

### Cyber noticias

**Campaña de Phishing EvilProxy dirigida a 120.000 usuarios de Microsoft 365.** EvilProxy está emergiendo como una de las plataformas de Phishing más destacadas para apuntar a cuentas que cuentan con protección autenticación multifactor MFA. Los investigadores han detectado el envío de más de 120.000 correos electrónicos con Phishing a más de un centenario de organizaciones con el fin de comprometer las cuentas de Microsoft 365. Esto genera una alerta sobre el aumento drástico de incidentes exitosos a cuentas en la nube durante los últimos cinco meses. Fuente: [Bleepingcomputer](#).

**Nueva característica de seguridad de Android 14: los administradores de TI ahora pueden deshabilitar las redes 2G.** Google ha implementado una nueva función de seguridad en Android 14, que da la posibilidad a los administradores de tecnología deshabilitar la compatibilidad con redes 2G de los dispositivos móviles. Las redes 2G presentan vulnerabilidades debido a su cifrado limitado y la ausencia de autenticación mutua, lo que las hace susceptibles a ataques como la interceptación de datos y el descifrado del tráfico al hacerse pasar por una torre 2G legítima. Fuente: [Thehackernews](#).

**Nuevo malware Rilide, ataca a usuarios empresariales para extraer credenciales.** El malware Rilide es una extensión maliciosa para navegadores que fue identificada por Trustwave SpiderLabs en mes de abril. La versión más reciente de este malware parece estar enfocada en obtener credenciales de acceso a usuarios en entornos empresariales, así como carteras de criptomonedas. Además, captura imágenes de pantalla a intervalos predefinidos y transfiere la información sustraída a través de un canal de Telegram. Fuente: [Escudodigital](#).

**Según IBM, la filtración de datos tiene un costo de 4,45 millones de dólares.** La división de ciberseguridad IBM Security, ha lanzado en su informe anual acerca del costo relacionado con la filtración de datos, un promedio a nivel mundial sobre incidentes de esta índole ha llegado a los 4,45 millones de dólares, lo que representa un incremento del 15% en los últimos 3 años. Además, el estudio señala que los costos relacionados con la detección y el manejo de estos incidentes, han experimentado un aumento del 42% en el mismo periodo. Fuente: [Escudodigital](#).

## Modalidad más reportada al CAI Virtual ;Phishing!

A través del servicio CAI Virtual, la ciudadanía ha reportado una campaña de **Phishing**, la cual mediante la modalidad de suplantación de sitios web, informan a usuarios de tecnología Apple, la inhabilidad temporal de su cuenta iCloud por temas de seguridad. El objetivo de esta campaña, es realizar la captura de credenciales de acceso a los servicios de iCloud y obtener acceso a la información personal como contactos, imágenes y realizar configuraciones del dispositivo.

Este correo está asociado al asunto: **"LA CUENTA HA DESACTIVADO TEMPORALMENTE LA VERIFICACIÓN AHORA"**

1 El correo adjunto, solicita al usuario que para reactivar presuntamente su cuenta iCloud, deber dar clic en **"Actualizar cuenta"**.

Verificación de Cuenta <[kky3d3a39hbpki38jkky3d3@paulinekenny.com](mailto:kky3d3a39hbpki38jkky3d3@paulinekenny.com)> escribió:

