Instituto Nacional de Cancerología Colombia
Por el control del cáncer

COLCERT

BOLETIN DE CIBERSEGURIDAD

JORNADA DE ELECCIONES PRESIDENCIALES

31 DE MAYO 2026

Gráfico: freepik

1 Boletín: Alerta de Seguridad Digital

Objetivos

- Dar a conocer los últimos vectores de ataque empleados por los atacantes sobre delitos cibernéticos.

- Establecer recomendaciones para los usuarios del INC para evitar ser el objetivo de ciberataques durante la jornada electoral del próximo 31 de mayo, correspondiente a las elecciones presidenciales de 2026.

¿Qué está pasando?

- Colombia registró cerca de **7.100 millones de intentos de ciberataques** en el primer semestre de 2025, manteniéndose entre los países más atacados de América Latina.
- El sector salud sigue siendo objetivo prioritario de ciberataques. En marzo, la **Superintendencia de Salud reportó más de 23 millones de ciberataques** en un solo mes, con robo de información de su plataforma documental.
- Los delincuentes ya usan **Inteligencia Artificial para engañar a las personas:** videos y noticias falsas (deepfakes), correos que imitan a o entidades o personalidades reales, y llamadas fraudulentas cada vez más convincentes.
- Con las elecciones presidenciales los ataques aumentan: los ciberdelincuentes aprovechan la coyuntura y la inmediatez informativa para lanzar **campañas masivas de fraude y robo de datos.**

2 Ataque Superintendencia de Salud

El ataque a la Superintendencia Nacional de Salud ocurrió en marzo de 2026, convirtiéndose en uno de los incidentes de ciberseguridad más significativos del sector salud en Colombia.

Los atacantes explotaron vulnerabilidades en el sistema de gestión documental SUPERARGO, logrando acceso no autorizado y la descarga masiva de información institucional sensible. La entidad detectó la actividad anómala mediante sus sistemas de monitoreo y bloqueó los accesos comprometidos.

El tipo de ataque empleado fue de acceso y exfiltración de datos, utilizando técnicas avanzadas combinadas con herramientas de inteligencia artificial para evadir controles de seguridad.

En total, la entidad registró más de 23 millones de intentos de ciberataque en un solo mes, de los cuales una parte logró comprometer el 1,6% de su bodega documental, exponiendo información de entidades del sistema de salud colombiano.

La SuperSalud restableció sus servicios e inició acciones legales contra los responsables, reforzando sus controles de seguridad perimetral y monitoreo continuo.

COMO ATACARON SUPERSALUD

- **Reconocimiento y escaneo del sistema SUPERARGO**

- **Explotación de vulnerabilidades de acceso**

- **Acceso no autorizado y desplazamiento lateral**

- **Descarga masiva y exfiltración de datos institucionales**

- **Extorsión, y exposición de información en internet y Dark Web**

3 Vectores de ataque

- **NOTICIAS Y ENCUESTAS FALSAS** sobre candidatos y eventos durante la jornada, discusión política, comportamiento del dólar, fraude, terrorismo, pánico económico.
- **GENERACIÓN DE CONTENIDO DIFAMATORIO** como injurias, calumnias, noticias falsas, estigmatización, polarización, aprovechado también para recabar datos e información personal
- **DISTRIBUCIÓN DE CÓDIGO MALICIOSO** (malware) en archivos adjuntos o enlaces de correo relacionados con las elecciones.
- **CAPTURA DE DATOS PERSONALES** a través de falsos portales, suplantación de correos, mensajería instantánea, encuestas, mensajes de texto o llamadas telefónicas.
- **SUPLANTACIÓN DE CORREOS, MENSAJES DE TEXTO, REDES SOCIALES Y CALL CENTERS** de registraduría, entidades públicas, medios de comunicación, sector bancario.
- **CIBER-EXTORSION Y SEXTING** con amenaza de difamación en redes sociales a cambio de dinero. Recepción de correos genéricos suplantando cuenta de entidades o personales, con amenazas de publicación de videos de contenido sexual y con solicitud de extorsión en bitcoins.
- **EXPLOTACIÓN DE VULNERABILIDADES** de sistemas operativos APLICACIONES y cuentas cloud, en equipos y dispositivos móviles sin actualizar o desatendidos.
- **SOBORNO O EXTORSION A FUNCIONARIOS** por grupos de ciberdelincuentes, solicitado información o entrega de cuentas y contraseñas corporativas.
- **ATAQUE DE CADENA DE SUMINSITRO,** mediate la explotación de vulnerabilidades de proveedores de servicios de internet, nube y comunicaciones, buscando causar gran afectación a gobierno y sectores productivos, con fines de lucro económico.

4 Desinformación
Fake News

Comprende la elaboración y difusión de contenidos falsos en internet o redes sociales con el objetivo de hacerlos pasar como noticia veraz, y que se utilizan para desinformar a la ciudadanía bajo la pretensión de afectar o influir en las decisiones democráticas en el marco de escenarios políticos y/o electorales.

En 2026, esta amenaza se ha intensificado **con el uso de Inteligencia Artificial generativa**, que permite crear videos, audios e imágenes sintéticas (deepfakes) y textos automatizados prácticamente indistinguibles de contenido real, lo que **hace significativamente más difícil su detección** tanto para los ciudadanos como para las plataformas digitales.

¿Cómo identificarlas?

Realice una revisión integral del contenido recibido y confróntelo con otras fuentes de información.

