

# Guardianes Digitales 2026



Tu defensa contra amenazas potenciadas por IA

Basado en NIST 2.0 & ISO/IEC 27001:2026

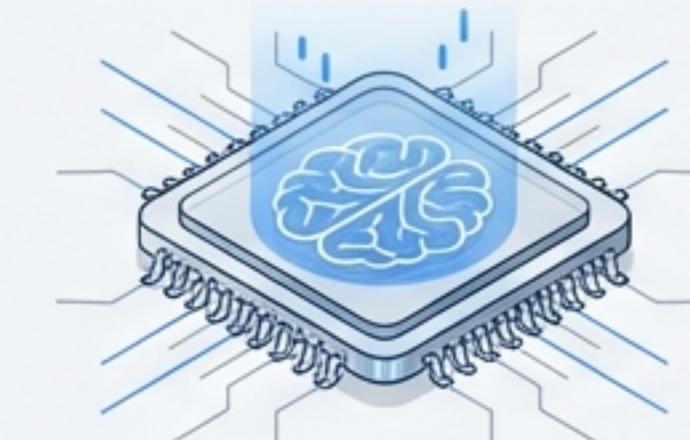
# El enemigo ha evolucionado. Nosotros también.

ANTES (2024)



Faltas de ortografía.  
Estafas genéricas.  
Fácil de detectar.

AHORA (2026)



Gramática perfecta.  
Contexto personalizado.  
Potenciado por LLMs (IA).

El marco NIST 2.0 es claro: La tecnología no es suficiente. El firewall humano es la última línea de defensa. Si el sistema falla, nos quedas tú.

# Phishing 3.0: Perfección Clínica



## Anomalía de Contexto

¿Es lógico que el CEO pida un cambio bancario un martes a las 11 PM? Los atacantes usan Spear Phishing para conocer tu rol y proyectos.



## Typosquatting



## Ingeniería Social

El pánico bloquea el juicio. Frases como "Acción inmediata requerida" son la firma del atacante.

# Amenazas Silenciosas y Letales

El malware moderno no ralentiza tu PC ni abre ventanas emergentes. Roba credenciales en silencio.



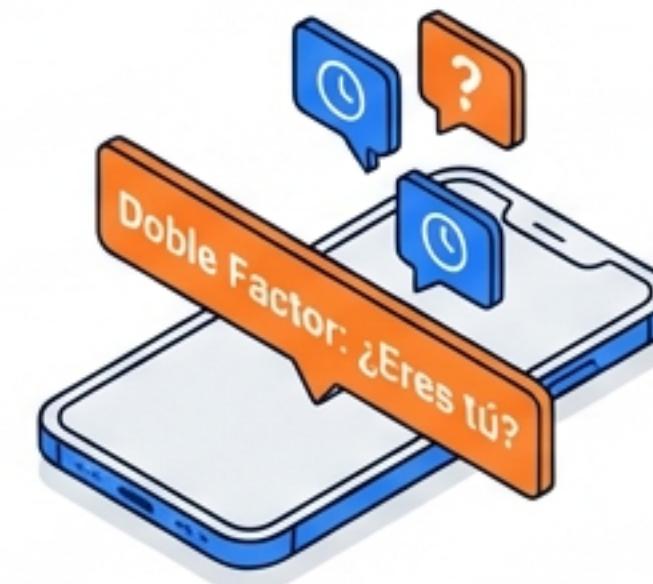
## Adjuntos Disfrazados

Archivos con contraseña para evadir escáneres.



## La Trampa de los Macros

Si pide 'Habilitar Contenido', asume que es una infección (CIS Controls).

