



SEGURIDAD EN DISPOSITIVOS (II)

45 HORAS

criteria





SEGURIDAD EN DISPOSITIVOS (II)

Hoy en día la seguridad en dispositivos electrónicos es un componente esencial de la estrategia general de ciberseguridad de una empresa, vital para proteger sus activos, cumplir con las regulaciones, y mantener la confianza y la operatividad del negocio

Esta formación va dirigida a diferentes personas dentro de la organización, ya que la seguridad es una responsabilidad compartida; personal de TI y ciberseguridad, ejecutivos y directivos, empleados de servicios generales así como personal de diferentes departamentos como RRHH y marketing y ventas.





CURSOS

Compartición segura de datos personales

Cuidado de la privacidad propia y ajena

Sistema de navegación privada y comunicación encriptada

Mantenimiento de la cadena de custodia y veracidad de la información

Identificación y actuación ante los riesgos para la salud

Reglas y configuraciones para el ahorro de energía en dispositivos móviles



COMPARTICIÓN SEGURA DE DATOS PERSONALES

7,5 HORAS

OBJETIVOS

- Aprender a compartir los datos personales de forma segura en el entorno digital para evitar riesgos.

CONTENIDOS

- Compartición segura de datos personales
- La huella digital
- Responsabilidad individual
- ¿Qué puedo hacer para protegerme?
- Utilizar un software de seguridad
- Examinar antes de hacer clic en los enlaces
- No compartir información personal sensible
- Utilizar una conexión segura
- Sitios web no seguros
- Sencillas mejoras en la seguridad
- Educación y concienciación
- Ejemplos de programas o recursos



CUIDADO DE LA PRIVACIDAD PROPIA Y AJENA

7,5 HORAS

OBJETIVOS

- Establecer medidas de privacidad propia y ajena para el intercambio de datos.

CONTENIDOS

- Compartición segura de datos personales propios y ajenos
- ¿Qué es la compartición segura de datos?
- Los términos de servicio y las políticas de privacidad
- Compartir información personal sensible
- La privacidad de las cuentas en las redes sociales
- Configurar las opciones de privacidad
- Poner en valor nuestra privacidad
- Usar aplicaciones y programas de seguridad en dispositivos móviles y ordenadores
- Los correos electrónicos y mensajes de texto sospechoso
- Respetar la privacidad de los demás
- El consentimiento
- Evaluar si realmente se necesita compartir información personal
- Las últimas tendencias en seguridad y privacidad



SISTEMA DE NAVEGACIÓN PRIVADA Y COMUNICACIÓN ENCRIPTADA

7,5 HORAS

OBJETIVOS

- Aprender sistemas de navegación privada y comunicación encriptada para un intercambio de datos más seguro.

CONTENIDOS

- Conceptos y elementos de privacidad y seguridad en línea; Navegar sin dejar rastro, Herramientas de acceso a la información
- Dirección IP, Buscadores, Navegadores
- Sistemas de navegación privada
- Introducción a los sistemas de navegación privada: Cómo funcionan; Cómo configurarlos y utilizarlos
- Herramientas de encriptación
- Introducción a las herramientas de encriptación: Cómo funcionan, Qué ventajas ofrecen, Cómo configurarlas y utilizarlas
- Seguridad en el navegador: Cómo proteger la privacidad y seguridad en el navegador
- 6. Comunicaciones seguras; Cómo proteger la privacidad y seguridad, Otras posibilidades de fácil acceso
- 7. Retirar información personal de Internet; La privacidad en línea y la retirada de información personal, Regulaciones actuales sobre la retirada de información personal



MANTENIMIENTO DE LA CADENA DE CUSTODIA Y VERACIDAD DE LA INFORMACIÓN

7,5 HORAS

OBJETIVOS

- Conocer el mantenimiento de la cadena de custodia y veracidad de la información para una navegación segura en el entorno digital.

CONTENIDOS

- Conceptos clave
- Control de acceso y registro de cambios; garantizar el control de acceso a los datos y registro, las modificaciones realizadas en un proceso
- Las técnicas y procedimientos para garantizar la integridad de los datos; técnicas y procedimientos para garantizar la integridad de los datos, registros y las copias de seguridad
- ¿Qué es la cadena de custodia? ¿Cuál es el procedimiento para mantener la Cadena de custodia, los requisitos específicos
- Auditorías y documentación; cómo llevar a cabo una auditoría para verificar la integridad de los datos y registros, introducción sobre la documentación necesaria para mantener la cadena de custodia
- 6. Tecnologías y herramientas para garantizar la cadena de custodia y veracidad de la información
- 7. Ejemplos de buenas prácticas en la cadena de custodia en la industria



IDENTIFICACIÓN Y ACTUACIÓN ANTE LOS RIESGOS PARA LA SALUD

7,5 HORAS

OBJETIVOS

- Conocer los riesgos para la salud que pueden suponer el uso en exceso de las Nuevas tecnologías de la información para evitarlos en nuestro día a día.

CONTENIDOS

- Identificación y actuación ante los riesgos para la salud
- Riesgos físicos
- Riesgos psicológicos
- Riesgos externos
- Ergonomía en el puesto de trabajo y con dispositivos móviles
- Puesto de trabajo
- Dispositivos móviles
- Medidas para la desconexión digital
- La inclusión digital
- Adicciones y trastornos psicológicos ante la exposición prolongada con RRSS, herramientas digitales y comunicaciones 2.0
- Adicción a los dispositivos
- Adicción a las tecnologías



REGLAS Y CONFIGURACIONES PARA EL AHORRO DE ENERGÍA EN DISPOSITIVOS MÓVILES

7,5 HORAS

OBJETIVOS

- Conocer el impacto ambiental que pueden suponer el uso de las tecnologías digitales para así poder establecer medidas de ahorro y eficiencia en el uso de los dispositivos.

CONTENIDOS

- Reglas y configuraciones para el ahorro de energía en dispositivos móviles
- Cómo alargar la vida de los dispositivos
- Clasificación de los dispositivos según su impacto ambiental
- Protocolos de reciclaje de dispositivos eléctricos y electrónicos
- Sistemas colectivos de Responsabilidad Ampliada del Productor
- Cadena de reciclaje
- Puntos de entrega de los Residuos electrónicos y eléctricos



criteria

CON COBERTURA A NIVEL NACIONAL

