

Pasto, 30 de septiembre de 2026

CIRCULAR No. 027

PARA: SECRETARIOS, SUBSECRETARIOS, DIRECTORES DE DEPARTAMENTO, JEFES Y COORDINADORES DE OFICINA, PERSONAL DE PLANTA, CONTRATISTAS Y DEMÁS FUNCIONARIOS DE LA ADMINISTRACIÓN MUNICIPAL.

ASUNTO: Alerta de seguridad digital por campaña de correos maliciosos dirigida a entidades públicas y solicitud de copias de seguridad de programas y aplicativos.

La Subsecretaría de Sistemas de Información, en atención a la alerta emitida por el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) el 25 de septiembre de 2026, informa a todo el personal de la entidad que se encuentra activa una campaña de ciberataques dirigida a funcionarios de entidades públicas colombianas, atribuida al grupo criminal conocido como BlindEagle (APT-C-36).

Adicionalmente, en las últimas semanas se han conocido intentos de fraude contra entidades territoriales del país orientados a la sustracción de recursos públicos a través de medios digitales. Por esta razón, es indispensable que cada funcionario conozca esta amenaza, adopte medidas de prevención y que las dependencias protejan la información a su cargo.

1. ¿En qué consiste el ataque?

Los atacantes envían correos electrónicos que aparentan ser notificaciones judiciales, utilizando cuentas institucionales .gov.co reales que previamente fueron comprometidas, por lo cual el remitente puede parecer confiable. Las principales características identificadas son:

- **Asunto:** de temática judicial, como "Traslado de demanda", con amenaza de consecuencias legales en un plazo de pocos días.
- **Archivo adjunto:** con extensión .xhtml, .html o .svg, con nombres que simulan citaciones de juzgados, por ejemplo: "armenia 10112026 MIN-pasto.xhtml".
- **Contraseña en el correo:** el mensaje incluye una clave (por ejemplo THG2026) para abrir un archivo comprimido (.zip) que se descarga automáticamente al abrir el adjunto.
- **Documento señuelo:** tras la infección se muestra un PDF falso de un juzgado para que la víctima no sospeche.

NIT: 891280000-3

CAM Anganoy - los Rosales II

Teléfono: +57 (602) 7244326 Ext: 1301

Correo electrónico: contactenos@pasto.gov.co

- Es su responsabilidad ecológica imprimir este documento -

Al abrir el adjunto se instala de forma silenciosa un programa espía que permite a los delincuentes controlar el equipo sin que el usuario lo note, registrar todo lo que se escribe en el teclado, robar contraseñas y sesiones abiertas de correo, plataformas y portales bancarios, tomar capturas de pantalla, activar el micrófono y la cámara, y copiar o eliminar archivos. Este tipo de acceso puede ser utilizado para suplantar funcionarios, alterar información o realizar transacciones fraudulentas.

2. Medidas que debe adoptar todo el personal

- NO abrir archivos adjuntos con extensión .xhtml, .html, .svg, .js o .vbs, ni archivos comprimidos protegidos con contraseña, aunque provengan de cuentas conocidas o de otras entidades .gov.co.
- Desconfiar de cualquier correo que genere urgencia, amenazas legales, plazos cortos o solicitudes de pago, cambio de cuentas bancarias o envío de credenciales.
- Ante una notificación judicial, verificarla directamente con la Oficina Jurídica o por los canales oficiales de la Rama Judicial, nunca a través de los enlaces o adjuntos del correo.
- No compartir usuarios, contraseñas, tokens ni códigos de verificación con ninguna persona, incluso si dice pertenecer a la Subsecretaría de Sistemas de Información o a una entidad bancaria.
- Toda solicitud de pago, transferencia o modificación de datos bancarios de proveedores o contratistas debe confirmarse por un segundo medio (llamada telefónica a un número conocido o de manera presencial) antes de ser tramitada.
- Si ya abrió un archivo sospechoso o nota comportamientos extraños en su equipo (lentitud, ventanas que se abren solas, cierre de sesiones), desconecte el equipo de la red (cable o Wi-Fi), no lo apague, y comuníquese de inmediato con la Subsecretaría de Sistemas de Información.
- No reenviar el correo sospechoso a otros compañeros; repórtelo a la Subsecretaría de Sistemas de Información para su análisis.

3. Solicitud de copias de seguridad a las dependencias

Teniendo en cuenta que este tipo de ataques puede ocasionar la pérdida, el secuestro o la alteración de la información institucional, se solicita a cada una de las dependencias que administren o utilicen programas, aplicativos, sistemas de información o bases de datos propios (misionales, financieros, contables, de trámites o de atención al ciudadano) realizar de manera inmediata copias de seguridad de dicha información, atendiendo las siguientes indicaciones:

NIT: 891280000-3
CAM Anganoy - los Rosales II
Teléfono: +57 (602) 7244326 Ext: 1301
Correo electrónico: contactenos@pasto.gov.co
- Es su responsabilidad ecológica imprimir este documento -

- Realizar una copia de seguridad completa de las bases de datos, archivos de configuración y documentos asociados a cada aplicativo.
- Almacenar las copias en al menos dos ubicaciones distintas, una de ellas desconectada de la red institucional (disco externo o medio extraíble custodiado por el responsable de la dependencia).
- Verificar que las copias puedan restaurarse correctamente y que la información se encuentre completa.
- Establecer una periodicidad mínima de copias (diaria, semanal o mensual según la criticidad de la información) y designar un responsable.
- Revisar que solo el personal autorizado tenga acceso a los aplicativos y retirar los usuarios de personal desvinculado.

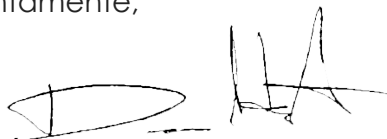
Una vez realizadas las copias, cada dependencia deberá remitir un reporte que indique:

- Dependencia y subdependencia
- Nombre del programa o aplicativo
- Nombre del responsable y cargo
- Fecha de la copia de seguridad realizada
- Ubicación o medio de almacenamiento de la copia
- Periodicidad establecida

El plazo máximo para el envío de este reporte será hasta el 9 de octubre de 2026, al correo electrónico soportesistemas@pasto.gov.co. La Subsecretaría de Sistemas de Información brindará el acompañamiento técnico a las dependencias que lo requieran.

Se agradece a todos su colaboración y atención a estas recomendaciones, las cuales contribuyen a proteger la información institucional, los recursos públicos y la confianza de la ciudadanía. Para reportar correos sospechosos o recibir orientación, pueden comunicarse con la Subsecretaría de Sistemas de Información a través del teléfono (ext. 1301) o al correo electrónico soportesistemas@pasto.gov.co.

Atentamente,



DARÍO FERNANDO ALFARO FIGUEROA
Subsecretario Sistemas de Información

Proyecto: ANDERSON FELIPE SALAZAR CASTILLO
Cargo: Técnico operativo.
Dependencia: Subsecretaría de Sistemas de Información.

NIT: 891280000-3
CAM Anganoy - los Rosales II
Teléfono: +57 (602) 7244326 Ext: 1301
Correo electrónico: contactenos@pasto.gov.co
- Es su responsabilidad ecológica imprimir este documento -