

LA CIBERSEGURIDAD EN EL ÁMBITO EDUCATIVO



NAVEGACIÓN SIN SOBRESALTOS



EL ARTE DE NAVEGAR DESAPERCIBIDO



HUELLA DIGITAL: IMPACTO Y GESTIÓN

Entendiendo qué es una huella digital.

Cómo se crea y se acumula información.

Riesgos asociados a una huella digital amplia.

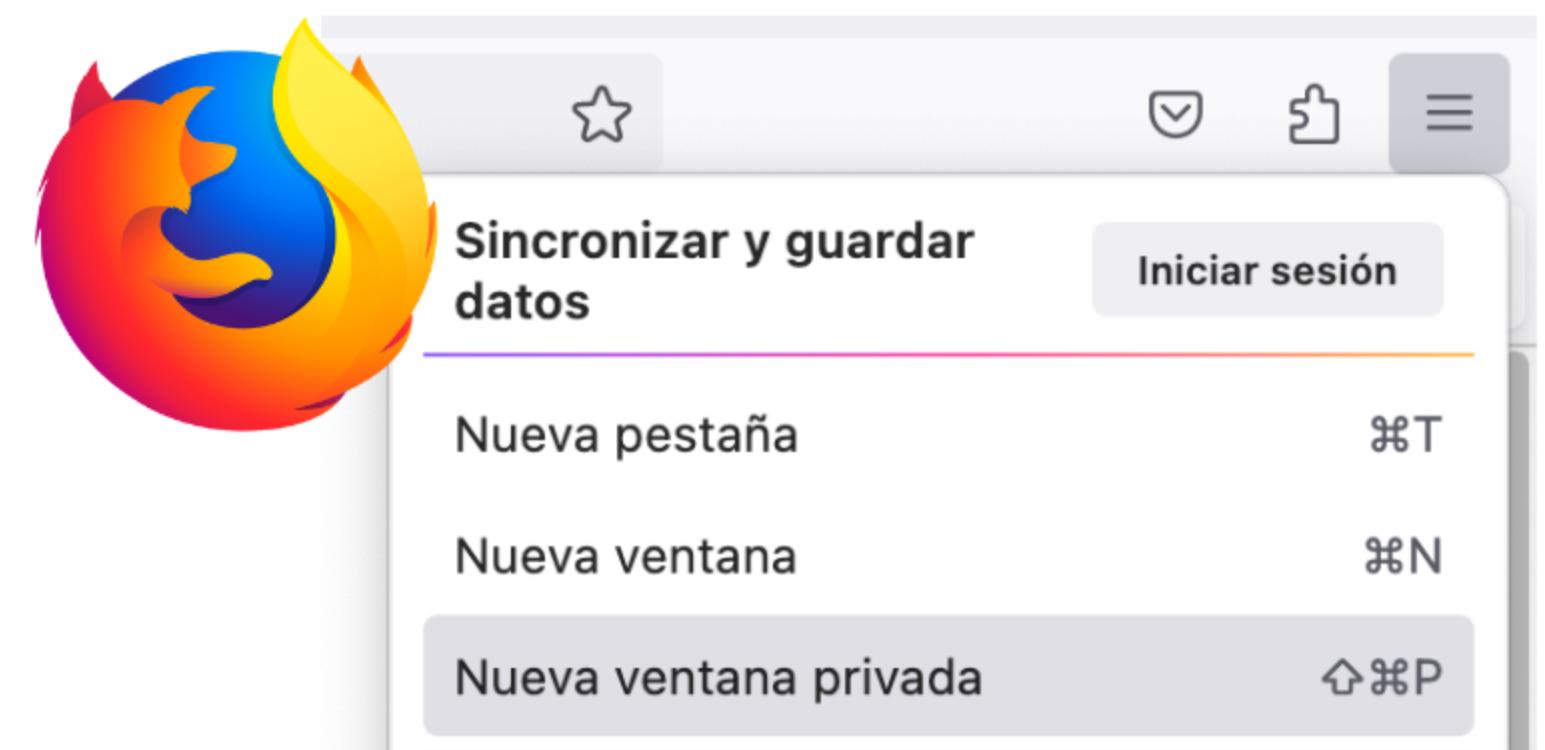
