Hábilon elearning

CONTENIDO

SEGURIDAD DIGITAL PARA TRABAJO HÍBRIDO

CÓDIGO	AUTOR	DURACIÓN ESTIMADA	NIVEL DE FORMACIÓN
01B09C05	Yolanda Corral	12 h	Medio

Dirigido a

Profesionales que alternen trabajo presencial, remoto o en movilidad y utilicen cuentas corporativas, correo, herramientas colaborativas, redes y dispositivos fuera del entorno habitual de la empresa.

Descripción

Con este contenido de curso profesional el alumnado aprenderá a aplicar medidas de seguridad en modalidades de trabajo híbrido. Se priorizarán la protección de credenciales y accesos, el uso seguro del correo y de los documentos compartidos, la seguridad física del puesto y la protección de información, conexiones y dispositivos durante el teletrabajo y la movilidad.

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. Aplicar hábitos de seguridad física y ambiental en el puesto de trabajo para proteger la información en diversos soportes, los dispositivos y los recursos de la organización frente a accesos o uso no autorizados.
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. 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. Aplicar pautas de mesas y pantallas limpias, bloqueando la sesión al alejarse del puesto de trabajo. Identificar riesgos de ingeniería social presencial y situaciones de acceso no autorizado de terceros a las instalaciones o al puesto de trabajo. Manejar y destruir adecuadamente documentación confidencial y dispositivos de almacenamiento extraíbles, aplicando las pautas establecidas por 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.

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. Medidas de seguridad en el entorno de trabajo presencial

1. Seguridad en el entorno físico de trabajo
   1.1. Políticas de mesas y pantallas limpias
   1.2. Bloqueo de sesión manual y automático

2. Control de accesos y presencia de terceros
    2.1. Ingeniería social presencial y acompañamiento de visitas (tailgating)
3. Custodia y destrucción segura de información y soportes

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