Hábilon elearning

CONTENIDO

PROTECCIÓN DE INFORMACIÓN Y HERRAMIENTAS DIGITALES

CÓDIGO	AUTOR	DURACIÓN ESTIMADA	NIVEL DE FORMACIÓN
01B09C04	Yolanda Corral	15 h	Medio

Dirigido a

Profesionales que gestionen datos, documentos, correo, aplicaciones, servicios cloud o herramientas de IA y necesiten proteger la información corporativa y los accesos en su actividad diaria.

Descripción

Con este contenido de curso profesional el alumnado aprenderá a proteger accesos, información y herramientas digitales en contextos presenciales y remotos. Se priorizarán la autenticación segura, los permisos en correo y entornos colaborativos, el uso responsable de IA y aplicaciones, la clasificación y protección de datos sensibles y la actuación ante posibles brechas de seguridad.

COMPETENCIAS

1. 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.
2. Utilizar el correo electrónico y las herramientas colaborativas aplicando hábitos de seguridad preventiva para reducir riesgos en comunicaciones, el intercambio de archivos y el trabajo compartido.
3. Usar herramientas digitales e inteligencia artificial de forma segura y responsable, protegiendo la información corporativa y respetando las aplicaciones y servicios autorizados por la organización.
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.
5. Comprender las obligaciones básicas en materia de protección de datos y seguridad de la información, identificando situaciones que puedan constituir una brecha de datos personales y comunicándolas a través de los canales establecidos.

CRITERIOS DE EVALUACIÓN (Objetivos)

1. 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.

2. Aplicar pautas seguras en el envío de correos electrónicos, verificando destinatarios, adjuntos y enlaces y utilizando la copia oculta (CCO) cuando sea necesario para proteger las direcciones de los destinatarios. Reconocer riesgos habituales en entornos colaborativos al compartir, editar o dar acceso a documentos, especialmente cuando intervienen usuarios externos a la organización. Configurar, revisar y revocar permisos de acceso al compartir carpetas o archivos con usuarios internos o externos, aplicando criterios de necesidad y mínimo acceso."
3. Identificar información confidencial o sensible que no debe introducirse en prompts de herramientas de IA públicas o chatbots externos, de acuerdo con las políticas de la organización. Reconocer los riesgos asociados al Shadow IT y al uso o instalación no autorizada de aplicaciones, extensiones de navegador y otros servicios o software. Aplicar pautas de uso seguro, ético y responsable de soluciones de IA corporativas y herramientas digitales, verificando los contenidos generados y respetando las políticas y condiciones de uso de la organización.
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.
5. Reconocer los principios fundamentales del RGPD y la LOPDGDD aplicados al tratamiento y manejo cotidiano de datos personales en el puesto de trabajo. Identificar situaciones que puedan constituir una brecha de seguridad de datos personales mediante supuestos prácticos del entorno laboral. Comprender la importancia de comunicar inmediatamente las posibles brechas de datos personales a través de los canales establecidos por la organización, de acuerdo con sus procedimientos y obligaciones legales.

CONTENIDOS

Unidad 1. 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 2. Uso seguro del correo y herramientas colaborativas

1. Uso seguro del correo corporativo
   1.1. Adjuntos, enlaces y verificación de remitentes
   1.2. Uso de CCO y prevención de exposición de información
2. Herramientas colaborativas e intercambio en la nube

2.1. Permisos de acceso, edición e invitación a participantes externos

Unidad 3. Uso seguro, ético y responsable de la IA y herramientas digitales

1. Riesgos en el uso de herramientas de IA públicas
   1.1. Fuga de información confidencial y propiedad intelectual en prompts
2. Shadow IT y software no homologado
   2.1. Extensiones de navegador y herramientas descargadas sin autorización
3. Pautas para un uso seguro, ético y responsable de la IA en la empresa

Unidad 4. 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

Unidad 5. Marco normativo, protección de datos y brechas de seguridad

1. Marco normativo básico de ciberseguridad y privacidad.
   1.1. RGPD y LOPDGDD: principios y obligaciones
   1.2. Nociones básicas del marco normativo de ciberseguridad: NIS2 y ENS
2. Protección de datos en el puesto de trabajo
3. Brechas de seguridad de datos personales
   3.1. Definición, tipos y supuestos prácticos de brecha
   3.2. Comunicación interna y actuación ante una posible brecha