Bienvenidos

# BOLETÍN CYBER seguridad

Boletín 012
2025

Oficina de Tecnologías de la Información y las Comunicaciones TIC's
Alcaldía de Paipa

# 1 Ransomware como Servicio (RaaS): Blindando la Infraestructura

**El Ransomware es una amenaza crítica. Un ataque exitoso puede cifrar los sistemas de gestión de trámites, las bases de datos de ciudadanos o las nóminas, interrumpiendo servicios esenciales.** Los atacantes ven a las entidades públicas como blancos vulnerables que se verán forzados a pagar rápidamente para restablecer la atención a la ciudadanía.

## ¿Cómo evitarlo desde tu rol?

- **Gestión de Credenciales:** Nunca uses la misma contraseña de tu cuenta de trabajo para servicios personales. Un solo compromiso abre la puerta a toda la red.
- **Reporte de Sospechas:** Si notas cualquier lentitud, aparición de archivos extraños o solicitudes de rescate en pantalla, informa de inmediato al equipo de tecnología de la Alcaldía.
- **Concientización:** El eslabón más débil es el humano. Evita hacer clic en enlaces sospechosos para no ser la puerta de entrada de este malware.

Oficina de Tecnologías de la Información y las Comunicaciones TIC's
Alcaldía de Paipa

# 2 Ingeniería Social en Plataformas de Colaboración (Teams, Zoom)

**Los atacantes se hacen pasar por personal de TI, secretarios o directivos, enviando mensajes urgentes a través de chats internos de la entidad.** El objetivo es robar tus credenciales de acceso a la red de la Alcaldía o engañarte para que abras un documento infectado (malware en archivos de oficina) que parece venir de un colega de confianza.

## ¿Cómo evitarlo desde tu rol?

- **Verificación Cruzada:** Si un superior o compañero te pide datos confidenciales o que instales algo, verifica por otro medio (una llamada telefónica) antes de actuar.

- **Cuidado con Archivos Adjuntos:** Desconfía de archivos adjuntos inesperados que se presenten como peticiones o convocatorias, incluso si parecen venir de una fuente legítima.

- **Nunca desactives Macros:** Si un documento de Word o Excel te pide que desactives las macros, **¡NO LO HAGAS!** e informa inmediatamente al equipo de tecnología.

# 3 Abuso de Cuentas Inactivas o Desatendidas (Shadow IT)

**Una cuenta antigua de un ex-funcionario o un servicio en la nube (como un portal para compartir documentos)** que fue instalado sin supervisión oficial, puede ser una vulnerabilidad crítica para la Alcaldía. **El atacante usa estas cuentas olvidadas para acceder a información pública clasificada** o para lanzar ataques más grandes.

## ¿Cómo evitarlo desde tu rol?

- **Limpieza Constante:** Si tienes cuentas que ya no utilizas para trabajar, solicita su desactivación o elimínalas para reducir las posibles vulnerabilidades.
- **No Usar Servicios Personales:** Evita instalar o usar servicios en la nube o aplicaciones no aprobadas por la entidad (Shadow IT) para manejar documentos de la Alcaldía.
- **Control de Permisos:** Si utilizas una aplicación autorizada, asegúrate de que solo tenga los permisos estrictamente necesarios para tu función.

# 4 Fraude con Pagos Digitales Móviles (Cuentas Suplantadas)

**Las transferencias fraudulentas son un riesgo doble: fraude al ciudadano** (cuando la entidad es suplantada para pedir pagos falsos) o **fraude a la Alcaldía** (cuando un atacante intenta que un funcionario o proveedor realice un pago a una cuenta suplantada). En Colombia, los atacantes simulan ser de entidades gubernamentales (DIAN, Sisbén o la Alcaldía misma) para robar dinero

## ¿Cómo evitarlo desde tu rol?

- **Verifica Canales Oficiales:** Si recibes una notificación de pago o transferencia de la Alcaldía por un medio inusual (WhatsApp, correo personal), siempre accede escribiendo la dirección web de forma manual en tu navegador o llamando a un número oficial.
- **No te dejes Presionar:** Los fraudes telefónicos (Vishing) usan el sentido de urgencia ("será bloqueado", "debe pagar de inmediato") para evitar que verifiques.
- **Cuidado con Códigos QR de Pago:** En puntos de recaudo o información, asegúrate de que los códigos QR no hayan sido reemplazados por copias falsas que redirigen a cuentas suplantadas.

Oficina de Tecnologías de la Información y las Comunicaciones TIC's
Alcaldía de Paipa

# 5 Ataques "Man-in-the-Middle" en Redes Wi-Fi Públicas

**Como funcionario que asiste a eventos, conferencias o reuniones fuera de la oficina, usar redes Wi-Fi públicas (aeropuertos, cafeterías) es un alto riesgo.** Un atacante puede interceptar y **robar la información sensible** que envías (incluyendo tus credenciales de la Alcaldía) mientras estás conectado a esa red no segura

## ¿Cómo evitarlo desde tu rol?

- **Evita Transacciones Sensibles:** Nunca inicies sesión en cuentas de trabajo, realices trámites bancarios, o ingreses información sensible de la Alcaldía mientras estés conectado a una red Wi-Fi pública.

- **Usa Redes Móviles Seguras:** Si necesitas acceder a datos de trabajo fuera de la oficina, prefiere usar los datos móviles de tu dispositivo, ya que son más seguros que una Wi-Fi pública.

- **Verifica la Red:** Pregunta siempre al personal del lugar por el nombre exacto de la red Wi-Fi. Los atacantes crean redes falsas con nombres muy similares a las oficiales.

Oficina de Tecnologías de la Información y las Comunicaciones TIC's
Alcaldía de Paipa