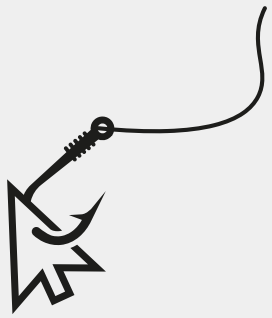
# Protocolo de respuesta rápida Anti-Phishing para pymes



## INTRODUCCIÓN

Este protocolo ha sido diseñado por Cosmomedia para guiar a las pymes y autónomos a través de tres fases críticas de la gestión de una **suplantación de identidad digital** (phishing de marca, réplicas web o robo de credenciales).

Cabe mencionar que ninguna empresa está libre del phishing; incluso las grandes compañías con departamentos enteros de ciberseguridad pueden sufrir de suplantación de identidad. **La clave está en responder y en hacerlo rápido.**

La rapidez en la respuesta reduce exponencialmente el daño económico y reputacional, **fortaleciendo la confianza de tus clientes.**

## FASES

Este protocolo tiene tres fases: **prevención, detección y contención, y erradicación y refuerzo.**

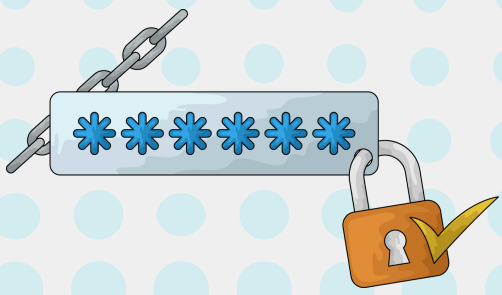
## Fase 0: Prevención y preparación (antes del ataque)

La mejor defensa es tener sistemas que, de entrada, frustren la mayoría de los ataques e impidan que la web sea replicada o controlada por terceros.

### 1. Fortalecimiento de accesos (la cerradura digital)

La suplantación de identidad busca robar las credenciales sensibles.

- **Implementación de 2FA/MFA obligatoria**: **Haz obligatorio** el doble factor de autenticación (2FA) o multifactor (MFA) en todos los servicios críticos: correo electrónico corporativo, banca online, CRM, y **administración del dominio/hosting**. El 2FA exige un segundo paso de verificación (un código temporal enviado al móvil, por ejemplo), haciendo inútil la contraseña robada por el phishing.
- **Uso de gestores de contraseñas: Prohíbe** el uso de la misma contraseña en distintos servicios. Utiliza un gestor de contraseñas (como LastPass o 1Password) para generar claves complejas y únicas automáticamente.
- **Blindaje del dominio y DNS (el activo central)**: Asegúrate de que las credenciales del registrador de dominio (la empresa donde compraste tu dominio, ej: midominio.es) son las más seguras. Si un atacante accede al panel del dominio, puede redirigir tu web a la falsa.
- **Separación de cuentas**: Las cuentas de administración y gestión (por ejemplo, el acceso a la web, hosting o FTP) deben tener credenciales distintas a las cuentas de correo electrónico diario.



## 2. Formación continua del equipo (el factor humano)

El empleado es la primera línea de defensa. La formación debe enfocarse en proteger las credenciales de la web y los datos de los clientes.

- **Simulacros de phishing específicos**: Realiza simulacros internos periódicos enfocados en correos que piden credenciales de hosting o de administrador de la web. El personal debe saber a quién notificar (punto 3).
- **Protocolo del candado (HTTPS)**: Instruye al personal para que siempre verifique que cualquier web de login o pago muestre el candado de seguridad (HTTPS) en la barra de direcciones y que la URL sea exactamente la oficial.
- **Reforzar el registro de usuarios con respuesta oficial**: El usuario que quiera comprar en tu ecommerce deberá registrarse previamente, recibiendo un email de confirmación desde un email oficial de la empresa.

## 3. Contacto de emergencia en caso de suplantación

- **¿A quién informar?**: Define a una única persona o empresa (el proveedor web, la empresa o departamento de Soporte Técnico...) como el contacto de emergencia en caso de intrusión. Saber qué hacer y a quién recurrir agiliza todo el proceso.

## Fase 1: Detección y contención (durante la crisis)

Si un cliente contacta alertando de una web falsa o si se detectan credenciales robadas, la acción debe ser instantánea y escalada.

### Paso 1: Aislamiento inmediato de dispositivos o cuentas

- **Si se ha hecho clic en un enlace o se han introducido credenciales:** Desconecta inmediatamente el dispositivo (PC, móvil) de la red Wi-Fi y del cable de red. La contención es prioritaria para evitar la propagación.

### Paso 2: Cambio masivo y urgente de contraseñas

- **Prioridad absoluta (activos web)**: Cambia de forma inmediata las contraseñas de TODAS las cuentas sensibles vinculadas, desde el correo corporativo afectado, el acceso a la banca online, y principalmente el CMS de gestión web (Wordpress, Accesive, Web Activa...)
  - Advertencia: **NO uses la cuenta comprometida** para realizar los cambios. Utiliza un dispositivo limpio, aislado de la red y con una conexión segura (por ejemplo, un móvil sin conexión a la WIFI de empresa, con datos 4G/5G).