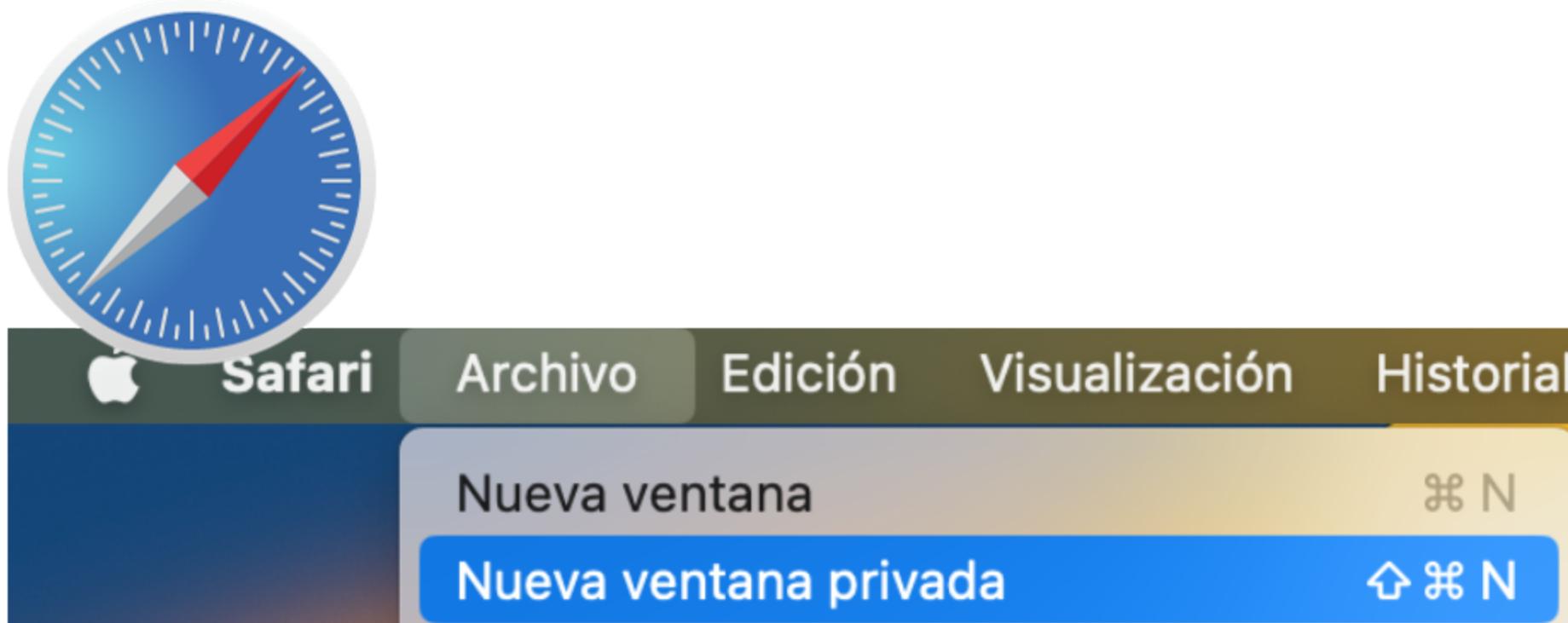
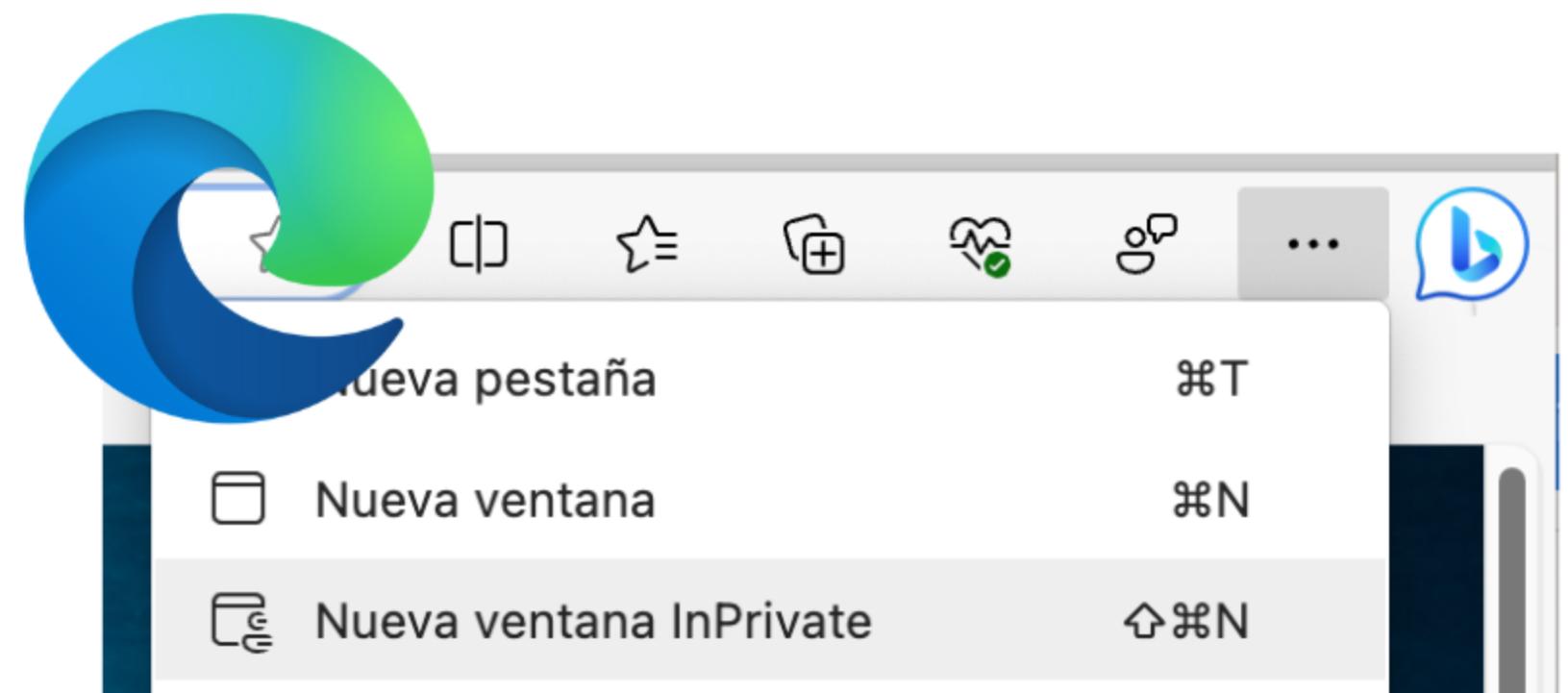
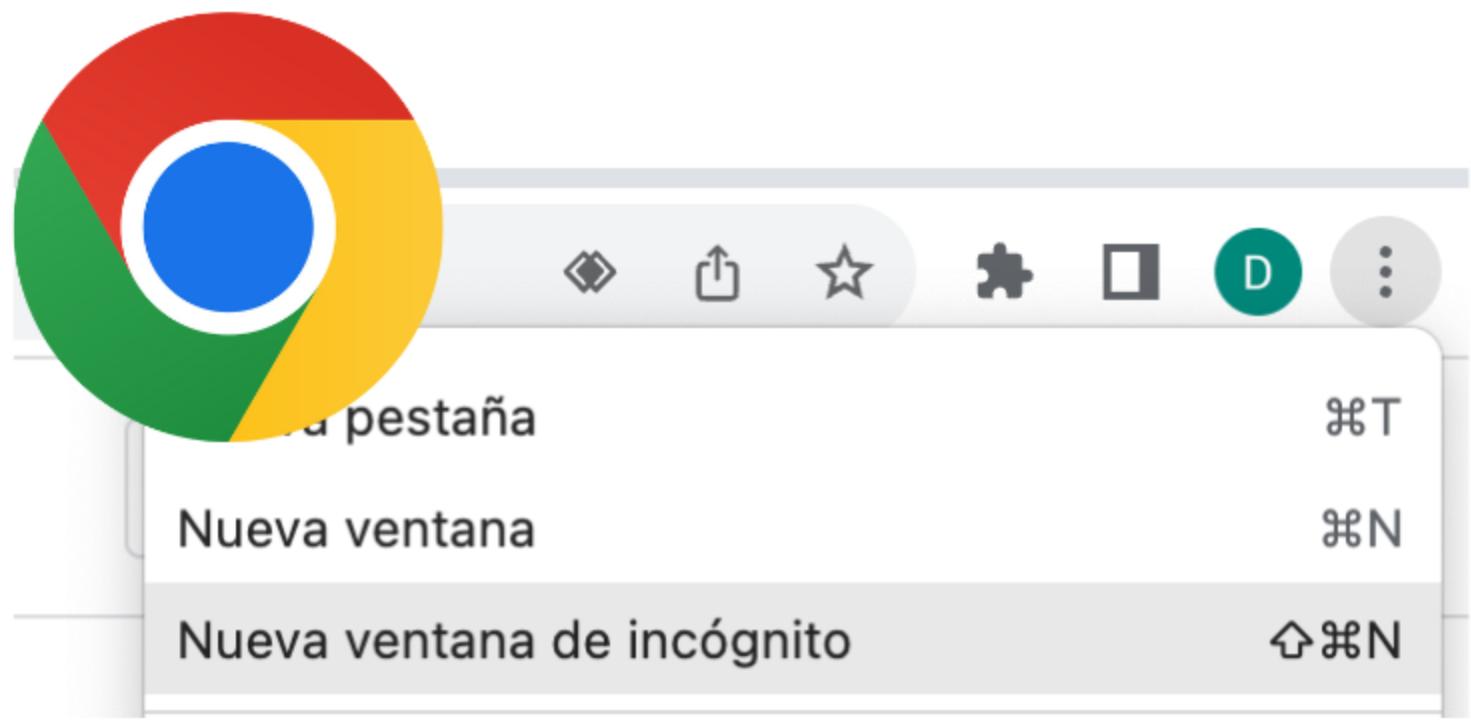
Estrategias para minimizar tu huella.