Gráfico: freepik

5 No caiga en el Phishing

El **phishing** es un método para engañarle y hacer que comparta contraseñas, números de tarjeta de crédito, y otra información confidencial o personal haciéndose pasar por una institución de confianza en un mensaje de correo electrónico, mensaje de redes sociales o llamada telefónica.

¿Cómo prevenirlo?

- **Realice una revisión inicial del origen y contenido recibido por correo y redes sociales**. No ejecute o descargue archivos adjuntos de remitentes que no conozca, o que parezcan sospechosos.

- **Verifique el certificado SLL (HTTPS) de las paginas a las que accede**. Digite siempre la dirección de los sitios web a los que quiere ingresar. Evite ingresar por links de origen desconocido o de dudosa procedencia.

- **Desconfíe de concursos, premios u ofertas demasiado tentadoras**. Evite registrar sus datos en campañas de mercadeo de origen desconocido. No use sus cuentas corporativas para registro de temas personales.

- **Evite suministrar información personal, contraseñas o códigos de verificación** por via telefónica, mensajes de texto o aplicaciones de mensajería instantánea.

6 Fraudes Online

Los fraudes online son un tipo de estafa que se lleva a cabo a través de Internet o medios digitales. Los estafadores utilizan una variedad de técnicas e ingenieria social para engañar a sus víctimas.

¿Cómo prevenirlos?

En el INC hemos preparado un recurso en el que recoge y comparte la información y buenas prácticas necesarias para que todos los usuarios seamos capaces de disfrutar de las ventajas que nos ofrece Internet, sin caer en las trampas con las que los ciberdelincuentes tratan de obtener un beneficio a nuestra costa.

Guía Aprendiendo a identificar fraudes online

A través de esta guía haremos un repaso de los tipos de fraudes más comunes que circulan por la Red, detallando en qué consisten y cómo detectar cada uno de ellos. Esta información evitará que caigamos en los engaños y nos permitirá disfrutar de Internet con mayor seguridad.

7 Recomendaciones

- Protejer sus datos personales usando opciones de privacidad , bloqueo automático de dispositivos, doble factor de autenticación de cuentas, y evite o publicar fotos o información personal sensible.
- No prestarse para administrar o gestionar cuentas de correos o redes sociales de terceros o personas desconocidas durante la jornada.
- No descargar archivos adjuntos o hacer click en links que se reciban por medio de correos electrónicos o menajes de texto, sin verificar antes el remitente o el origen. Tome su tiempo para analizarlo, si tiene alguna duda informe a la mesa de ayuda.
- Validar las fuentes de información, verificar la autenticidad y reputación de los generadores de contenidos y noticias en las redes sociales.
- No realizar difusión de noticias o cadenas compartidas a través de mensajería instantánea hasta no verificar la veracidad de las mismas.
- Evite reaccionar impulsivamente ante noticias, audios, videos o cadenas o mensajes; el atacante quiere apelar a una reacción emocional o instintiva de su victima usando noticias falsas o que causen controversia.
- No contestar llamadas, videollamadas o mensajes de números desconocidos, y/o con indicativos de otros países.

8 Mas Recomendaciones

- Reiniciar los equipos de computo y dispositivos al iniciar o finalizar su jornada de trabajo para permitir la instalación de las actualizaciones de seguridad
- Aplicar medidas de prevención para restringir el acceso e instalación de programas maliciosos en sus dispositivos móviles y equipos de propiedad personal. Verificar que el antivirus de equipo corporativo y personal se encuentre siempre activos.
- Apagar equipos de cómputo, servidores, impresoras, sistemas y dispositivos que no se vayan a utilizar durante la jornada electoral, desde el viernes 29 de mayo si es posible, para reducir la superficie de ataque.
- No conectar dispositivos de almacenamiento USB , cámaras , celulares etc , que se encuentre olvidados en calle, en las instalaciones o alrededores de la institución.
- Utilice contraseñas robustas, largas y complejas, cámbielas periódicamente, y active MFA para sus cuentas con un programa autenticador o a correo electrónico (Nunca SMS), No utilice la misma contraseña para manejar todas sus cuentas y aplicaciones. Nunca comparta sus contraseñas.
- Mantenga siempre sincronizada y resguardada su información en las nubes corporativas ONE DRIVE y SHAREPOINT del INC.

8 Canales de atención

Si es víctima de un ataque informático, ciberextrosion u ofrecimiento de soborno por entrega de informacion y cuentas, o sospecha de alguna actividad anómala dentro o fuera de las instalaciones del INC durante la jornada de elecciones, **¡comunique la situación inmediatamente!**

El atacante espera que su victima por vergüenza, pudor o miedo no reporte el evento de seguridad, y así poder contar con el tiempo y la oportunidad para causar una mayor afectación a la entidad o a la persona, y lograr sus objetivos.

El INC dispone de los siguientes canales de atención durante la jornada de elecciones, para reportar cualquier incidente de seguridad digital o seguridad física.

Mesa de ayuda –Colsof
(+571) 3905012 Linea 7000
Correo: sima@cancer.gov.co

Administrador de Seguridad Informática
Correo/Teams: palarcon@cancer.gov.co

Oficial de Seguridad de la Información – CISO
Correo/Teams: caguerrero@cancer.gov.co

Gráficos: freepik

Instituto Nacional de Cancerología
Colombia
Por el control del cáncer

COLCERT

¡Soy inteligente, soy Ciberseguro!

Gráficos: freepik