Presentación del trabajo

Aclaraciones:

- Trabajo grupal, máximo 4 integrantes por grupo.
- Deben respetarse los plazos de entrega y las condiciones definidas.
- El trabajo incluye como actividad final un coloquio oral entre todos los grupos.

Entregables:

- El Informe con los contenidos investigados debe ser presentado en formato Word y PDF con las siguientes características:
    - Debe contar con una carátula detallando::
        - Título del trabajo
        - Materia
        - Profesor
        - Alumnos
        - Fecha de presentación
        - Universidad
    - Debe incluir un índice de títulos principales.
    - Numeración pertinente para cada página.
    - Bibliografía y fuentes consultadas (Libros o sitios web, estos últimos con fecha de acceso y enlace completo)
- Al momento de la exposición del trabajo, se debe saber lo realizado en el trabajo del grupo y participar activamente del debate.

Fecha de entrega:

Fecha de presentación:

Puntos a resolver

1. ¿Qué se entiende por seguridad de los datos e información? Mencione las diferencias entre seguridad física y lógica.

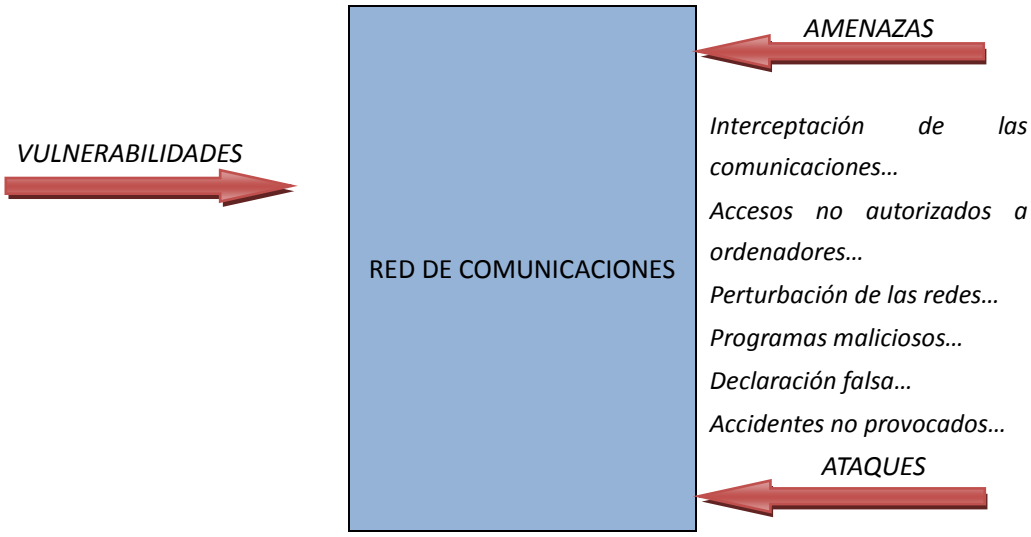
2. La seguridad se ha convertido en un factor primordial de cualquier red actual, defina y justifique con sus palabras en que se relacionan las siguientes oraciones con el concepto de "seguridad":
    a. En la actualidad predomina la propiedad y gestión privada de las redes.
    b. Las redes y los sistemas de información están en un proceso de convergencia.
    c. Las redes son internacionales.

3. Defina los siguientes conceptos básicos de seguridad utilizando sus palabras, recuerde siempre realizarlo en relación a la información y comunicación.
    a. Seguridad
    b. Bien
    c. Vulnerabilidad
    d. Amenaza
    e. Ataque

    ¿Qué debe protegerse en la industria de las telecomunicaciones hoy en día?

4. Existen 4 conceptos que en conjunto dan paso a una correcta gestión de seguridad, ellos son: *disponibilidad, autenticación, integridad y confidencialidad.* Defina a que se refiere cada uno de ellos en torno al mundo de la información y comunicación. Explique como se relacionan y actúan en conjunto.

5. En el siguiente gráfico se presentan algunos de los conceptos básicos de seguridad ya definidos, describa el gráfico de la manera más completa posible detallando cuales son las amenazas y ataques que figuran en dicho gráfico y de que se trata cada una de ellas.



6. Dimensión de la seguridad se entiende como un conjunto de tareas o actividades de seguridad creadas para tratar un punto específico de la seguridad de las redes. Generalmente se definen 8 d estas dimensiones, las cuales ustedes deben investigar y documentar de que se trata cada una.

- Control de acceso
- Autenticación
- No repudio
- Confidencialidad de los datos
- Seguridad de la comunicación
- Integridad de los datos
- Disponibilidad
- Privacidad

7. Habiendo definido ya todos los conceptos importantes de seguridad en torno a la información y comunicación, defina a que se refiere el concepto de "*Contingencia y respaldo de la información*". Busque en internet y redacte de manera resumida algún plan de respaldo de información.

8. ¿Qué se entiende por método de encriptación de la información? ¿Qué es una firma digital?

9. Describa los dos grandes grupos de métodos de encriptación denominados como: *clave secreta (simétrica) y clave pública (asimétrica)*. Explique de manera detallada el funcionamiento de ambos tipos de encriptación apoyándose con cuadros o imágenes.

10. ¿Qué es SSL y en donde se utiliza? Explique su funcionamiento de manera breve.

11. Entendiendo que se investigaron previamente los métodos de encriptación, describa los siguientes grupos de algoritmos de encriptación, detallando entre sus características si pertenecen a una encriptación simétrica o asimétrica.

- DES
- Diffie-Hellman
- RC5
- RSA
- IDEA
- 3DES
- AES
    - AES-CBC
    - AES-OFB
    - AES-CFB