

PROTOCOLO DE EMPRESA · CHECKLIST

Phishing, suplantación y deepfakes: qué hacer antes de actuar

Una guía de escritorio para verificar pagos, cambios bancarios, credenciales y solicitudes urgentes cuando un correo, una voz o un vídeo también pueden falsificarse.

- 01 PAUSA**
No ejecutes la petición durante la misma conversación.
- 02 CLASIFICA**
Identifica si implica dinero, datos, credenciales, acceso o un cambio sensible.
- 03 VERIFICA**
Usa el directorio interno o un contacto conocido; nunca el canal incluido en la petición.
- 04 APRUEBA**
Aplica doble control y límites, aunque la voz o el mensaje parezcan auténticos.
- 05 REGISTRA**
Conserva evidencias y anota cómo se verificó y qué se decidió.
- 06 ESCALA**
Informa al canal interno ante presión, incoherencia o intento confirmado.

REGLA

La urgencia no elimina el control. Cuanto más excepcional sea la petición, más importante es utilizar el procedimiento normal de verificación.

Uso rápido

Imprime las páginas 2 y 3 para finanzas, dirección, RR. HH., administración, soporte e IT. Adapta los contactos, importes y responsables a tu empresa y practica el protocolo antes de un incidente.

DECISIÓN INDIVIDUAL

Antes, durante y después de una petición

1. Antes de confiar

No intentes decidir si el contenido es perfecto. Comprueba si la operación encaja con el proceso.

- ☐ La petición llega por un canal y una cuenta habituales.
- ☐ La persona tiene capacidad real para solicitar esta operación.
- ☐ El tono de urgencia o secreto no intenta anular un control.
- ☐ El dominio, enlace y archivo se han revisado sin abrir contenido dudoso.
- ☐ El cambio de cuenta, beneficiario, acceso o procedimiento estaba previsto.

2. Antes de ejecutar

Verifica por un canal independiente y aplica las reglas normales, incluso si has visto u oído a la persona.

- ☐ He usado un teléfono, directorio o contacto que ya estaba registrado.
- ☐ No he utilizado el número, enlace o identidad propuestos en el mensaje.
- ☐ La verificación describe importe, destinatario, finalidad y cambio solicitado.
- ☐ Se ha aplicado la segunda aprobación correspondiente.
- ☐ Nadie ha compartido contraseñas, códigos MFA o credenciales.

3. Si algo no encaja

Detener una operación razonablemente sospechosa es parte del trabajo, no una molestia.

- ☐ He detenido el pago, cambio, acceso o envío de información.
- ☐ He guardado correo original, cabeceras, archivos, números y capturas útiles.
- ☐ He avisado al canal interno sin reenviar el contenido a más personas de las necesarias.
- ☐ Si ya hubo pago, se ha contactado de inmediato con la entidad financiera.
- ☐ No he investigado por mi cuenta ni interactuado más con el posible atacante.

PREPARACIÓN DE LA EMPRESA

El protocolo necesita una organización detrás

Personas y proceso

Controles para que la decisión no dependa de una impresión.

- ☐ Directorio de verificación accesible y mantenido.
- ☐ Doble aprobación para pagos y cambios sensibles.
- ☐ Límites por importe, rol, canal y horario.
- ☐ Sustitutos definidos si el aprobador no está disponible.
- ☐ Canal de incidentes conocido por toda la plantilla.
- ☐ Cultura sin culpa para avisos razonables.

Tecnología y respuesta

Capas que reducen exposición y limitan el recorrido del atacante.

- ☐ MFA y mínimo privilegio en cuentas críticas.
- ☐ SPF, DKIM y DMARC supervisados.
- ☐ Filtrado y análisis de enlaces y adjuntos.
- ☐ Protección y actualización de equipos.
- ☐ Copias probadas y respuesta a incidentes.
- ☐ Simulacros conectados con este procedimiento.

Contactos que deben completarse

ÁREA / PERSONA	CANAL	CUÁNDO AVISAR
Seguridad / IT		Correo, acceso, malware o cuenta comprometida
Finanzas		Pago, cambio bancario o proveedor
Privacidad / DPD		Datos personales o posible brecha
Dirección / continuidad		Interrupción o impacto relevante
Entidad financiera		Transferencia o fraude ejecutado

Fuentes para profundizar

INCIBE: medidas de seguridad del correo electrónico, fraude de email comprometido y kit de concienciación. Línea 017 de ayuda en ciberseguridad. Este documento es orientativo y debe adaptarse a los procesos, riesgos y obligaciones de cada empresa.