Título:	CIBERSEGURIDAD PARA EMPRESAS	Código:	CAP-CYBERSEG/2024
Elaboró:	Capacitaciones y RRHH	Versión	1.3
Revisó:	Dirección y Gerencia de RRHH.	Fecha:	18/06/2024
Aprobó	Dirección General	Página:	1 de 2

CIBERSEGURIDAD.

Propósito.

Este documento establece los lineamientos y objetivos del presente curso. En este curso, exploraremos los conceptos y técnicas de ciberseguridad para proteger los activos digitales de la empresa, incluyendo la información confidencial, los sistemas y la infraestructura.

Objetivos.

1. Comprender los conceptos básicos de ciberseguridad y sus aplicaciones en la empresa.
2. Identificar los riesgos y amenazas de ciberseguridad que enfrenta la empresa.
3. Aprender técnicas y estrategias para proteger los activos digitales de la empresa.
4. Desarrollar habilidades para implementar medidas de ciberseguridad en la empresa.
5. Aprender a responder a incidentes de ciberseguridad y a minimizar sus efectos.

Módulo 1: Introducción a la Ciberseguridad.

- Definición de ciberseguridad y sus objetivos.
- Importancia de la ciberseguridad en la empresa.
- Marco teórico de la ciberseguridad.

Módulo 2: Riesgos y Amenazas de Ciberseguridad.

- Identificación de los riesgos y amenazas de ciberseguridad.
- Análisis de las causas y consecuencias de los riesgos y amenazas.
- Estrategias para mitigar los riesgos y amenazas.

Módulo 3: Protección de los Activos Digitales.

- Implementación de medidas de seguridad para proteger los activos digitales.
- Uso de firewalls, antivirus y otros sistemas de seguridad.

- Configuración de sistemas de autenticación y autorización.

Módulo 4: Respuesta a Incidentes de Ciberseguridad.

- Identificación de incidentes de ciberseguridad.

- Análisis de incidentes de ciberseguridad.

- Respuesta a incidentes de ciberseguridad y minimización de sus efectos.

Módulo 5: Implementación de una Estrategia de Ciberseguridad.

- Desarrollo de una estrategia de ciberseguridad para la empresa.

- Implementación de la estrategia de ciberseguridad.

- Monitoreo y evaluación de la estrategia de ciberseguridad.

Metodología de Implementación.

- Clases en línea o presenciales.

- Videos y presentaciones.

- Actividades y ejercicios prácticos.

- Discusiones en grupo y trabajo en equipo.

Duración.

- 40 horas de clase en línea o presencial

- 20 horas de práctica y ejercicio

Público objetivo.

- Empleados de la empresa

- Profesionales de seguridad informática

- Administradores de sistemas y redes.

Certificado.

- Se otorgará un certificado de finalización del curso a los participantes que completen todos los módulos y actividades.

Recursos.

- Libros y manuales de ciberseguridad.

- Software y herramientas de seguridad informática.

- Recursos en línea y comunidades de profesionales de ciberseguridad.