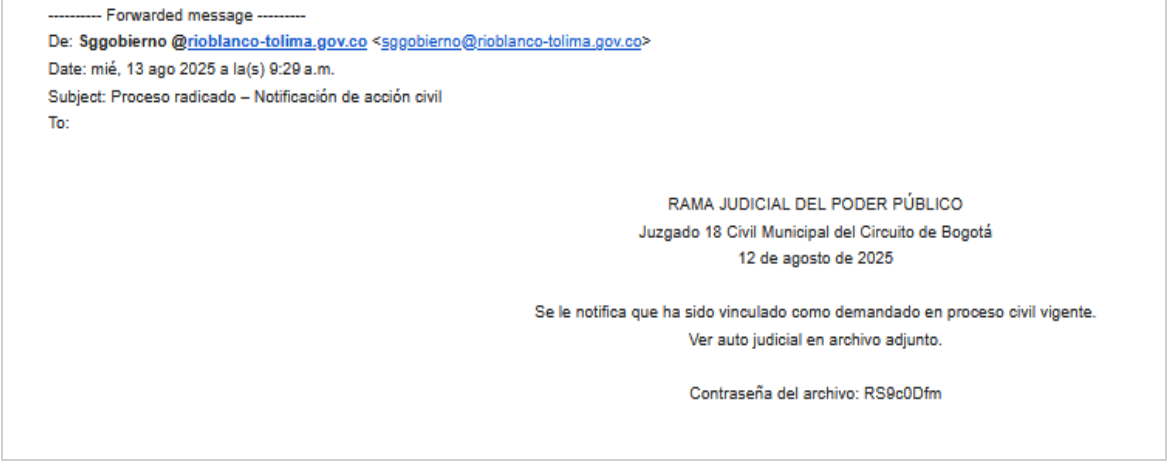
Agosto 20 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Scr.MalSvg!gen2
Cuenta de correo del remitente:	sggobierno@rioblanco-tolima.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Sggobierno @rioblanco-tolima.gov.co** <sggobierno@rioblanco-tolima.gov.co>
Date: mié, 13 ago 2025 a la(s) 9:29 a.m.
Subject: Proceso radicado – Notificación de acción civil
To:

RAMA JUDICIAL DEL PODER PÚBLICO
Juzgado 18 Civil Municipal del Circuito de Bogotá
12 de agosto de 2025

Se le notifica que ha sido vinculado como demandado en proceso civil vigente.
Ver auto judicial en archivo adjunto.

Contraseña del archivo: RS9c0Dfm

El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido identificado y abordado por este Equipo. Se ha detectado un evento de phishing dirigido a miembros de nuestra comunidad. Es preciso indicar que la técnica de Phishing es un tipo de ataque cibernético en el cual los adversarios intentan engañar a los usuarios para que se revele información confidencial, como contraseñas, números de tarjetas de crédito o información personal.

Se ha realizado la respectiva indagación y se han identificado una serie de indicadores de compromiso (IoCs) asociados con este asunto.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	01_notificacion_demanda_laboral_juzgado_civil_18_BOGOTA_D.C (2)_cq3gikov.svg
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	August 20, 2025 at 15:08:02
MIME:	image/svg+xml
Información del archivo:	SVG Scalable Vector Graphics image
MD5:	FED7E2E5570740699DA87160F242F3DE
SHA1:	DAD8EE06A49711624851950DF111401FF537FA6E

SHA256:	DCFB512980164EC6BC223FC750A551CEA248285A4461E59A27D4E52B0B0555EA
SSDEEP:	3072:YRFE/CkiKx4tg7PehY8mf65OL7LlSNsgS8NrTuyXPRtudC8wfnysV22tVpj44hN1:qFxmiGXdSyQFPJAFxmiGXdSyQFPJi

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Program Files\Internet Explorer\iexplore.exe" "C:\Users\admin\AppData\Local\Temp\01_notificacion_demanda_laboral_juzgado_civil_18_BOGOTA_D.C (2)_cq3gikov.svg"	"C:\Program Files\Internet Explorer\iexplore.exe" "C:\Users\admin\AppData\Local\Temp\01_notificacion_demanda_laboral_juzgado_civil_18_BOGOTA_D.C (2)_cq3gikov.svg"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516