- **Verificación 2FA**: Confirma que el doble factor de autenticación de las cuentas críticas sigue activo y no ha sido desactivado o modificado por el atacante.

## Paso 3: Notificación interna y externa para proteger al cliente

- **Alerta pública (suplantación web):** Si se confirma la réplica de la web, **publica** inmediatamente una **alerta VISIBLE y URGENTE** en todos tus canales legítimos (redes sociales, cabecera de la web oficial, perfil de Google Business Profile, correo masivo a clientes) advirtiendo claramente sobre la URL fraudulenta y proporcionando la URL **correcta** para transacciones seguras.
- **Aviso de registro de usuarios (si aplica):** Además, si tu *ecommerce* dispone de un registro de usuarios vinculado a una dirección de email propia de la empresa que esté limpia, **INDÍCALO**. Por ejemplo: "Para comprar se requiere registro de usuario. Al formalizar el registro, recibirás un email desde la cuenta oficial ejemplo@ejemplo.es"
- **Alerta a la empresa:** Aplica el Contacto de emergencia (Punto 3 de la Fase 0) para iniciar el protocolo de aviso y protección.

## Fase 2: Erradicación y refuerzo (post-incidente)

Una vez contenida la amenaza, el foco pasa a la eliminación total y al blindaje de tu marca de empresa, para que el SEO actúe como una muralla de confianza.

### 4. Eliminación de la amenaza

- **Denuncia de la suplantación (takedown):** La prioridad es conseguir la caída de la web falsa para proteger a tus clientes.
  - Denuncia a Google: Usa las herramientas de Google para denunciar el phishing y solicitar la caída del sitio fraudulento.
  - Contacto con el hosting: Si se conoce el proveedor de hosting de la web falsa, contacta con ellos para que suspendan el dominio.
  - Denuncia legal: Presenta una denuncia formal para tener respaldo legal en el proceso de solicitud de takedown (eliminación) del dominio falso.
- **Limpieza de puntos de entrada**: Realiza una auditoría forense para determinar exactamente cómo entró el atacante (correo, web, dispositivo) y elimina el malware o el acceso remoto instalado.
- **Estrategia en caso de copia externa**: En el caso de suplantación de web (no han entrado en tu sistema, sino que han copiado tu página) la estrategia debe centrarse en: educar a tu cliente y en mejorar tu SEO para reforzar tu autoridad digital. **Puedes enviar emails a clientes o proveedores**, informando de la dirección real y avisando de los mecanismos de seguridad que tengas incorporados, como por ejemplo, el registro de usuarios antes de comprar, con confirmación de identidad desde una dirección de email corporativa.

## 5. Refuerzo del SEO de marca (el blindaje digital anti-suplantación)

**Tu estrategia de SEO de marca** es la defensa a largo plazo para que tus clientes solo vean tu web oficial.

- **Dominio total de búsquedas de marca: Debes garantizar** que cuando un cliente busque el nombre de tu empresa, **TODOS** los resultados de la primera página sean tuyos y de confianza. La web falsa debe ser relegada fuera de la vista.
  - **Acciones: Refuerza** y **optimiza** tu perfil de **Google Business Profile**, tus perfiles sociales (*LinkedIn*, *Instagram*) y **asegúrate** de que la descripción (*meta description*) de tu web oficial es clara. Utiliza términos de seguridad.
- **Publicación de contenido defensivo:** Publica contenido en tu web legítima que hable de tu seguridad y elige una *meta description* que incluya el nombre de la marca. Esto refuerza la Autoridad Temática y Digital ante Google.
- **Monitorización de marca (*brand monitoring*): Utiliza** herramientas de *marketing* digital (como alertas de Google o herramientas SEO específicas) para rastrear de forma diaria cualquier mención, URL o dominio que contenga el nombre de tu marca para detectar réplicas futuras en fase temprana. Es especialmente útil **activar una alerta de Google con el nombre de tu empresa**, para rastrear de forma directa y automática todo lo que se dice de ti en Internet.

## 6. Lecciones aprendidas y documentación

- **Documentación**: Registra la fecha, hora, tipo de ataque y respuesta realizada. Esta documentación es vital para futuras auditorías o posibles litigios.
- **Auditoría de vulnerabilidad**: Tras el incidente, es imprescindible realizar una auditoría completa de ciberseguridad y SEO para identificar y cerrar todas las vulnerabilidades expuestas durante el ataque, asegurando que el perímetro digital de tu pyme está blindado.

Este protocolo es una guía rápida de respuesta. En una situación real de phishing o suplantación, **recomendamos contactar inmediatamente con especialistas en ciberseguridad**, para garantizar la erradicación completa y el cumplimiento legal.

¿Estás seguro de que tu empresa es la única que aparece cuando te buscan, o dejas espacio para que otros se apropien de tu identidad digital? **En Cosmomedia, te ayudamos a auditar tu presencia online y a construir el blindaje digital que necesitas. Pregúntanos**

## Vías de contacto:

**Email**: hola@cosmomedia.es

**Formulario online**: https://www.cosmomedia.es/contacta-con-cosmomedia

# Te ayudamos a gestionar la ciberseguridad de tu empresa

hola@cosmomedia.es