

TEMAS

Módulo 1

Conceptos Fundamentales de la Ciberseguridad

Introducción a la ciberseguridad

Diferencia entre seguridad de información y ciberseguridad

Objetivos, roles y dominios de ciberseguridad

Gestión de Riesgos según ISO 31000:2018

Políticas y procedimientos de ciberseguridad

Tipos de ataques cibernéticos comunes

ISO 27032:2012

ISO 27002:2013

COBIT 2019

Certificaciones internacionales

Taller: Identificación de activos de información y riesgos de ciberseguridad

Producto: Matriz de riesgos y controles de ciberseguridad

Módulo 2

Descripción General del Marco de Ciberseguridad

Descripción General del Marco

Gestión de riesgos y el marco de ciberseguridad

Conceptos básicos sobre el marco

Núcleo de marco

Funciones

Categorías

Sub Categorías

Las cinco funciones básicas del marco

Niveles de implementación del marco

Perfil del marco

Revisión básica de las prácticas de ciberseguridad

Establecimiento o mejora de un programa de ciberseguridad

Comunicación de requisitos de ciberseguridad a las partes interesadas

Metodología para proteger la privacidad y las libertades civiles

Autoevaluación del riesgo de seguridad cibernética con el marco

Taller: Elaboración de Programa de Ciberseguridad

Producto: Programa de ciberseguridad de una organización

Módulo 3

Medidas de seguridad en la red, sistemas, aplicaciones y datos para proteger las organizaciones ante ataques cibernéticos.

Visión general de la arquitectura de seguridad

Modelo OSI. Defensa en profundidad

Controles de proceso - Gestión de la vulnerabilidad

Controles de proceso - Pruebas de penetración

Seguridad de la red

Seguridad del sistema operativo

Seguridad de las aplicaciones

Seguridad de datos

Análisis forense

Recuperación de desastres y planes de continuidad del negocio

Taller: Herramientas para la identificación de vulnerabilidades en el entorno tecnológico

Taller: Elaboración de política y plan de continuidad del negocio

Producto: Informe de vulnerabilidades de plataformas tecnológicas

Módulo 4

Introducción a la auditoría de ciberseguridad según la ISO 19011:2018

Normativa aplicable a la auditoría. Perfil del auditor

Normativas de apoyo para auditar la Ciberseguridad

Planificación, revisión de documentación y preparación de la auditoría

Ejecución de la auditoría

Informe de auditoría

No conformidades de la auditoría. Acciones correctivas

Ejemplos de Observaciones relacionadas a la Ciberseguridad

Taller: Elaborar un programa de auditoría de ciberseguridad y presupuesto de auditoría

Taller: Elaboración de informe de auditoría de ciberseguridad

Producto: Informe de Auditoría de Ciberseguridad

Producto Final: Informe de Estado Situacional de la Ciberseguridad en una organización