

Alumna: Araceli de la Rosa Rojas

Profesora: Giselle Montero González

Materia: Tecnologías de la Información y la Comunicación

Tema: Cuestionario de Sistemas de Información

Grupo: 1

Cuatrimestre: 9

**1. ¿Por qué son tan vulnerables los SI?**

Pueden ser vulnerables por diversos factores como:

**Diseño**

* Debilidad en el diseño de protocolos utilizados en las redes.
* Políticas de seguridad deficiente e inexistente.

**Implementación**

* Errores de programación.
* Existencia de “puertas traseras” en los sistemas informáticos.
* Descuido de los fabricantes.

**Uso**

* Mala configuración de los sistemas informáticos.
* Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
* Disponibilidad de herramientas que facilitan los ataques.
* Limitación gubernamental de tecnologías de seguridad.

2.    **¿Cuáles amenazas consideras que los SI son especialmente vulnerables? ¿Por qué lo crees así?**

En la implementación ya que son más casuales en los errores de programación.

**3.      ¿Por qué están difícil proteger a Internet y a las redes Wi-Fi? porque** son grandes redes y publicas que son vulnerables ya que están abiertas a todo el mundo por ello existe una gran dificultad al protegerlas.

4.      **¿Qué es el malware?** El malware es un tipo de [software](http://es.wikipedia.org/wiki/Software) que tiene como objetivo infiltrarse o dañar una [computadora](http://es.wikipedia.org/wiki/Computadora) o [sistema de información](http://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n) sin el consentimiento de su propietario. El gusano es un Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, y puede llevar virus o aprovechar bugs de los sistemas a los que conecta para dañarlos. Los caballos de Troya son instrucciones incluidas en un programa que simulan realizar tareas que se esperan de ellas, pero en realidad ejecutan funciones con el objetivo de ocultar la presencia de un atacante o para asegurarse la entrada en caso de ser descubierto.

5.    **¿Qué es un hacker? ¿De qué manera los hackers crean problemas de seguridad y dañan los SI?**  Un **hacker** es una persona que entra de forma no autorizada a computadoras y redes de computadoras. Su motivación varía de acuerdo a su ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo.

. Violan los candados de seguridad accediendo a la información privada, no dañan el sistema pero si agravian a la empresa.

6**.      ¿Crees que los defectos en software y en los datos causen perdidas en la productividad?** Obvio, porque todo defecto genera una sucesión de eventos inesperados que nos dan malos resultados en tareas o acciones, y si hay una falla en la colección de datos pude haber una perdida y generar un gran dolor de cabeza para la empresa.

7.      **¿Qué es un delito informático?** es toda aquella [acción, típica, antijurídica y culpable](http://es.wikipedia.org/wiki/Teor%C3%ADa_del_delito), que se da por vías informáticas o que tiene como objetivo destruir y dañar [computadoras](http://es.wikipedia.org/wiki/Ordenador), medios electrónicos y redes de Internet. No es bueno el hacer trampa por internet debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito.

Los **delitos informáticos** tienden a proliferar y evolucionar, lo que complica aun más la identificación y persecución de los mismos.

8**.      Proporciona dos ejemplos de delitos informáticos en los cuales las computadoras son objeto del delito y dos ejemplos en los cuales son instrumento para el delito.**

* **Ataques que se producen contra el derecho a la intimidad**
* **Pornografía infantil**
* **Amenazas**

### 9.      ¿Qué problemas de seguridad propician los empleados?

* Ingeniería social: consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
* Shoulder Surfing: consiste en "espiar" físicamente a los usuarios para obtener generalmente claves de acceso al sistema.
* Masquerading: consiste en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno.
* Basureo: consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo.
* Actos delictivos: son actos tipificados claramente como delitos por las leyes, como el chantaje, el soborno o la amenaza.
* Atacante interno: la mayor amenaza procede de personas que han trabajado o trabajan con los sistemas. Estos posibles atacantes internos deben disponer de los privilegio mínimo, conocimiento parcial, rotación de funciones y separación de funciones, etc.

10. **¿De qué manera afecta el software la confiabilidad y la seguridad de los Sistemas?** De muchas formas afecta pues el sistema debe tener los tres principios básicos que son:

* Confidencialidad: nadie no autorizado accede a la información.
* Fiabilidad: capacidad de recuperación
* Confidencialidad: proporcionar el servicio correcto
* Integridad: los datos enviados no se modifican en el camino.
* Disponibilidad: la recepción y acceso es correcto.
* Facilidad de mantenimiento: estabilidad y facilidad de modificación

Si alguno falla la seguridad está en peligro y puede haber perdidas enormes.