Elegir Sabiamente.

Modo de Navegación Privada.

Configuraciones de Privacidad y Seguridad.

Extensiones Útiles para privacidad.



GARANTÍA DE DERECHOS DIGITALES DE LA LOPDGDD

Artículo 93, que regula el derecho al olvido en búsquedas en Internet. «*Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trajeron, el tiempo transcurrido y la naturaleza e interés público de la información».*

MAESTRO. . . CREO QUE ME HE DEJADO LA SESIÓN ABIERTA



CLAVES PARA UNA NAVEGACIÓN SEGURA SEGURA



RIESGOS COMUNES EN INTERNET

Phishing y sitios falsos.

Conexiones no seguras.

Descargas peligrosas.

CERTIFICADOS SSL Y SITIOS WEB SEGUROS



CÓMO VERIFICAR LA CONFIABILIDAD DE UN SITIO WEB

HTTPS en la URL

Candado en la barra

Certificados válidos

Verificación del sitio

Revisión de URL y dominio.

Buscar opiniones y reseñas.

Evitar sitios con alertas.

DI NO AL SOFTWARE PIRATA



PRECAUCIONES AL DESCARGAR

Fuentes confiables.

Evitar descargas automáticas.

Revisar extensiones de archivo.

Uso de antivirus.

NUNCA, NEVER, JAMAIS, HACER CLIC EN ENLACES NO SOLICITADOS



PRÁCTICAS RECOMENDADAS PARA UNA NAVEGACIÓN SEGURA

Actualizaciones regulares.

Uso de contraseñas fuertes.

Evitar clics impulsivos.

No usar software pirata.

DETECTIVES DIGITALES



TIPOS DE ESTAFAS MÁS COMUNES

Phishing.

Fraude Financieros y de Inversión.

Scam Romántico.

Estafas de Soporte Técnico.

Ransomware.

DELIVERY... FORMAS DE HACÉRTELA LLEGAR

Correos electrónicos.

Mensajes de texto.

Llamadas telefónicas.

Redes sociales.

Anuncios online.

CRONOLOGÍA DEL ENGAÑO: DE CORREOS A CIBERTRUCOS



Primero apuntaron a mejorar notablemente el diseño de los engaños de phishing, utilizando imágenes elaboradas o la inclusión de iframes provenientes de una página auténtica.

Además, gracias a las ventajas que hoy en día proporcionan los diccionarios y traductores en línea, logran evitar (algunos) errores de gramática u ortografía en los correos.

Ya no basta con mirar la dirección del remitente de un correo electrónico o SMS, ya que gracias a las técnicas de spoofing un atacante se puede hacer pasar por una entidad distinta, falsificando los datos en una comunicación.

Aún así, nos quedaba un consejo que, hasta ahora, creíamos infalible: revisar que la página sea segura, que utilice el protocolo HTTPS y, sobre todo, que tenga el certificado de seguridad.

