Hábilon elearning

CONTENIDO

SEGURIDAD DIGITAL EMPRESARIAL ESENCIAL

CÓDIGO	AUTOR	DURACIÓN ESTIMADA	NIVEL DE FORMACIÓN
01B09C02	Yolanda Corral	15 h	Medio

Dirigido a

Profesionales de pymes y empresas que utilicen información, cuentas, dispositivos y servicios digitales en su actividad diaria y necesiten adquirir hábitos esenciales de seguridad empresarial.

Descripción

Con este contenido de curso profesional el alumnado aprenderá los fundamentos necesarios para proteger la información y los accesos en la actividad empresarial. Se priorizarán la responsabilidad individual, las contraseñas y la autenticación multifactor, la identificación de fraudes y amenazas habituales y la protección de información sensible en situaciones de movilidad y teletrabajo.

COMPETENCIAS

1. Reconocer y asumir la responsabilidad individual en la seguridad digital empresarial, aplicando hábitos seguros en el puesto de trabajo para proteger sus activos de información.
2. Aplicar buenas prácticas de autenticación y gestión de accesos corporativos para proteger las credenciales, evitar accesos no autorizados y garantizar un uso adecuado de los recursos de la organización.
3. Identificar fraudes y amenazas digitales dirigidos a la organización, aplicando criterios de verificación antes de realizar acciones que puedan comprometer la información, los recursos o la actividad empresarial.
4. Manejar la información sensible y aplicar pautas de seguridad en movilidad y teletrabajo para evitar pérdidas, fugas o accesos no autorizados fuera del entorno corporativo habitual.

CRITERIOS DE EVALUACIÓN (Objetivos)

1. Identificar riesgos digitales habituales en la actividad profesional, relacionándolos con los principios de confidencialidad, integridad y disponibilidad de la información. Diferenciar hábitos seguros e inseguros en el puesto de trabajo, identificando aquellos que puedan aumentar o reducir la exposición a riesgos de seguridad. Comprender el modelo de responsabilidad compartida y el papel del empleado en la protección de la organización.

2. Aplicar pautas para crear y utilizar contraseñas robustas y únicas, evitando su reutilización y utilizando mecanismos seguros para su gestión. Utilizar la autenticación multifactor (MFA) de forma habitual y reaccionar y actuar de manera preventiva ante solicitudes de autenticación inesperadas o intentos de fatiga de MFA. Aplicar el principio de mínimo privilegio en la gestión de permisos y accesos corporativos, evitando el uso compartido de credenciales y favoreciendo la trazabilidad de las acciones.
3. Reconocer señales características de phishing, smishing, vishing, qrishing y otros fraudes digitales habituales en el entorno profesional. Diferenciar comunicaciones legítimas de intentos de engaño, aplicando criterios de contraste sobre remitentes, dominios, enlaces, archivos adjuntos, solicitudes y otros elementos de la comunicación. Aplicar pautas de verificación mediante canales seguros antes de responder, descargar archivos, ejecutar software o autorizar operaciones financieras o bancarias.
4. Clasificar la información empresarial según su nivel de sensibilidad y aplicar las medidas de protección, cifrado y restricción de acceso correspondientes. Identificar riesgos de interceptación o exposición asociados al uso de conexiones no seguras, especialmente mediante redes Wi-Fi públicas o abiertas, en situaciones de movilidad o teletrabajo. Aplicar medidas preventivas en entornos de trabajo remoto, utilizando los mecanismos de seguridad establecidos por la organización, como VPN corporativa, cifrado de dispositivos y separación de los usos personal y profesional.

CONTENIDOS

Unidad 1. Cultura de seguridad digital en la empresa y responsabilidad en la empresa
1. Seguridad de la información en la actividad empresarial
    1.1. Triada CID: Confidencialidad, integridad y disponibilidad de la información
2. El papel del empleado en la seguridad digital
    2.1. Hábitos seguros e inseguros en el puesto de trabajo
3. Responsabilidad compartida en la organización

Unidad 2. Contraseñas, autenticación y gestión segura de accesos corporativos
1. Protección y gestión de credenciales.
    1.1. Buenas prácticas de uso de contraseñas
    1.2. Gestores de contraseñas y almacenamiento seguro de credenciales
2. Autenticación multifactor (MFA)
    2.1. Métodos de autenticación multifactor y buenas prácticas de uso
    2.2. Detección y respuesta ante solicitudes de autenticación sospechosas
3. Gestión segura de accesos corporativos
    3.1. Principio de mínimo privilegio y asignación de permisos
    3.2. Cuentas compartidas, trazabilidad y gestión de sesiones
    3.3. Ciclo de vida de los accesos: altas, cambios y bajas

Unidad 4. Riesgos y amenazas: phishing, ransomware y fraudes empresariales
1. Fraudes digitales habituales en la empresa
    1.1. Phishing mediante correo electrónico corporativo

1.2. Smishing y mensajería instantánea
1.3. Qrishing mediante códigos QR
1.4. Vishing y llamadas de suplantación
2. Suplantación y fraude en las relaciones empresariales
2.1. Estafas BEC: fraude del CEO, suplantación de directivos y proveedores
2.2. Solicitudes fraudulentas: pagos, cambios de cuenta y peticiones de información
3. Ransomware y secuestro de información
3.1. Vías de entrada y consecuencias del ransomware
3.2. Extorsión y exposición de información robada
4. Verificación antes de actuar

Unidad 5. Protección de información sensible, teletrabajo y conexiones seguras
1. Clasificación y protección de la información.
1.1. Niveles de sensibilidad: pública, uso interno, confidencial y restringida o crítica
1.2. Medidas de protección, cifrado y prevención de fugas de información
2. Ciberseguridad en movilidad y teletrabajo
2.1. Conexiones seguras y redes no confiables
2.2. Dispositivos corporativos, BYOD y separación de usos personal y profesional
2.3. Protección de dispositivos e información en movilidad y espacios públicos