Normas de sistemas de gestión

Sensibilización en ciberseguridad

Media jornada para que cada colaborador reconozca las amenazas más comunes y adopte los reflejos adecuados: suplantación de identidad, contraseñas, puesto de trabajo, dispositivos móviles, intercambio de archivos y comunicación de incidentes. La sesión se apoya en ejemplos de mensajes fraudulentos, en las reglas vigentes en su empresa y, si existe, en su política de seguridad de la información.

Duración : 0,5 día

Objetivos

1. Reconocer un mensaje de phishing, un fraude del falso directivo o un falso soporte técnico
2. Aplicar las reglas básicas: contraseñas, doble autenticación, bloqueo del puesto, actualizaciones
3. Proteger la información de la empresa en el puesto, en desplazamiento y en los dispositivos personales
4. Comunicar sin demora un incidente o una duda siguiendo el procedimiento interno

Programa

Media jornada

• Por qué los atacantes apuntan a las personas más que a las máquinas

• Phishing, fraude del falso directivo, ransomware: ejemplos y señales de alerta

• Contraseñas, doble autenticación, bloqueo del puesto, actualizaciones

• Memorias USB, wifi público, dispositivos personales, uso compartido de archivos y redes sociales

• Comunicación de un incidente; cuestionario final

Metodología

• Ejercicio de detección sobre mensajes fraudulentos reales, anonimizados

• Cuestionario interactivo durante la sesión

• Repaso de las reglas internas de su empresa, validadas previamente con su servicio informático

• Posibilidad de impartir en francés, en darija o en inglés, para los equipos de oficina y de campo

Evaluación y documentos

Cuestionario al final de la sesión, evaluación en caliente a J+1. Certificado numerado, verificable en línea, para cada participante; informe de formación con los resultados del cuestionario entregado a la empresa.

Materiales bilingües para cada participante; cada formación presencial incluye su gemelo digital en OmniLearn.

Conviene saber

Para estructurar un sistema de gestión de la seguridad de la información, véase «ISO/IEC 27001:2022 — Requisitos». La protección de los datos personales se trata en «ISO/IEC 27701:2025 y ley 09-08».

Información práctica

Duración	0,5 día
Público	Todos los colaboradores que utilizan un puesto informático, correo electrónico o un teléfono profesional
Requisitos previos	Ningún requisito previo
Número de participantes	Grupos de 6 a 12 participantes, en la empresa
Formato	En la empresa, presencial en sus instalaciones
Idioma	Francés, darija o inglés; materiales bilingües
Financiación	Contratos especiales de formación de la OFPPT (TFP), GIAC, Maroc PME: preparamos los expedientes con usted, sin coste adicional.
Personalización del programa	Programa adaptado a sus procedimientos, sus equipos y su público

Preguntas frecuentes

¿A quién se dirige esta sesión?
A todos los colaboradores que utilizan correo electrónico, un ordenador o un teléfono profesional, del asistente al director. Puede repetirse por grupos para cubrir todo un sitio.

¿Hacen falta conocimientos de informática?
Ninguno. El vocabulario técnico se reduce al mínimo y cada noción se ilustra con una situación de trabajo.

¿Sirve esta sensibilización a un proyecto ISO/IEC 27001:2022?
Contribuye al requisito de toma de conciencia del personal y deja constancia de ello: lista de asistencia, resultados del cuestionario, informe. No sustituye la implantación del propio sistema de gestión.

¿Se puede adaptar a nuestras herramientas?
Sí. Integramos sus reglas de uso, su procedimiento de comunicación de incidentes y las herramientas que utiliza, tras hablar con su servicio informático.