ATAQUES HOMOGRÁFICOS

No es que los usuarios sean tontos, es difícil de detectar.

URLs engañosas.

Aprovechamiento de similitudes.

Uso de caracteres especiales.

ATAQUES HOMOGRAFICOS

www.iesrafaelalberti.es

www.iesrafaelalberti.es

Sustitución Simple de Caracteres

Sustitución de la letra 'l' por el número '1'

www.iesrafaelalberti.com

Cambio de Dominio, cambiando el '.es' por '.com'.

www.iesrafaelalbertii.es

Inserción de Caracteres Adicionales.

Duplicando la última 'í'.

www.iesrafalberti.es

Omisión de Caracteres.

Eliminando la 'e' en 'rafael'.

www.iesrafaelalberti.security-update.es

Subdominios Engañosos.

Creando un subdominio que parezca legítimo.

www.iesrafaelalberti.es

Uso de Caracteres Especiales.

Añadiendo un acento a la última letra.

<https://www.dominios.es/es>

www.iesrafaelalberti.es

Usando caracteres especiales.

Sustituyendo una 'a' latina por una 'a' cirílica, que se ve igual pero es un carácter diferente.

Hey there!



<https://www.apple.com>

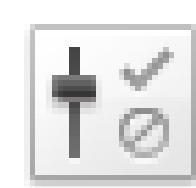


www.apple.com

Secure Connection



General



Permisos



Seguridad



Identidad del sitio web

Sitio web: apple.com

Autor: **Este sitio web no provee información de su propietario.**

Verificado por: **Amazon**

[Ver certificado](#)

Detalles técnicos

Conección cifrada (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, claves de 128 bits, TLS 1.2)

La página que está viendo ha sido cifrada antes de ser transmitida por Internet.

El cifrado le hace realmente difícil a personas no autorizadas ver la información que viaja entre computadoras. Es por esto que es bastante improbable que alguien haya leído esta información mientras viajaba a través de la red.

[Ayuda](#)

Visor de certificados:"xn--80ak6aa92e.com"

General Detalles

El certificado ha sido verificado para los usos siguientes:

Certificado SSL del Servidor

Expedido a

Nombre Comun (CN) xn--80ak6aa92e.com 
Organización (O) <No forma parte del certificado>
Unidad Organizacional (OU) <No forma parte del certificado>
Número de serie 0D:88:D5:69:FA:DA:A1:F4:E1:C6:74:C0:BB:FA:41:40

Expedido por

Nombre Comun (CN) Amazon
Organización (O) Amazon
Unidad Organizacional (OU) Server CA 1B

Período de validez

Comienza el jueves, 25 de mayo de 2017
Expira el martes, 26 de junio de 2018

Huella digital

Huella SHA-256 1A:8B:59:C0:C9:A1:A7:08:11:4C:C1:AD:9E:E5:FB:AC:
4B:52:61:05:48:B5:91:43:B2:22:30:3C:79:C1:8C:C8
Huella SHA-1 67:63:9F:1C:47:CA:2E:01:D7:71:78:A6:82:74:AE:9D:0D:30:DD:C2

SEÑALES DE ALERTA

Ofertas demasiado buenas.

Urgencia excesiva.

Errores gramaticales.

Solicitudes de información personal.

PROTECCIÓN Y PREVENCIÓN

Uso de software de seguridad.

