Carrera de la Ciberseguridad

En este apartado descubriremos las diferentes carreras en la ciberseguridad.

Tarea 1: Introducción.

La carrera de la ciberseguridad cada vez es más demandada en el mundo informativo, y con un alto salario laboral. Existen diferentes puestos de trabajo en la ciberseguridad, como prueba de penetración ofensiva (PenTesting), hasta seguridad ofensiva (defender e investigar ciberataques).

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 2: Analista de Seguridad.

El analista de Seguridad es un rol muy importante y fundamental en el desarrollo de medidas de seguridad en todas las organizaciones y protegerlas de ataques de diferentes tipos.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 3: Ingeniería de Seguridad.

Los ingenieros de seguridad desarrollan e implementan sistemas de seguridad para proteger y evitar ataques de diferentes tipos, como ser ataques de sitios web, ataques a redes y proteger los datos sobre amenazas y vulnerabilidades.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 4: Respondedores de Incidencia.

Los equipos de respuestas e incidentes responden de forma productiva y eficiente a la brecha de seguridad, su responsabilidad incluye en la creación de planes, políticas y protocolos para que las organizaciones y empresas puedan implementar durante y después de un ataque.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 5: Examinador Forense Digital.

En este apartado brindó una frase, “Si te gusta ser Detective, este podría ser tu trabajo ideal”.
Si trabajas en un departamento público, con estas habilidades podrás centrarte en la recopilación de datos, para exonerar al inocente, encontrar y acusar al culpable.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 6: Analista de Malware.

El trabajo de un Analista de Malware consiste en el análisis de programas sospechosos y redactar un informe de manera simple para redactar lo encontrado. En este apartado el analista necesita un alto conocimiento en programación en especial en lenguajes de bajo nivel. El trabajo final es comprender el funcionamiento del programa malicioso y reportarlo.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 7: Tester de Penetración.

Es posible que alguna vez hayas escuchado nombrar el término pentesting o hacking ético. Son aquellos que prueban un sistema y su seguridad, y el software de la empresa para determinar si es seguridad o no, esto es logrado mediante intentos de fallos y vulnerabilidades mediante hacking sistematizados.
La empresa puede utilizar esta información para corregir problemas y prevenir un ciberataque real.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 8: Equipo Rojo.

El equipo rojo tiene un rol muy cercano al del Tester de Penetración que vimos en el apartado anterior, pero su función es más específica.
Los encargados de los equipos rojos se dedican en poner a prueba las capacidades de detección y respuesta de la empresa, esta función consiste en simular ataques de ciberdelincuentes conservando los datos de la empresa y evitar su detección.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 9: Cuestionario (Quiz).

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).