

# Ciberseguridad en el puesto de trabajo (Usuarios)

Este curso de Ciberseguridad en el puesto de trabajo para usuarios busca **transformar al empleado en la primera línea de defensa de la organización**. El objetivo central es que los participantes adquieran las habilidades necesarias para identificar riesgos y actuar correctamente ante posibles amenazas en su entorno digital cotidiano.

Conocer las principales amenazas a los sistemas de información e identificar las principales herramientas de seguridad y como aplicarlas en cada caso. La Concienciación es para la empresa una obligación y el punto más importante de cumplimiento con las normas ISO 27001 y ENS.

---

## Objetivos Didácticos

Al finalizar esta formación, los participantes serán capaces de:

- Entender por qué cada empleado forma parte de la primera línea de defensa de la empresa.
- Identificar las principales amenazas a los sistemas de información en su actividad diaria.
- Reconocer señales de alerta en correos sospechosos, enlaces fraudulentos y mensajes de suplantación.
- Detectar ataques de phishing, smishing y vishing.
- Aplicar buenas prácticas de gestión de contraseñas y autenticación multifactor.
- Comprender el valor de los gestores de contraseñas y del doble factor de autenticación.
- Proteger portátiles, móviles, memorias USB y otros dispositivos de uso habitual.
- Reducir riesgos relacionados con aplicaciones, permisos, redes Wi-Fi públicas y dispositivos desactualizados.
- Navegar con mayor seguridad y evitar fugas de información en redes sociales.
- Adoptar pautas claras de teletrabajo seguro.
- Saber cómo actuar y reportar con rapidez ante un posible incidente.

---

## Audiencia

Este curso está especialmente dirigido a empresas que quieren reforzar la seguridad de sus equipos y reducir incidentes derivados del factor humano.

Encaja especialmente bien en:

- Plantillas de cualquier sector que utilicen correo electrónico, aplicaciones corporativas o acceso a información sensible.
- Empleados de áreas como administración, finanzas, recursos humanos, comercial, atención al cliente, operaciones o dirección.
- Organizaciones que quieran impulsar acciones de concienciación en ciberseguridad.
- Empresas que necesiten mejorar hábitos digitales seguros en entornos presenciales, híbridos o remotos.
- Equipos no técnicos que deban aprender a identificar y gestionar amenazas habituales en su puesto de trabajo.

---

## Metodología

Aula virtual en directo.

---

## Duración

4 horas

---

## Temario del curso

### Módulo 1: El Eslabón Más Fuerte (y el Más Débil)

*Objetivo: Cambiar la mentalidad de "la seguridad es cosa del departamento de IT" a "yo soy la primera línea de defensa".*

#### 1. Bienvenida y Rompehielos

- ¿Qué dato tuyo vale más dinero en la Dark Web?" (Mostrar precios reales de cuentas robadas).

#### 2. La realidad actual

- Estadísticas recientes de brechas causadas por error humano.
- Concepto de "Ingeniería Social": Por qué nos engañan tan fácil.

#### 3. Taller Práctico: "Anatomía de un Ataque

- Análisis en vivo de correos reales (phishing) vs. legítimos.
- Identificación de "banderas rojas" (urgencia, remitente extraño, enlaces sospechosos).

### Módulo 2: Contraseñas y Autenticación: Olvida el Post-it

*Objetivo: Eliminar malas prácticas de gestión de credenciales.*

#### 1. Por qué fallan las contraseñas tradicionales

- Cuánto tarda un hacker en romper "Password123".

#### 2. Gestores de Contraseñas

- Qué son, por qué son seguro.

#### 3. Autenticación en Dos Pasos (2FA/MFA)

- Explicación "Algo que sabes + Algo que tienes".

#### 4. La seguridad biométrica

### **Módulo 3: Phishing y Vishing**

*Objetivo: Detectar ataques modernos que no parecen spam obvio.*

- 1. Más allá del correo: SMS (Smishing) y Llamadas (Vishing)**
  - Casos reales de suplantación de directivos (CEO Fraud) o de soporte técnico.
- 2. Protocolo de Actuación**
  - ¿Qué hago si hice clic? (Importancia de reportar rápido sin miedo a represalias).
  - Canales de reporte en la empresa.

### **Módulo 4: Dispositivos Seguros: Portátiles, Móviles y USB**

*Objetivo: Proteger el hardware y los datos en movilidad.*

- 1. Amenazas Físicas**
  - Riesgos de dejar el portátil desbloqueado ("Shoulder Surfing").
  - Peligro de los USB encontrados en la calle o parking.
- 2. Seguridad en el Móvil**
  - Apps maliciosas, permisos excesivos y redes Wi-Fi públicas.
  - Taller: Revisión de permisos en sus propios móviles (Android/iOS).
- 3. Actualizaciones y Parches**
  - Por qué ese mensaje de "Actualizar ahora" es vital.
  - Vulnerabilidades conocidas por no actualizar.
- 4. Limpieza de escritorio y pantalla**
  - Política de mesa limpia y bloqueo automático.

### **Módulo 5: Navegación Segura y Redes Sociales**

*Objetivo: Proteger la huella digital y evitar fugas de información.*

- 1. Navegación Inteligente**
  - HTTPS, candados y extensiones de seguridad básicas.
  - Descargas seguras vs. software pirata (riesgos de malware).

## 2. Redes Sociales y OSINT para usuarios

- Cómo los atacantes usan LinkedIn/ Facebook para crear perfiles falsos creíbles.
- Configuración de privacidad: Qué ven los extraños.

## 3. Teletrabajo Seguro

- Riesgos específicos al trabajar desde casa (redes domésticas, dispositivos compartidos con familia).