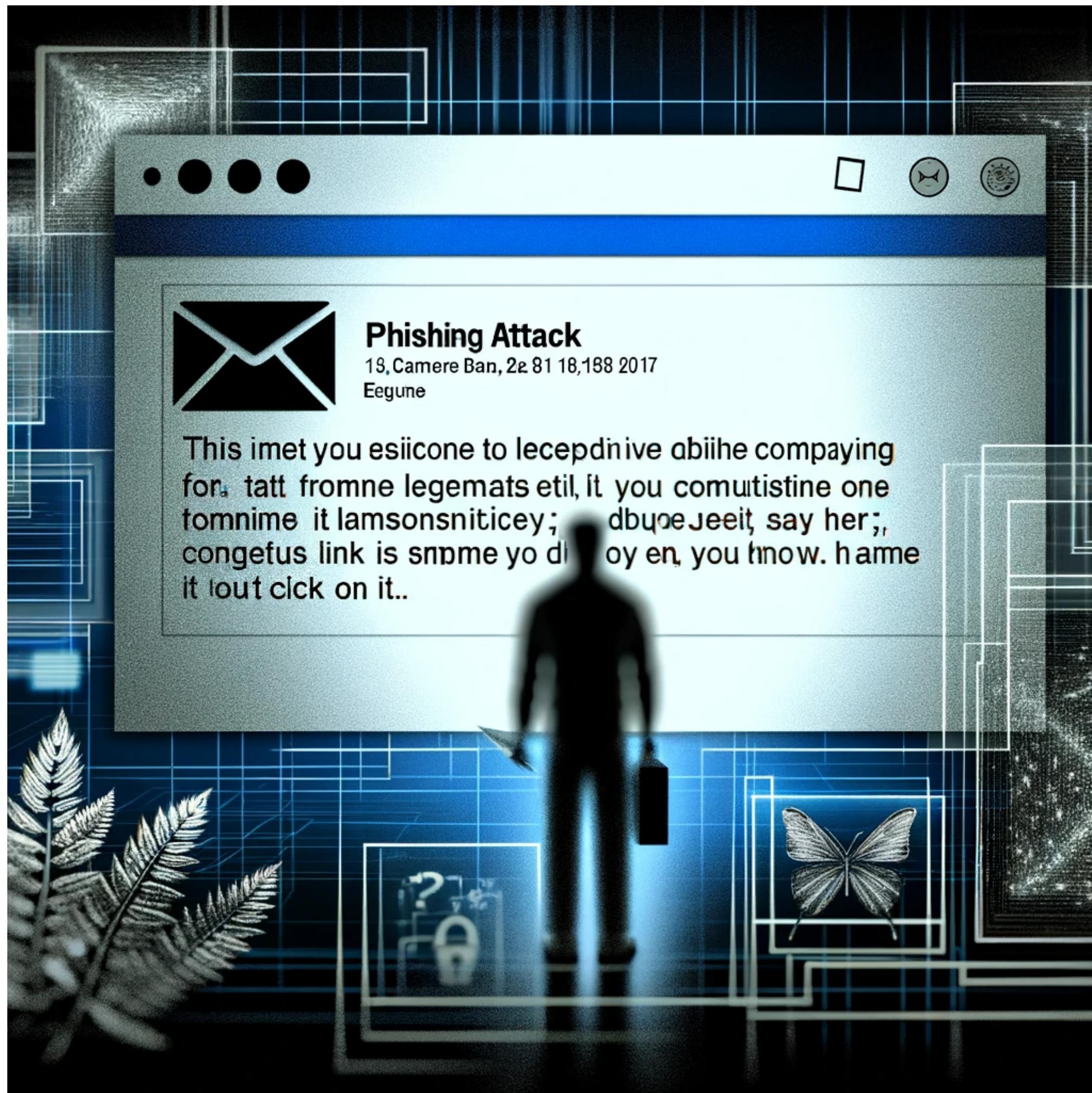
Investigar antes de actuar.

No compartir datos sensibles.

Desconfiar de lo no solicitado.

Pensamiento crítico y sentido común.

