**C:\Users\Vlad\Pictures\upam.PNG**

**INGENIERÍA EN SOFTWARE IX**

**GRUPO: 1**

**TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN**

**CUESTIONARIO: VULNERABILIDAD.**

**ALUMNA: LIDIA SOLEDAD CORTÉS.**

**DOCENTE: GISELLE MONTERO GONZALES**

1. **¿Por qué son tan vulnerables los SI?** Son sistemas de información son vulnerables a la destrucción, mal uso, error, fraude y fallas que hay en el hardware o en software.

En el uso pueden ser vulnerables debido a la mala configuración de los sistemas informáticos, desconocimiento que los usuarios tienen sobre ellos.

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

Yo creo que las amenazas físicas debido a que las personas desconocen su funcionamiento y al no usarlos correctamente los pueden dañar fácilmente.

1. **¿Por qué están difícil proteger a Internet y a las redes Wi-Fi?** Porque son redes grandes y publicas y son vulnerables ya que están abiertas a todo tipo de personas.
2. **¿Qué es el malware?** El malware es un término general que se le da a todo aquel software que perjudica a la computadora. La palabra **malware** proviene del término en inglés **mal**icious soft**ware**, y en español es conocido con el nombre de código malicioso.
3. **¿Qué es un hacker? ¿De qué manera los hackers crean problemas de seguridad y dañan los SI?** Un hacker es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro Pueden penetrar a los sistemas violando su seguridad para realizar cualquier daño a esta información almacenada en los SI.
4. **¿Crees que los defectos en software y en los datos causen perdidas en la productividad?** Si porque si hay una mal software y por lo tanto una mala colección de datos esto no dará buenos resultados y no serán eficaces para los usuarios que consulten dicha información.
5. **¿Qué es un delito informático?** Un delito informático o ciberdelicuencia 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 [ordenadores](http://es.wikipedia.org/wiki/Ordenador), medios electrónicos y redes de Internet
6. **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.**

\*La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el [fraude](http://es.wikipedia.org/wiki/Fraude), el [robo](http://es.wikipedia.org/wiki/Robo), [chantaje](http://es.wikipedia.org/wiki/Chantaje), [falsificación](http://es.wikipedia.org/wiki/Falsificaci%C3%B3n) y la [malversación de caudales públicos](http://es.wikipedia.org/wiki/Malversaci%C3%B3n_de_caudales_p%C3%BAblicos) en los cuales ordenadores y redes han sido utilizados como medio.

\*Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, [Spam](http://es.wikipedia.org/wiki/Spam), ataques masivos a servidores de Internet y generación de virus

1. **¿Qué problemas de seguridad propician los empleados?**

* Ingeniería social: En la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían por ejemplo proporcionar información.
* Basureo: 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: Los posibles atacantes internos deben disponer de los privilegios mínimos y conocimiento sobre las funciones que se pueden realizar.
* Atacante externo: Se hace pasar por un usuario legítimo y acceder a la información.

1. **¿De qué manera afecta el software la confiabilidad y la seguridad de los Sistemas?**

Puede ser en cuanto a su integridad, Confidencialidad, Disponibilidad:

* Confidencialidad: Ya que no puede acceder ninguna persona que no cuente con ningún permiso a la información.
* Integridad: En que los datos que se van o se envían no tienen ninguna modificación.
* Disponibilidad: El acceso a los datos se realiza de manera correcta.