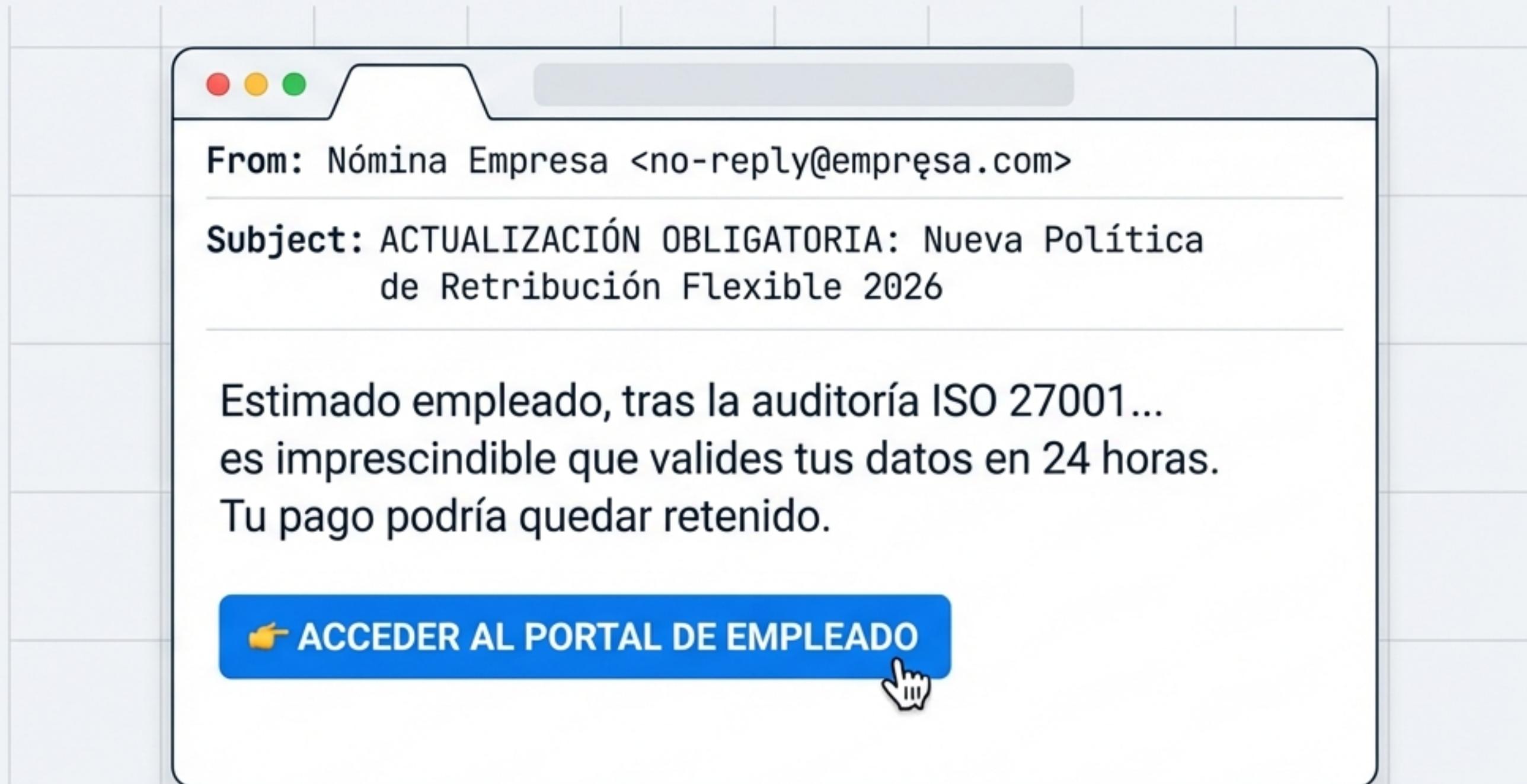


## MFA Fatigue

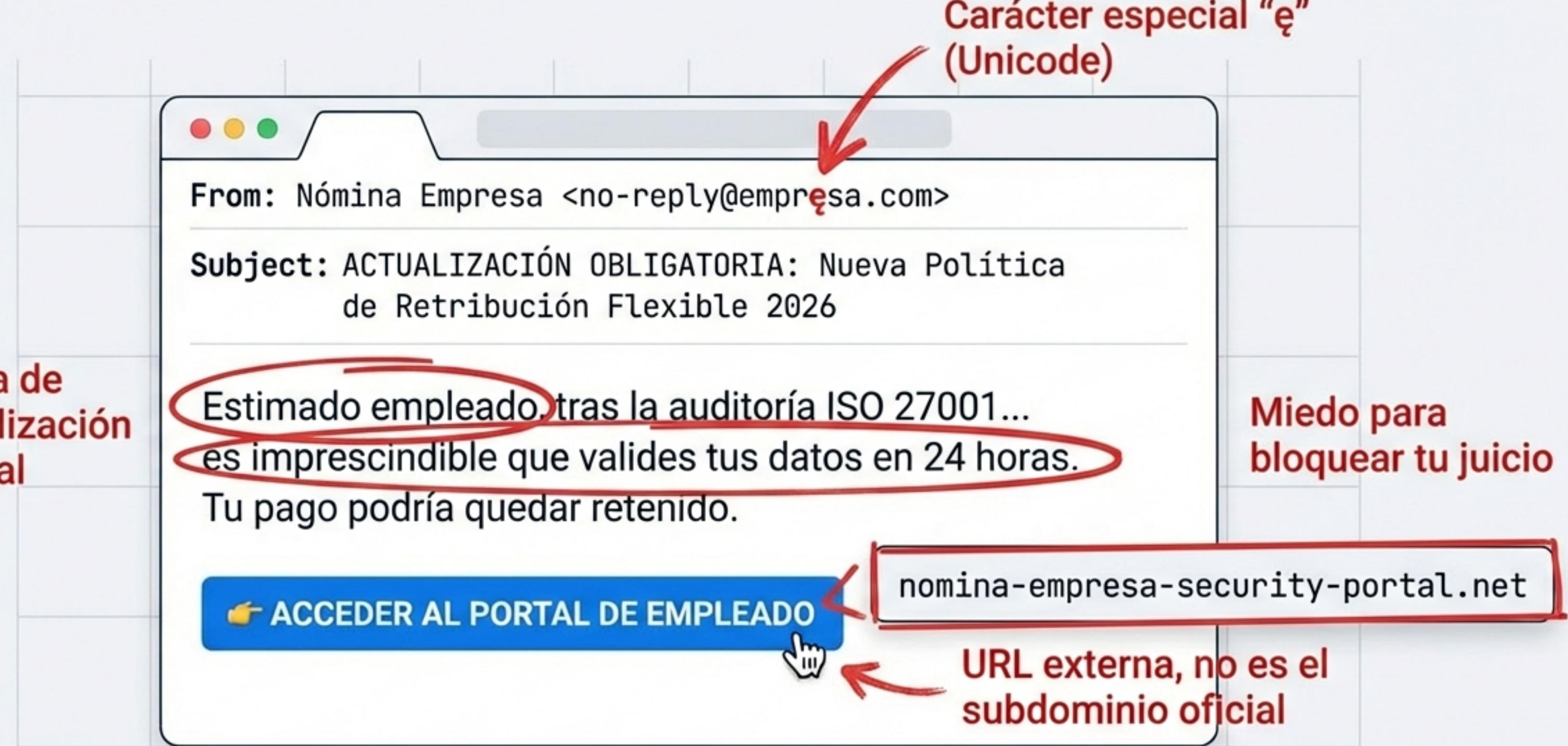
¿Recibes notificaciones de doble factor sin intentarlo? Es un ataque de fatiga.

