IFCT160. Directrices de seguridad para garantizar la protección de redes y sistemas de información en el entorno empresarial

Sku: PC862

Horas: 20

Formato: HTML

OBJETIVOS

Aplicar las herramientas y estrategias de ciberseguridad para el desarrollo de una cultura de seguridad en una organización, la protección al cliente y en la contratación de proveedores

CONTENIDOS

• Unidad 1: Ciberseguridad: concepto y contexto normativo

? Para comenzar

? En esta lección introductoria exploraremos la importancia de la ciberseguridad en el entorno empresarial

? Descubriremos qué riesgos enfrentan las organizaciones, por qué es crucial proteger la información y qué temas se tratarán a lo largo de la unidad

? Al finalizar esta lección, tendrás una visión general sobre cómo la ciberseguridad puede marcar la diferencia en el éxito y la continuidad de cualquier empresa

? Este es solo el punto de partida para sumergirte en conceptos, buenas prácticas y normativas esenciales para proteger redes y sistemas de información

? Conocimientos básicos sobre seguridad de los sistemas de información

? Establecimiento de los fundamentos esenciales de la ciberseguridad en el entorno empresarial

? Aprendizaje de los conceptos clave, como la triada CIA (Confidencialidad, Integridad y Disponibilidad), así como los riesgos, amenazas y vulnerabilidades más habituales

? Conocimiento de las principales estrategias de defensa y la importancia de la ciberseguridad como factor estratégico para cualquier organización

? Al finalizar esta lección, estarás preparado para identificar amenazas clave, comprender por qué la seguridad de la información es indispensable en la empresa moderna, y sentarás las bases para especializarte en la protección de redes y sistemas informáticos

? Buenas prácticas de seguridad y la Triada CIA

? Exploración en profundidad de las mejores prácticas para garantizar la seguridad de la información en las organizaciones

? Análisis de cómo la implementación de contraseñas robustas, actualizaciones periódicas, segmentación de redes, protección de datos, gestión de incidentes y formación de usuarios contribuyen a una estrategia sólida de ciberseguridad

? Profundización en la Triada CIA (Confidencialidad, Integridad, Disponibilidad), sus implicaciones en el entorno empresarial y las medidas para asegurar cada uno de estos pilares fundamentales

? Manejo del contexto normativo que afecta a la ciberseguridad en el entorno empresarial

? Exploración de los principales marcos normativos y estándares internacionales que regulan la ciberseguridad en el entorno empresarial

? Revisión de los conceptos clave, la importancia de cumplir con dichas normativas, y cómo adaptar los marcos existentes (como ISO/IEC 27001 y NIST) a las necesidades específicas de cada empresa

? Análisis de normas complementarias como GDPR y PCI-DSS, así como los procesos de evaluación de riesgos y certificación

? Inclusión de explicaciones detalladas, infografías y actividades para desarrollar una comprensión profunda y aplicada del contexto normativo de la ciberseguridad empresarial

? Evaluación de riesgos y auditoría

? Profundización en los procesos fundamentales para la protección de los sistemas de información corporativos: la evaluación de riesgos y la auditoría

? Aprendizaje para identificar, analizar y priorizar riesgos de ciberseguridad, conocer las metodologías más utilizadas internacionalmente, y comprender cómo las auditorías contribuyen a la mejora continua y el cumplimiento normativo en las empresas

? Recursos gráficos, ejercicios interactivos y ejemplos prácticos que te permitirán consolidar tu aprendizaje y aplicar los conceptos a tu entorno profesional

? Ejercicio práctico de libre expresión escrita

? Oportunidad de poner en práctica tus conocimientos adquiridos sobre ciberseguridad en el entorno empresarial

? Mediante ejercicios de libre expresión, podrás reflexionar, investigar y argumentar sobre situaciones reales o hipotéticas, aplicando creatividad y un enfoque crítico

? Aprovecha este espacio para consolidar tus competencias clave en la protección de redes y sistemas de información, así como en la gestión de riesgos y el cumplimiento normativo

? Role playing y estado de avance

? Lección de repaso para consolidar los conceptos clave sobre ciberseguridad, buenas prácticas y el marco regulatorio que has estudiado en la unidad

