PROGRAMA DE CAPACITACIÓN CORPORATIVA

CURSO 5

Ciberseguridad y Protección de Datos para Empleados

Que el empleado reconozca y responda correctamente a las amenazas de seguridad que llegan a su puesto de trabajo, y maneje la información de la empresa y de terceros conforme a la política interna y al marco de protección de datos aplicable.

12 horas (3 sesiones de 4 h, o 6 de 2 h)

Modalidad in-company

Ficha técnica

Campo	Detalle
Duración	12 horas (3 sesiones de 4 h, o 6 de 2 h)
Modalidad	Presencial o virtual sincrónico. Escalable a cohortes grandes
Participantes	15 a 30 por cohorte
Perfil de entrada	Ninguno. Todo empleado con acceso a sistemas
Herramientas	Gestor de contraseñas, simulador de phishing, plataforma corporativa del cliente
Entregable final	Evaluación de conocimiento aprobada + compromiso de prácticas seguras firmado

Objetivo general

Que el empleado reconozca y responda correctamente a las amenazas de seguridad que llegan a su puesto de trabajo, y maneje la información de la empresa y de terceros conforme a la política interna y al marco de protección de datos aplicable.

Objetivos específicos

1. Identificar intentos de suplantación e ingeniería social, incluidos los generados con IA.
2. Aplicar prácticas correctas de autenticación y manejo de credenciales.
3. Clasificar la información según su sensibilidad y tratarla en consecuencia.
4. Reconocer y reportar un incidente dentro del tiempo requerido.
5. Cumplir las obligaciones básicas de protección de datos personales en su puesto.

Pensum detallado

Módulo 1 — Amenazas e ingeniería social (4 h)

1.1 El panorama real - Por qué el empleado es el objetivo principal y no el sistema - Costo de un incidente: operativo, legal y reputacional - Casos anonimizados del sector del cliente

1.2 Phishing y variantes - Correo fraudulento: señales de alerta - Suplantación de proveedores y de ejecutivos - Fraude de cambio de cuenta bancaria - Phishing por mensajería y por teléfono - Códigos QR maliciosos

1.3 Suplantación asistida por IA - Clonación de voz y video: qué es posible hoy - Por qué "reconocí su voz" ya no es verificación - Protocolo de verificación por canal alterno - Correos fraudulentos sin errores de redacción

1.4 Taller de detección - Ejercicio con 20 mensajes reales y falsos mezclados - Discusión de los criterios de decisión

Entregable: resultado del ejercicio de detección con análisis de los propios errores.

Módulo 2 — Higiene digital y manejo de información (4 h)

2.1 Credenciales - Por qué la reutilización de contraseñas es el problema central - Gestores de contraseñas: instalación y uso práctico - Autenticación de múltiples factores: tipos y cuál es más seguro - Fatiga de notificaciones de aprobación y cómo se explota

2.2 Dispositivos y conexiones - Actualizaciones y por qué no se posponen indefinidamente - Redes públicas y uso de VPN - Dispositivos personales con información de la empresa - Bloqueo de pantalla y seguridad física del puesto

2.3 Clasificación y manejo de información - Niveles: pública, interna, confidencial, restringida - Reglas de tratamiento por nivel - Compartición de archivos: enlaces, permisos y caducidad - Errores de destinatario y cómo prevenirlos - Almacenamiento no autorizado y TI en la sombra

2.4 IA y confidencialidad - Qué no debe ingresarse a herramientas de IA públicas - Diferencias de tratamiento de datos entre planes - Política interna de uso de IA

Entregable: gestor de contraseñas configurado + inventario personal de información sensible manejada.

Módulo 3 — Protección de datos, incidentes y evaluación (4 h)

3.1 Protección de datos personales - Qué constituye un dato personal y qué un dato sensible - Principios: finalidad, minimización,

exactitud, conservación limitada - Derechos de los titulares y cómo se atienden - Obligaciones del empleado en su puesto concreto - *Contenido a validar con asesoría legal local antes de cada cohorte*

3.2 Terceros y proveedores - Riesgo de la cadena de suministro - Qué revisar antes de compartir datos con un proveedor - Servicios en la nube no aprobados

3.3 Respuesta a incidentes - Qué constituye un incidente - Los primeros diez minutos: qué hacer y qué no - Por qué no se apaga el equipo ni se borran evidencias - Canal y plazo de reporte interno - Cultura de reporte sin castigo: por qué ocultar un incidente es peor

3.4 Evaluación y compromiso - Simulacro integral - Evaluación de conocimiento - Firma del compromiso de prácticas seguras

Entregable final: evaluación aprobada + compromiso firmado.