# 🚩 Ejercicio Práctico: ¿Detectas la Amenaza?

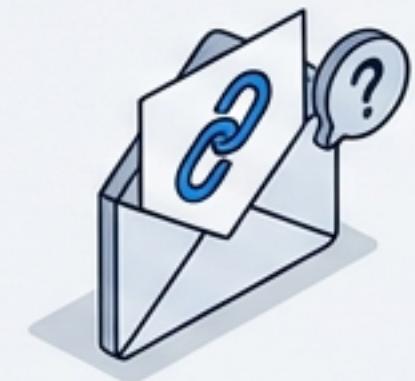
Tienes 10 segundos. ¿Haces clic o reportas?



# Solución: Las 4 Banderas Rojas



# Tu Matriz de Decisión Rápida



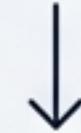
Link Inesperado



HOVER (No clic, ver URL real)



Pide Datos Sensibles



VERIFICAR (Llamada o Slack interno)



Adjunto No Solicitado



REPORTAR (Botón Phishing)



La Regla de los 3 Segundos: Respira, Mira el remitente, Haz Hover.

# Protocolo: Detecta, Detén y Notifica

## 1. ¡No Interactúes!



- Prohibido hacer clic.
- No respondas para “trolear”.
- No reenvíes a compañeros preguntando “¿Es esto real?” (propaga la amenaza).

## 2. Reporte Oficial



### Vía Directa

Usa el botón ‘Reportar Phishing’.



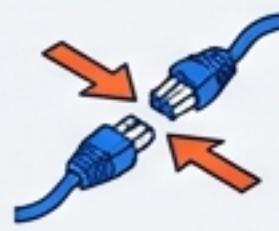
### Vía Manual

Reenvía como \*adjunto\* a ciberseguridad@tuempresa.com

Tu reporte bloquea el ataque para toda la organización.

# ¿Hiciste Clic? No entres en Pánico. La velocidad gana a la vergüenza.

---



## 1. Aísla el equipo:

Desconecta el cable de red o apaga el Wi-Fi inmediatamente.



## 2. Contacta a Soporte:

Llama o escribe por Teams/Slack oficial.



## 3. Credenciales:

Cambia tu contraseña desde un dispositivo diferente (móvil).



# Cultura de Cero Culpa



## **Filosofía:**

El silencio es el mejor aliado del hacker.  
Si te equivocas, repórtalo. No serás  
sancionado por informar de inmediato.

## **Gamificación:**

Simulamos ataques para entrenar, no  
para castigar. La seguridad es un deporte  
de equipo.

# Eres un Guardián Digital

---



**Scepticismo:** Desconfía de la perfección y la urgencia.



**Hover:** Nunca hagas clic sin mirar la URL.



**Macros:** Jamás habilites contenido en archivos desconocidos.

**Dudas o Reportes:** ciberseguridad@tuempresa.com | Intranet/Seguridad

**Cero Culpa. Máxima Protección.**