Incidentes de ciberseguridad

Para estos ejercicios, deberás elegir una organización o empresa (real o ficticia), para diseñar un plan de ciberseguridad. Los ejercicios se dividen en:

- **Política de seguridad**, donde se establecen las normas y procedimientos para proteger la información de la organización.
- **Plan de formación**, donde se establecen los cursos y capacitaciones que se deben realizar para que los empleados conozcan las políticas de seguridad.
- **Plan de evaluación**, donde se establecen los procedimientos para evaluar la efectividad de las políticas de seguridad.
- **Materiales de formación**, donde se crearán los materiales que se utilizarán en los cursos y capacitaciones.

El ejercicio se entregará en un repositorio con los informes y materiales desarrollados.

Política de seguridad

En este ejercicio deberás crear un informe que contenga la política de seguridad de la organización. La política de seguridad debe contener, entre otros, los siguientes puntos:

- **Introducción**, donde se de una descripción general de la organización elegida y se exponga la situación actual en materia de ciberseguridad.
- **Objetivos**, donde se establezcan los objetivos de la política de seguridad.
- **Alcance**, donde se defina el alcance de la política de seguridad, por ejemplo, si se aplica a todos los empleados de la organización o solo a un grupo específico.
- **Normas**, donde se establezcan las normas de seguridad que deben seguir los empleados.
- **Procedimientos**, donde se establezcan los procedimientos de seguridad que deben seguir los empleados.
- **Responsabilidades**, donde se establezcan las responsabilidades de los empleados en materia de seguridad.
- **Sanciones**, donde se establezcan las sanciones en caso de incumplimiento de las normas de seguridad, si las hay.
- **Revisión y actualización**, donde se establezca la periodicidad con la que se revisará y actualizará la política de seguridad.

Plan de formación

En este ejercicio deberás crear un informe que contenga el plan de formación de la organización. El plan de formación debe contener, entre otros, los siguientes puntos:

- **Introducción**, donde se de una descripción general de la organización y el plan de formación desarrollado.
- **Objetivos**, donde se establezcan los objetivos del plan de formación.
- **Contenidos**, donde se establezcan los contenidos de los cursos y capacitaciones que se deben realizar.
- **Metodología**, donde se establezca la metodología que se utilizará en los cursos y capacitaciones, por ejemplo, si serán presenciales o a distancia, si se usarán plataformas de e-learning o se realizarán simulaciones, etc.
- **Materiales**, donde se establezcan los materiales que se utilizarán en los cursos y capacitaciones.

Plan de evaluación

En este ejercicio deberás crear un informe que contenga el plan de evaluación de la organización. El plan de evaluación debe contener, entre otros, los siguientes puntos:

- **Introducción**, donde se de una descripción general de la organización y el plan de evaluación desarrollado.
- **Objetivos**, donde se establezcan los objetivos del plan de evaluación.
- **Indicadores**, donde se establezcan los indicadores que se utilizarán para evaluar la efectividad de las políticas de seguridad.
- **Procedimientos**, donde se establezcan los procedimientos que se utilizarán para evaluar la efectividad de las políticas de seguridad.
- **Responsables**, donde se establezcan los responsables de llevar a cabo la evaluación de las políticas de seguridad.
- **Frecuencia**, donde se establezca la frecuencia con la que se llevará a cabo la evaluación de las políticas de seguridad.
- **Informes**, donde se establezca la forma en que se presentarán los informes de evaluación de las políticas de seguridad.
- **Acciones correctivas**, donde se establezcan las acciones correctivas que se tomarán en caso de detectarse incumplimientos de las políticas de seguridad.

El plan de evaluación debe incluir, además, una campaña de **phishing** para evaluar la concienciación de los empleados en materia de ciberseguridad. La campaña de phishing debe incluir, al menos, los siguientes puntos:

- **Objetivos**, donde se establezcan los objetivos de la campaña de phishing.
- **Contenidos**, donde se establezcan los contenidos de los correos electrónicos de phishing que se enviarán a los empleados.
- **Metodología**, donde se establezca la metodología que se utilizará para llevar a cabo la campaña de phishing.
- **Resultados**, donde se establezcan los resultados de la campaña de phishing y las acciones correctivas que se tomarán en caso de detectarse incumplimientos de las políticas de seguridad.

Materiales de formación

Desarrolla material de formación para los empleados de la organización. Este material puede ser:

- **Presentaciones**, que se utilizarán en los cursos y capacitaciones.
- **Manuales**, que se entregarán a los empleados para que los consulten en caso de dudas.
- **Ejercicios**, que se utilizarán para evaluar el conocimiento de los empleados.
- **Simulaciones y labs**, que se utilizarán para que los empleados practiquen situaciones reales de ciberseguridad.