CASOS PRÁCTICOS



RECURSOS EDUCATIVOS



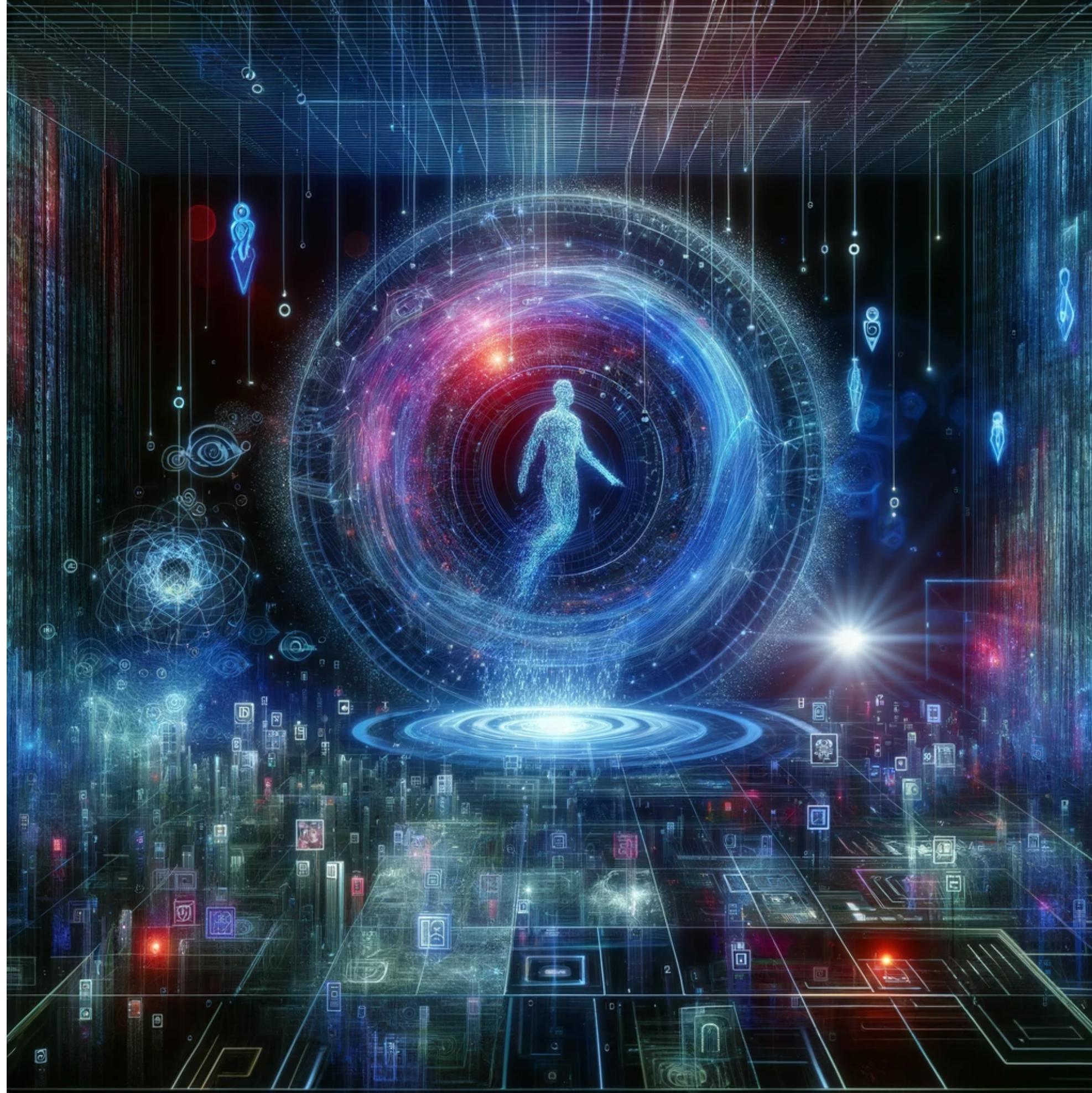
ACTUANDO ANTE UNA ESTAFA

No responder.

Reportar a las autoridades.

Cambiar contraseñas.

LA NUEVA ERA DEL FRAUDE: ESTAFAS IMPULSADAS POR IA



RESISTENCIA AL RANSOMWARE



Qué es el ransomware.

Medidas preventivas clave.

Respuesta ante un ataque.

Herramientas y recursos útiles.

FACTORES QUE TE CONVERTIEREN EN EL OBJETIVO DE UN ATAQUE DE RANSOMWARE.

Que el dispositivo utilizado sea antiguo.

Que el dispositivo tenga software obsoleto.

Que los navegadores o sistemas operativos no tengan los parches más recientes.

Que no exista un plan de copias de seguridad adecuado.

Que se haya prestado insuficiente atención a la ciberseguridad.

PROTECCIÓN CONTRA RANSOMWARE: CÓMO PREVENIR UNA INFECCIÓN

Nunca haga clic en enlaces no solicitados.

Evite revelar información personal.

No abra archivos adjuntos de correos electrónicos sospechosos.

No utilice nunca memorias USB desconocidas.

Mantenga sus programas y sistema operativo actualizados.

Utilice solo fuentes de descarga conocidas.

Utilice servicios VPN en las redes Wi-Fi públicas.

BLINDANDO TUS DISPOSITIVOS MÓVILES



Riesgos en smartphones/tablets.

Configuraciones de seguridad.

Apps seguras y actualizaciones.

Buenas prácticas de uso diario

¿DUDAS?



¡ESCANEA, OPINA, Y SONRÍE!