

EVITA LOS ENGAÑOS EN LA RED

UTILIZA SOLUCIONES ANTIFRAUDE

INCIBE
BALANCE 2025



El fraude online representa **4 de cada 10 incidentes** de seguridad (45.445), un **19%** más que en 2024.

La Línea de Ayuda 017 atendió **142.767** consultas, un **45%** más que el año anterior.

1 LOS ENGAÑOS DIGITALES ESTÁN EN TODAS PARTES

Los ciberdelincuentes usan ingeniería social para ganar tu confianza y conseguir dinero, credenciales o información.



La IA generativa permite crear mensajes más creíbles, clonación de voz y deepfakes para suplantar a personas y empresas.

2 SOLUCIONES Y CONTROLES CLAVE

SI TU EMPRESA UTILIZA SERVICIOS ONLINE

- 1 Protege el correo: antiphishing, antispam, análisis de enlaces y adjuntos.
- 2 Filtra la navegación: bloqueo de sitios maliciosos, DNS filtering y análisis de URLs.
- 3 Fortalece la identidad: MFA resistente al phishing, passkeys, gestores de contraseñas.
- 4 Previene el fraude del CEO: doble validación, confirmación por canal alternativo, límites y revisión de cambios de IBAN.
- 5 Monitoriza accesos: detección de inicios de sesión anómalos y dispositivos desconocidos.
- 6 Forma y conciencia: simulaciones de phishing, smishing, vishing, QR y deepfakes.
- 7 Gestiona vulnerabilidades y actualizaciones.
- 8 Protege endpoints: EDR/XDR, antimalware y control de aplicaciones.
- 9 Copias de seguridad y plan de respuesta ante incidentes.
- 10 Revisa permisos de usuarios, proveedores y aplicaciones.



SI TU EMPRESA VENDE ONLINE

- Usa certificados digitales válidos (HTTPS). HTTPS no garantiza legitimidad.
- Medios de pago seguros y autenticación reforzada (3DS 2.0 / SCA).
- Detección de fraude: scoring de riesgo, análisis de comportamiento y patrones anómalos.
- Revisa pedidos sospechosos: datos incoherentes, IPs, cambios de dirección, tarjetas rechazadas.
- Protege cuentas de clientes: MFA, políticas de contraseñas y control de sesiones.
- Monitoriza tu marca: dominios similares, perfiles falsos, anuncios maliciosos.
- Proceso de takedown: reporta y solicita la retirada de páginas o anuncios fraudulentos.
- Protege tu web y pasarelas de pago: actualizaciones, WAF y copias de seguridad.
- Detecta bots y abuso de cuentas.
- Gestiona chargebacks y devoluciones fraudulentas.



3 CAPAS ESENCIALES DE PROTECCIÓN INTEGRADA

- | | | | | | | |
|-------------------------------------|---------------------|---------------------|--|------------------------------|------------------------------------|---------------------------|
| Protección de correo y colaboración | Seguridad web y DNS | Identidad y accesos | Dispositivos y red (EDR/XDR, firewall) | Pagos y comercio electrónico | Monitorización de marca y amenazas | Respuesta ante incidentes |
|-------------------------------------|---------------------|---------------------|--|------------------------------|------------------------------------|---------------------------|

Tecnología + Procesos + Personas = Menos riesgos, menos fraudes.

4 REGLAS DE ORO

- ✓ Desconfía de la urgencia y presiones inusuales.
- ✓ Verifica siempre por un canal alternativo.
- ✓ No hagas clic en enlaces ni escanees QR sospechosos.
- ✓ Nunca compartas credenciales, códigos o datos bancarios.
- ✓ Si algo te resulta extraño, para, consulta y reporta.



5 ¿NECESITAS AYUDA?

Línea de Ayuda en Ciberseguridad 017
Gratuita, confidencial y disponible 24/7

TU AYUDA EN
CIBERSEGURIDAD



WhatsApp
900 116 117

Telegram
@INCIBE017

Formulario
web

ANTE CUALQUIER DUDA, CONTACTA CON EL 017

La mejor defensa sigue siendo sencilla: parar, verificar y actuar con criterio.



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
E INFRAESTRUCTURAS DIGITALES

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD

