# TECNICO EN SEGURIDAD INFORMATICA

Este conjunto de materiales didácticos permitirá al alumnado adquirir las competencias profesionales necesarias para conocer el concepto y modelos de seguridad, los tipos de control de acceso, autentificación de datos y posibles ataques a los que pueden estar sometidos los sistemas informáticos, aprender las pautas y ámbitos de aplicación para el Reglamento de Seguridad y la aplicación de sus principales puntos del reglamento en Windows, saber aplicar la ley de protección de datos aplicada en España: los principios de protección de datos y la forma en que se debe aplicar, así como garantizar la continuidad de las operaciones de los elementos críticos que componen los sistemas de información, mediante acciones y procedimientos.

## CONTENIDO DEL CURSO:

MÓDULO 1. SEGURIDAD INFORMATICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS
Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
Salvaguardas y tecnologías de seguridad más habituales
La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO
Identificación de procesos de negocio soportados por sistemas de información
Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS
Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
Metodologías comúnmente aceptadas de identificación y análisis de riesgos
Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD
Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio
Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
Principios generales de protección de datos de carácter personal
Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS
Determinación de los perímetros de seguridad física
Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
Elaboración de la normativa de seguridad física e industrial para la organización
Sistemas de ficheros más frecuentemente utilizados
Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
Configuración de políticas y directivas del directorio de usuarios
Establecimiento de las listas de control de acceso (ACLs) a ficheros
Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
Sistemas de autenticación de usuarios débiles, fuertes y biométricos
Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS
Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

UNIDAD DIDÁCTICA 8. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
Definición de reglas de corte en los cortafuegos
Relación de los registros de auditoría del cortafuegos necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
Establecimiento de la monitorización y pruebas de los cortafuegos

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN
Introducción al análisis de riesgos
Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
Particularidades de los distintos tipos de código malicioso
Principales elementos del análisis de riesgos y sus modelos de relaciones
Metodologías cualitativas y cuantitativas de análisis de riesgos
Identificación de los activos involucrados en el análisis de riesgos y su valoración
Identificación de las amenazas que pueden afectar a los activos identificados previamente
Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
Determinación de la probabilidad e impacto de materialización de los escenarios
Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
Relación de las distintas alternativas de gestión de riesgos
Guía para la elaboración del plan de gestión de riesgos
Exposición de la metodología NIST SP 800-30
Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS
Herramientas del sistema operativo tipo Ping, Traceroute, etc.
Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
Herramientas de análisis de vulnerabilidades tipo Nessus
Analizadores de protocolos tipo WireShark, DSniff, Cain Abel, etc.
Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 11. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS
Principios generales de cortafuegos
Componentes de un cortafuegos de red
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
Arquitecturas de cortafuegos de red
Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN
Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
Guía para la elaboración del plan de auditoría
Guía para las pruebas de auditoría
Guía para la elaboración del informe de auditoría