? Comenzarás con una ronda interactiva de tarjetas para refrescar tus conocimientos principales, y luego te enfrentarás a un escenario de role play donde pondrás en práctica lo aprendido en una situación realista dentro de una empresa

? Este repaso te permitirá afianzar tu preparación antes de avanzar hacia la evaluación de la unidad

? Evaluación de la unidad

? Prueba para medir tus conocimientos sobre los temas tratados en la unidad: ciberseguridad, buenas prácticas, contexto normativo, evaluación de riesgos y auditoría

? Responde las preguntas cuidadosamente para comprobar tu comprensión y detectar áreas de mejora

• Unidad 2: Técnicas y recursos para la seguridad

? Para comenzar

? Lección introductoria para conocer los conceptos clave relacionados con la protección de redes, sistemas de información y los recursos más importantes para garantizar la seguridad en el entorno empresarial

? Descubrirás por qué este tema es esencial, cómo afectan las amenazas digitales a cualquier organización y de qué formas te puedes preparar para enfrentarlas

? Utilización de técnicas y recursos para la seguridad en la organización

? Estudio en profundidad de las principales técnicas y recursos para proteger redes y sistemas en el entorno empresarial

? Exploración del funcionamiento, la implementación y los beneficios de herramientas esenciales como firewalls, VPNs, IDS/IPS, además de estrategias de gestión de accesos y autenticación, y defensa frente a malware y ciberataques

? Gestión de incidentes de seguridad

? Exploración en profundidad de la gestión de incidentes de seguridad informática dentro de las organizaciones, abordando desde su importancia, la planificación y preparación, los protocolos de respuesta y recuperación, hasta el papel crucial de la mejora continua y la formación del personal

? Análisis de los elementos clave de un plan de respuesta, los pasos prácticos para afrontar un incidente y cómo alinearse con las regulaciones exigidas

? Lección esencial para preparar a cualquier profesional o responsable de la seguridad en el entorno empresarial, ayudando a proteger los activos críticos de la empresa y minimizar los impactos de los ataques cibernéticos

? Concienciación y formación en ciberseguridad

? Aprendizaje de por qué la concienciación y la formación en ciberseguridad constituyen el pilar fundamental de la protección de redes y sistemas dentro de la empresa

? Estudio de cómo la evolución de las amenazas cibernéticas exige una formación continua, detallando las competencias técnicas y organizativas esenciales, y profundizando en el papel central de los empleados en la protección de la información

? Estrategias prácticas para fomentar una cultura de seguridad y reducir los riesgos derivados del error humano

? Comprensión de cómo convertir a cada miembro de la organización en un agente activo de seguridad y resiliencia frente a los ciberataques

? Ejercicio práctico de libre expresión escrita

? Oportunidad de aplicar los conocimientos adquiridos a lo largo de la unidad sobre técnicas y recursos para la seguridad en el entorno empresarial

? A través de actividades de libre expresión escrita, podrás reflexionar sobre situaciones reales, proponer estrategias de protección y desarrollar tu punto de vista de forma creativa y argumentada

? Este ejercicio te ayudará a consolidar tu aprendizaje y a conectar la teoría con tu realidad profesional o académica

? Role playing y estado de avance

? Lección de repaso para consolidar los conocimientos adquiridos durante la unidad sobre técnicas y recursos clave para garantizar la seguridad en redes y sistemas de información empresariales

? Refuerzo de conceptos esenciales mediante tarjetas didácticas interactivas y práctica de lo aprendido en situaciones simuladas de la vida real a través de actividades de role play

? El objetivo es fortalecer tu comprensión, detectar posibles lagunas y adquirir mayor confianza antes de proceder a la evaluación final de la unidad

? Evaluación de la unidad

? Evaluación para comprobar tus conocimientos sobre las principales técnicas y recursos para la seguridad de redes y sistemas en el entorno empresarial, incluyendo la gestión de incidentes, la conciencia en ciberseguridad y el rol de los empleados en la protección de la información

• Evaluación final: Evaluación final

? Evaluación final

? Prueba para evaluar tus conocimientos y competencias adquiridos en el curso

? La evaluación abarca los conceptos clave, buenas prácticas, normativas, gestión de riesgos, respuesta a incidentes y cultura de seguridad

? Responde cuidadosamente cada pregunta, aplicando lo aprendido en situaciones reales y teóricas del entorno empresaria