
INFORME DE SIMULACIÓN DE PHISHING

Algorítmico S.A.

Evaluación de Concienciación y Resiliencia del Personal
Fecha: 28/05/2026
Elaborado por: Departamento de Ciberseguridad

---

1. Resumen Ejecutivo

El presente informe recoge los resultados de la campaña de simulación de phishing realizada en **Algorítmico, S.A.**, cuyo objetivo fue evaluar el nivel de concienciación del personal ante intentos de ingeniería social y medir la capacidad de detección y respuesta frente a correos fraudulentos.

La campaña se diseñó para replicar técnicas utilizadas habitualmente por atacantes reales, incluyendo suplantación de identidad, enlaces maliciosos y solicitudes de credenciales.

Conclusión general:
El nivel de exposición se considera **medio-alto**, debido a un porcentaje significativo de usuarios que interactuaron con el correo simulado y un número relevante que llegó a introducir credenciales en la página falsa.

---

2. Alcance del Proyecto

2.1 Objetivos

- Evaluar la capacidad del personal para identificar correos fraudulentos.
- Medir la tasa de clics en enlaces sospechosos.
- Analizar la tasa de introducción de credenciales.
- Identificar áreas de mejora en formación y concienciación.

2.2 Población objetivo

- Empleados de Algorítimico, S.A.
- Total de usuarios incluidos: **124**
- Exclusiones: Dirección General (a petición expresa)

2.3 Tipología de ataque simulado

- Correo de phishing con:
    - Suplantación de proveedor externo
    - Enlace a portal falso
    - Solicitud de actualización de credenciales

---

3. Metodología Aplicada

La campaña se desarrolló siguiendo las mejores prácticas de ingeniería social:

1. **Diseño del escenario**
    - Selección de un pretexto creíble (proveedor de servicios).
    - Creación de dominio similar al legítimo.
2. **Envío del correo simulado**
    - Distribución controlada a los 124 empleados.
3. **Monitorización de interacciones**
    - Apertura del correo
    - Clic en el enlace
    - Introducción de credenciales
4. **Análisis de resultados**
    - Clasificación por departamentos
    - Identificación de patrones de riesgo
5. **Informe y recomendaciones**

---

4. Resultados de la Campaña

4.1 Métricas globales

Indicador	**Resultado**
Correos entregados	124
Correos abiertos	97 (78%)
Usuarios que hicieron clic	41 (33%)

Indicador	Resultado
Usuarios que introdujeron credenciales	12 (10%)
Usuarios que reportaron el correo	4 (3%)

4.2 Análisis por fases

Apertura del correo

La tasa de apertura del 78% indica que el mensaje resultó creíble y relevante para los usuarios.

Clic en el enlace

Un 33% de usuarios accedió al enlace fraudulento, lo que supone un riesgo significativo ante un ataque real.

Introducción de credenciales

El 10% de los usuarios introdujo sus credenciales corporativas en la página falsa, lo que en un escenario real permitiría:

- Acceso no autorizado a sistemas internos
- Robo de información
- Movimientos laterales en la red
- Compromiso de cuentas de correo

Reportes del correo

Solo un 3% reportó el correo al departamento de TI, lo que evidencia la necesidad de reforzar los canales de comunicación y la cultura de reporte.

---

5. Evaluación del Riesgo Global

Categoría	Nivel
Riesgo humano	**Alto**
Riesgo operativo	**Medio**
Riesgo reputacional	**Medio-Alto**
Riesgo de cumplimiento	**Medio**

---

6. Recomendaciones Prioritarias

1. **Formación obligatoria en concienciación de phishing** para todo el personal.
2. **Campañas periódicas** (trimestrales) de simulación para medir la evolución.
3. **Refuerzo de la cultura de reporte**, facilitando canales rápidos y visibles.
4. **Implementación de banners de advertencia** en correos externos.
5. **Activación de MFA** en todos los accesos corporativos.
6. **Revisión de políticas de contraseñas** y detección de accesos anómalos.

---

7. Conclusiones

La campaña de phishing ha puesto de manifiesto que un porcentaje relevante de empleados sigue siendo vulnerable a técnicas de ingeniería social. La introducción de credenciales por parte del 10% de los usuarios supone un riesgo elevado que debe abordarse mediante formación continua y medidas técnicas complementarias.

La mejora de la concienciación del personal es un elemento clave para reducir la superficie de ataque y aumentar la resiliencia de ECOticias, S.L. frente a amenazas reales.

---

8. Anexos

- Capturas del correo enviado
- Diseño del portal falso
- Métricas detalladas por departamento
- Cronograma de la campaña
- Material formativo recomendado

Si quieres, puedo generarte también:

- **La portada corporativa**
- **La tabla de contenidos automática**

- **El diseño con estilos de Word (H1, H2, H3)**
- **Una versión extendida con gráficos y tablas**

¿Deseas que prepare la **versión final lista para maquetar en Word** con estilos aplicados?