y obligaciones de cada usuario del fichero. El responsable del fichero debe almacenar a su vez una lista de los usuarios con sus accesos y las contraseñas deben ser cambiadas en un periodo no superior a un año.

Debe crearse un registro de incidencias del fichero de datos.

Cualquier documento que se deseche y que contenga datos de carácter personal tendrá que ser borrado o destruido.

Las copias de seguridad deberán ser como mínimo una a la semana.

1.10.1. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.

a) Terremoto

Física

b)Subida de tensión

Física

c) Virus informático

Lógica

d) Hacker

Física

e) Incendio fortuito

Física

f) Borrado de información importante

Lógica

1.10.2. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.

a) Antivirus

Activa

b) Uso de contraseñas

Activa

c) Copias de seguridad

Pasiva

d) Climatizadores en el CPD

Activa

e) Uso de redundancia de discos

Pasiva

f)Cámaras de seguridad

Activa

g) Cortafuegos

Activa

1.10.3. Describe los medios de seguridad activa y pasiva que hay en el aula

Hay Cortafuegos, firewall, camara de seguridad.

1.10.4. Ordena de mayor a menor seguridad los siguientes formatos de claves.

a) Claves con sólo números

b) Claves con números, letras mayúsculas y letras minúsculas

c) Claves con números, letras mayúsculas, letras minúsculas y otros caracteres

d) Claves con números y letras minúsculas

e) Claves con sólo letras minúsculas

C, B, D,E,A

1.10.5. Busca en Internet las claves más comúnmente usadas.

23456 – sin cambios.
password – (contraseña) sin cambios.
123456789 – sube 3 posiciones.
12345678 – baja 1 posición.
12345 – sin cambios.
111111 – nueva.
1234567 – sube 1 posición.
sunshine – (luz del Sol) nueva.

1.10.6. Decides montar una empresa en Internet que se va a dedicar a ofrecer un disco duro on-line. Necesitas de cada usuario: nombre, teléfono y dirección de correo electrónico. ¿En qué afectarán estos datos a la formación de tu empresa? ¿Qué medidas de seguridad tendrás que tomar cuando almacenas esta información?

La medida de seguridad es basica, las medidas que se tomaran seran un documento donde estén reflejadas las funciones y obligaciones de cada usuario del fichero. El responsable del fichero debe almacenar a su vez una lista de los usuarios con sus accesos y las contraseñas deben ser cambiadas en un periodo no superior a un año. Debe crearse un registro de incidencias del fichero de datos. Cualquier documento que se deseche y que contenga datos de carácter personal tendrá que ser borrado o destruido. Las copias de seguridad deberán ser como mínimo una a la semana. Afectaran para poder comunicarse con el cliente.