Hábilon elearning

CONTENIDO

RESPUESTA Y CONTINUIDAD ANTE INCIDENTES DIGITALES

CÓDIGO	AUTOR	DURACIÓN ESTIMADA	NIVEL DE FORMACIÓN
01B09C06	Yolanda Corral	15 h	Medio

Dirigido a

Profesionales, mandos intermedios y equipos de pymes que necesiten detectar incidentes digitales, comunicarlos correctamente y contribuir a la continuidad y recuperación de la actividad empresarial.

Descripción

Con este contenido de curso profesional el alumnado aprenderá a actuar ante amenazas e incidentes digitales que puedan afectar a la organización. Se priorizarán la detección de fraudes y señales de compromiso, las primeras medidas de contención y reporte, las brechas de datos personales y los protocolos de continuidad, copias de seguridad y contingencia. El aprendizaje se trasladará a un plan personal de mejora aplicable al puesto de trabajo.

COMPETENCIAS

1. 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.
2. Detectar señales iniciales de incidentes digitales para actuar con rapidez, evitar daños mayores y canalizar la situación por la vía oficial de reporte.
3. 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.
4. 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.
5. Elaborar un plan personal de mejora en seguridad digital para aplicar hábitos preventivos sostenibles en el puesto de trabajo.

CRITERIOS DE EVALUACIÓN (Objetivos)

1. 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.

2. 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.
3. 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.
4. 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.
5. 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. 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 2. 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 3. 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 4. 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 5. 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