2 Al dar clic sobre el enlace, es remitido a un sitio web, simulando ser el portal de acceso a la plataforma de iCloud.

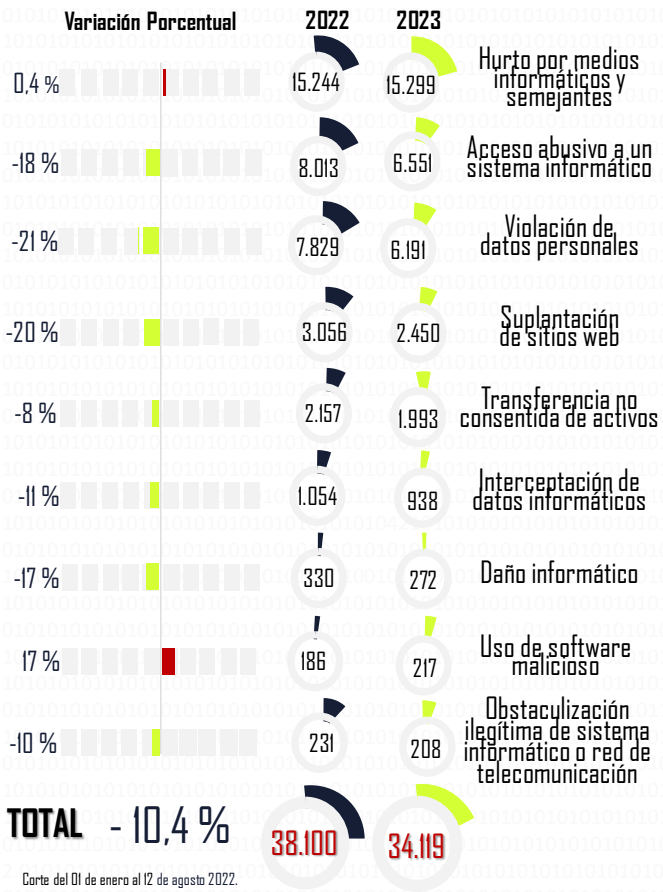


3 Después, le solicitará a la persona digitar las credenciales de acceso de la cuenta iCloud en la presunta plataforma y dar por terminada la fase de captura de datos.

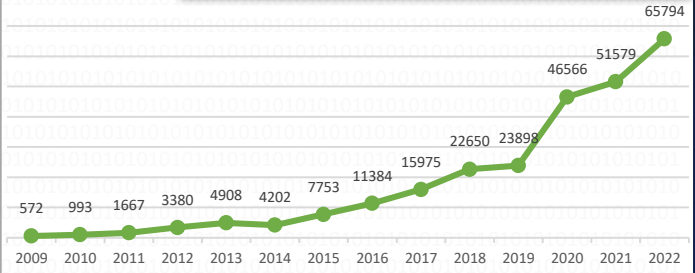
### RECOMENDACIONES

- EVITE dar clic sobre links o abrir archivos adjuntos en correos electrónicos desconocidos.
- VERIFIQUE ortografía y redacción, usualmente hay errores.
- UTILICE la autenticación de dos factores en su cuenta de servicios iCloud para aumentar la seguridad de la esta y evitar accesos no autorizados.
- No ingrese ningún tipo de información en el formulario mostrado en este sitio web.
- VERIFIQUE los enlaces o archivos antes de ejecutarlos en un entorno de prueba (sandbox), Ej: [Any.Run](#), [Csirt.Ponal](#).
- REPORTE el correo electrónico allegado, a través de nuestro canal de atención del CAI Virtual <https://caivirtual.policia.gov.co>

# Balance Cibercriminalidad - Ley 1273/09



## Evolución histórica (No. Denuncias vs año)



## Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto. No. Eventos, %)

Fuente: SIECOO Plus 2.0



Las denuncias a la fecha representan el 52% del total del 2022.  
Corte del 01 de enero al 12 de agosto 2023.

# Actividades de gestión en seguridad digital

### Capturas

Delitos informáticos.  
Explotación sexual infantil en Internet.

154

60

214

412

### Alertas y contenidos preventivos

15 durante la semana

### Incidentes gestionados

a través del CAI Virtual

9.809

140

### Actividades de relacionamiento

estratégico, resaltando en la semana:



### Charlas de ciberseguridad

Personas impactadas 11.024

96

19.240

### Páginas bloqueadas

Material de abuso sexual infantil.  
Juegos ilegales de azar.

17.739

1.501

Para sugerencias sobre este producto, por favor diligencie este formulario: <https://bit.ly/3mz5C8d>



# Canales de atención y redes sociales



Página web



X



Instagram



Facebook



Threads



WhatsApp