Instituto Nacional de Cancerología
Colombia
Por el control del cáncer

Fecha: 24 de febrero de 2026 | Ref: AL-20260222-095 -COLCERT

⚠ ALERTA DE SEGURIDAD DIGITAL ⚠

Correos Falsos sobre Jurados Electorales 2026

Información importante para todos los funcionarios del INC

Se ha detectado una campaña de engaño digital (phishing) que envía correos falsos haciéndose pasar por la Registraduría Nacional, informando a las personas que han sido designadas como jurados de votación para las elecciones de marzo de 2026. Si usted o alguien de su equipo recibe este tipo de mensaje, NO abra ningún archivo adjunto ni descargue nada.

¿Qué está pasando?

Delincuentes digitales están enviando correos electrónicos y mensajes de texto y whastapp diseñados para parecer oficiales de la Registraduría Nacional del Estado Civil con motivo de las elecciones del próximo 8 de marzo de 2026. El mensaje le dice que fue seleccionado como jurado de votación y le pide que abra un archivo para ver los detalles de su citación.

Ese archivo es un virus. Si lo abre, el programa malicioso se instala en su computador de manera silenciosa y sin que usted lo note.

¿Cómo funciona el engaño? — Paso a paso

El ataque ocurre en varios pasos sencillos de entender:

1	**Llega el correo falso:** Usted recibe un mensaje que parece oficial, con el logo y nombre de la Registraduría Nacional, informando su supuesta designación como jurado electoral.
2	**Le piden que descargue un archivo:** El correo incluye un archivo adjunto o un enlace. Al hacer clic, se descarga automáticamente un archivo comprimido (ZIP) a su computador.

3	**Le dan una contraseña para abrirlo:** El archivo viene protegido con la clave YHU120 (o una clave similar). Le dan esta contraseña en el mismo correo. Esto se hace para que el antivirus no detecte que es un virus.
4	**Se instala el virus en silencio:** Una vez que usted ingresa la contraseña y abre el archivo, el programa malicioso se instala sin mostrar ninguna advertencia ni ventana.
5	**El virus espía su actividad:** El programa roba contraseñas guardadas en su navegador, registra todo lo que usted escribe en el teclado y envía esa información a los delincuentes por internet.

Señales de alerta — ¿Cómo reconocer este correo /mensaje falso?

Desconfíe del mensaje si cumple alguna de estas características:

- Le notifican que es jurado de votación por correo electrónico con un archivo adjunto.
- El correo /mensaje viene con una contraseña para abrir el archivo (ej: YHU120 o similar).
- El archivo descargado tiene extensión .zip, .exe, .html o similar.
- El remitente tiene un dominio sospechoso (no termina en @registraduria.gov.co).
- Le piden actuar rápido o hay un tono de urgencia en el mensaje.

Recuerde: Las entidades del gobierno NUNCA envían citaciones oficiales como archivos comprimidos con contraseña. La Registraduría notifica a los jurados por medios oficiales, no por correos con archivos ejecutables.

Ejemplo del Mensaje de texto - Whatsapp

¿Qué debe hacer si recibe este correo o mensaje?

✓ SÍ DEBE HACER	✗ NO DEBE HACER
• Elimine el correo/mensaje inmediatamente. • Repórtelo a la mesa de ayuda del INC. • Avise a sus compañeros de trabajo. • Si ya abrió el archivo, apague el equipo y llame a la mesa de ayuda.	• No abra el archivo adjunto. • No haga clic en ningún enlace del mensaje. • No ingrese la contraseña YHU120 ni ninguna similar. • No reenvíe el correo a otras personas.

¿A quién contactar?

Si recibió este correo o sospecha que ya abrió el archivo malicioso, contáctese de inmediato con la mesa de ayuda del Instituto Nacional de Cancerología a la línea 7000 o al correo Sima@cancer.gov.co. No espere — entre más rápido se reporte, más fácil es proteger su información y la de la institución.

Recuerde: reportar a tiempo puede evitar consecuencias graves para usted y para la institución.

Buenas prácticas de seguridad digital

Aproveche este momento para recordar estos hábitos que le protegen en el día a día:

- Desconfíe de correos que le piden abrir archivos adjuntos inesperados, aunque parezcan oficiales.
- Verifique siempre el remitente: los correos oficiales del gobierno colombiano terminan en .gov.co
- Nunca ingrese contraseñas de archivos recibidos por correo sin confirmar con quien lo envió.
- Mantenga actualizado su sistema operativo y el antivirus de su equipo de trabajo.
- En caso de duda, consulte con el área de TI antes de abrir cualquier archivo o enlace.