**Cuestionario sobre Introducción a la Ciberseguridad**

**Docente: Carlos Castañeda Ramírez**

**Alumno: Rogelio Reveles Villegas**

**22 de Agosto de 2023**



1. **Defina que es la Seguridad:**

Es la forma de proteger la integridad y pertenencias propias o ajenas.

1. **Defina que es la Ciberseguridad:**

Es la aplicación de las Tecnologías, procesos y controles para proteger sistemas, redes, programas, dispositivos y datos de ciberataques.

1. **Cuál es el objetivo de la ciberseguridad?**

Su objetivo es reducir el riesgo de ciberataques y proteger contra la explotación no autorizada de tecnologías.

1. **¿Qué es la Criptografía Avanzada?**

Es el cifrado de información utilizando tokens.

1. **¿Qué elementos conforman la tríada de la ciberseguridad?**

Los elementos que conforman la tríada de la ciberseguridad son la confidencialidad, la integridad y la disponibilidad.

1. **Defina la Confidencialidad:**

Se encarga de garantizar que la información sea accesible sólo por personas autorizadas.

1. **Defina la Integridad:**

Es la que salvaguarda la integridad de la información, su exactitud y totalidad y los métodos de procesamiento y transmisión.

1. **Defina la Disponibilidad:**

Se encarga de garantizar que solo los usuarios autorizados tengan acceso a la información y a los recursos relacionados cada vez que lo requieran.

1. **Liste al menos 5 características de un riesgo de seguridad:**

* Activo
* Vulnerabilidad
* Amenaza
* Riesgo
* Impacto

1. **¿Qué es la Salvaguarda?**

Son las acciones llevadas a cabo para mitigar efectivamente las amenazas.

1. **Liste al menos 5 tipos de amenazas en la ciberseguridad:**

* Malware
* Phising
* Password Craking
* Covert Hardware
* Ramsonware

1. **¿Qué es Social Engineering en ciberseguridad?**

Es el intento de manipulación de las personas para que realicen acciones, cometan errores de seguridad o divulguen información confidencial.

1. **¿Qué es el Ransomware?**

Es un tipo de malware que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar la restricción.

1. **¿Qué es un Malware?**

Código utilizado para robar datos, evitar controles de acceso, ocasionar daños o comprometer un sistema de red e información.

1. **¿Qué es un DoS?**

El Denial of Service Attack se encarga de inundar los sistemas, redes o servidores con tráfico masivo, lo que hace que el sistema no pueda cumplir con las solicitudes legítimas.

1. **Describa que es un Hacker:**

Los hackers son personas con amplios conocimientos de informática, que explorar diversas técnicas para sobrepasar los controles de seguridad y explotar vulnerabilidades en redes y sistemas.

1. **Describa a un Black Hat Hacker:**

Son hackers causantes de ciberataques, utilizan su conocimiento para introducirse en los sistemas de manera maliciosa buscando beneficio personal o económico.

1. **Describa a un White Hat Hacker:**

Conocidos como Hackers Éticos, son aquellos hackers que utilizan sus conocimientos para encontrar vulnerabilidades en un sistema informático, y lo ponen en conocimiento de las compañías desarrolladoras o empresas, con el objetivo de poder estudiar y corregir los fallos.

1. **Describa a un Malicious Insider:**

Son personas con información privilegiada, pueden incluir empleados, proveedores externos, contratistas u otros socios comerciales.

1. **Liste a los 3 hackers más famosos:**

* Kevin Mitnick
* Jonathan James
* Albert Gonzales