PROTECCIÓN, GESTIÓN DE RIESGOS Y CONTINUIDAD DIGITAL EN LA EMPRESA

CÓDIGO	AUTOR	DURACIÓN ESTIMADA	NIVEL DE FORMACIÓN
01B09C01	Yolanda Corral	35 h	Medio

Dirigido a

Profesionales de pymes y empresas que utilizan correo electrónico, documentos, aplicaciones, datos, herramientas colaborativas, soluciones cloud o IA en su actividad diaria. Especialmente personal de administración, ventas, atención al cliente, RRHH, operaciones, mandos intermedios y equipos transversales.

Descripción

Con este contenido de curso profesional el alumnado aprenderá a prevenir riesgos digitales habituales en la empresa, reconocer fraudes y suplantaciones, proteger información y accesos, utilizar herramientas digitales con criterios seguros, comunicar incidentes a tiempo y contribuir a la continuidad de la actividad mediante hábitos preventivos, protocolos internos y roles claros.

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. Proteger la identidad digital corporativa y personal, aplicando hábitos de prevención en la exposición pública de información corporativa.
3. 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.
4. Reconocer las dinámicas de manipulación utilizadas en las técnicas de ingeniería social y aplicar criterios de verificación antes de realizar acciones que puedan comprometer la seguridad de la organización.
5. 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.
6. Identificar señales de engaño y suplantación facilitadas por la inteligencia artificial, aplicando pautas de verificación reforzada ante comunicaciones o solicitudes de riesgo para evitar engaños altamente sofisticados.

7. 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.
8. 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.
9. 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.
10. 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.
11. Detectar señales iniciales de incidentes digitales para actuar con rapidez, evitar daños mayores y canalizar la situación por la vía oficial de reporte.
12. 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.
13. Comprender el papel de los protocolos de continuidad, las copias de seguridad y las medidas de contingencia para contribuir a la continuidad y recuperación de la actividad de la organización.
14. Elaborar un plan personal de mejora en seguridad digital para aplicar hábitos preventivos sostenibles en el puesto de trabajo.

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. Diferenciar los límites entre la identidad digital personal y profesional en redes sociales y plataformas digitales. Identificar los riesgos asociados a la sobreexposición de información corporativa o personal (oversharing) y su uso en ataques dirigidos. Aplicar pautas de cuidado de la huella digital para proteger la reputación propia y la imagen corporativa.
3. 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.
4. Reconocer los principales mecanismos de manipulación psicológica utilizados en los intentos de ingeniería social, como la urgencia, la autoridad, el miedo, la ilusión o la confianza. Identificar situaciones de riesgo en las que se induce a la acción rápida, al incumplimiento de procedimientos

internos o a la revelación de información corporativa. Aplicar el pensamiento crítico y pautas de verificación ante peticiones inusuales, imprevistas o sospechosas, respetando los procedimientos de seguridad de la organización.

5. 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.
6. Reconocer usos de la inteligencia artificial generativa que pueden facilitar la suplantación y la elaboración de contenidos engañosos, como la clonación de voz, los deepfakes y la generación de textos persuasivos. Identificar señales de riesgo en comunicaciones, contenidos o solicitudes aparentemente legítimos, especialmente cuando implican suplantación de personas, cambios de instrucciones o acciones sensibles que puedan derivar en daños para la organización. Aplicar pautas de verificación reforzada ante solicitudes críticas o situaciones en las que pueda existir suplantación mediante contenidos generados o manipulados con IA.
7. 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."
8. 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.
9. 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.
10. 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.

11. Identificar señales tempranas de compromiso e incidentes técnicos en equipos, cuentas de usuario o sistemas, como comportamientos anómalos, accesos inusuales o archivos cifrados. Aplicar primeras acciones de actuación y contención ante una sospecha de incidente, evitando alterar evidencias digitales o provocar daños secundarios. Notificar el incidente de forma rápida, clara y ordenada a través de los canales oficiales de reporte a los responsables internos o soporte técnico autorizado.
12. 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.
13. Reconocer la función de las copias de seguridad como medida de protección y recuperación frente a pérdidas de datos o incidentes como el ransomware. Identificar los roles internos, canales oficiales y pautas de comunicación establecidos durante una interrupción de la actividad. Reconocer medidas de contingencia y alternativas operativas ante la indisponibilidad temporal de sistemas, aplicaciones o información.
14. Analizar las vulnerabilidades, riesgos y hábitos digitales presentes en las tareas, herramientas y rutinas del puesto de trabajo, identificando las principales áreas de mejora. Elaborar un plan de mejora en seguridad digital, priorizando acciones y hábitos preventivos realistas y aplicables al puesto de trabajo, y diferenciando entre medidas inmediatas y actuaciones que requieren coordinación interna.

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. Identidad digital personal, profesional y corporativa

1. Identidad digital en el entorno profesional
    1.1. Identidad digital personal, profesional y corporativa
    1.2. Separación de entornos, cuentas y límites de uso
2. Huella digital y reputación profesional y corporativa
3. Buenas prácticas de protección
    3.1. Cuidado de la presencia digital profesional
    3.2. Protección y gestión de los activos de identidad digital corporativa

Unidad 3. 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. Ingeniería social y psicología del engaño

1. Principios de la ingeniería social.
    1.1. Psicología del engaño: urgencia, autoridad, miedo, escasez y simulación de confianza
2. Técnicas de manipulación y persuasión en el entorno profesional
3. Verificación antes de actuar
    3.1. Criterio de verificación y pensamiento crítico
    3.2. Comprobación de la legitimidad de las peticiones

Unidad 5. 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 6. Evolución de los engaños y amenazas en la era de la IA

1. Evolución de los engaños con inteligencia artificial generativa (IA)
    1.1. Suplantación de identidad: deepfakes de voz y vídeo en el entorno empresarial
    1.2. Perfiles falsos e identidades sintéticas en entornos profesionales
2. Perfeccionamiento de los ataques mediante IA
3. Verificación reforzada ante solicitudes de riesgo

Unidad 7. 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 8. 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 9. 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 10. 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 11. Detección inicial de incidentes digitales y gestión de crisis
1. Incidentes de seguridad digital
    1.1. Qué se considera un incidente de seguridad y sus principales tipos
    1.2. Señales iniciales: comportamientos anómalos, avisos inusuales y archivos bloqueados
    1.3. Accesos o acciones no autorizadas
2. Primeras acciones de actuación y contención
    2.1. Pasos clave de actuación: qué hacer y qué evitar en un incidente de seguridad
3. Comunicación, escalado y reporte de incidentes
4. Gestión de crisis y clasificación de incidentes según impacto y gravedad

Unidad 12. 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

Unidad 13. Protocolos internos, continuidad digital y copias de seguridad

1. Continuidad digital y resiliencia en la empresa
    1.1. Procesos críticos, roles internos y planes de continuidad
2. Copias de seguridad y recuperación de la información
3. Contingencia y continuidad de la actividad
    3.1. Alternativas operativas ante la indisponibilidad de sistemas o herramientas

Unidad 14. Plan de mejora de la seguridad digital en el puesto de trabajo

1. Autodiagnóstico de hábitos y conductas digitales en el puesto de trabajo
2. Priorización de mejoras de seguridad
    2.1. Acciones inmediatas de bajo esfuerzo
    2.2. Cambios que requieren coordinación interna
3. Rutinas de higiene digital en el puesto de trabajo
4. Plan personal de seguridad digital
    4.1. Compromisos de mejora y hábitos preventivos sostenible