El futuro digital es de todos

MinTIC

CIBERSEGURIDAD EN EL PROCESO ELECTORAL COLOMBIANO

Asesoría de Sistemas

Consejo Nacional Electoral COLOMBIA

REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

#MásTICMejorPaís

Gráficos: freepik

1 PMU Ciber

Objetivo

Apoyar técnicamente la actividad electoral, proteger los activos de información susceptibles a vulneraciones y realizar acciones preventivas y reactivas frente a incidentes cibernéticos que afecten la confidencialidad, disponibilidad, privacidad e integridad de la información antes, durante y después del certamen electoral.

¿Quiénes lo integran?

La Mesa de Trabajo del Puesto de Mando Unificado de Ciberseguridad Nacional está integrado entre otras, por las siguientes entidades: Presidencia de la República, Ministerio de Defensa, Equipo de Respuesta a Emergencias Cibernéticas de Colombia, Consejo Nacional Electoral, Registraduría Nacional del Estado Civil, Centro Cibernético Policial, Centro Integrado de Información de Inteligencia, CSIRT-PONAL, Ministerio de Tecnologías de la Información y las Comunicaciones, Fiscalía General de la Nación y Dirección Nacional de Inteligencia (DNI).

2 Delitos relacionados

En el marco de la estrategia que adelanta la Policía Nacional como respuesta institucional contra los delitos electorales, también ha dispuesto la atención integral frente a las conductas penales establecidas en la **Ley 1273 de 2009**, las cuales se relacionan con la protección de la información y los datos, que comprenden penas que van de 48 a 96 meses de prisión y multas de los 100 a 1.000 SMLV:

1. Acceso abusivo a un sistema informático.
2. Obstaculización Ilegítima de sistema informático o red de telecomunicación.
3. Interceptación de datos informáticos.
4. Suplantación de sitio web para capturar datos personales.
5. Violación de datos personales.
6. Uso de software malicioso.
7. Daño informático.

Artículo 220.
Injuria

Artículo 221.
Calumnia

Artículo 222.
Injuria y calumnias indirectas

Artículo347.
Amenazas

Artículo348.
Instigación a delinquir

Además podrían incurrir en delitos definidos en la **Ley 599 de 2000.**

3 Vectores de ataque

- **Falsas notificaciones** de cambios de jurados o puestos de votación.
- **Falsas notificaciones** de impuestos, notificaciones de registros y/o bloqueos de productos financieros.
- **Generación de contenido difamatorio** (injurias, calumnias, falsas noticias, estigmatización).
- **Distribución de código malicioso** (malware) en archivos adjuntos o enlaces.
- **Captura de datos personales** a través de falsos portales, suplantación de correos, mensajería instantánea, encuestas o llamadas telefónicas (Phising, email spoofing, Smishing-Mensajes de texto, Vishing-Llamadas telefónicas).
- **Manipulación de datos personales** suministrados por los mismos usuarios durante el uso de encuestas, instalación de aplicaciones informáticas (Apps, programas, juegos, descarga de música, etc.).
- **Obstaculización ilegitima** de los recursos informáticos (Denegación de servicios).
- **Falsas campañas** de marketing.
- **Falsos candidatos y partidos políticos** en redes sociales.

4 Desinformación
Fake News

Comprende la elaboración y difusión de contenidos falsos en la 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 la toma de las decisiones democráticas en el marco de escenarios políticos y/o electorales.

¿Cómo identificarlas?

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

Gráfico: freepik

5 Recomendaciones

- Proteger sus datos personales y no suministre información sensible.
- No prestarse para administrar o gestionar cuentas de redes sociales desconocidas.
- No descargar archivos adjuntos que se reciban por medio de correos electrónicos desconocidos.
- 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.

Gráficos: freepik

5 Recomendaciones

- No contratar servicios para posicionamientos de marcas, perfiles, generación de tendencias, que puedan afectar la seguridad de la información y los datos.
- Aplique las medidas de prevención y control para restringir el acceso e instalación de programas maliciosos en sus dispositivos móviles.
- Las elecciones son un mecanismo de participación presencial y que se realiza en los lugares destinados para ello por la Organización Electoral. NO EXISTE VOTO VIRTUAL en Colombia.
- Generar un pacto entre los líderes de las campañas políticas para evitar el uso de instrumentos o servicios ilegales para generar tendencias o campañas de desinformación en la Internet.

Gráfico: freepik

6 Canales de atención

Fiscalía General de la Nación
Unidades de Reacción Inmediata (URI) en todo el país.
Línea Gratuita 122
www.uriel.mininterior.gov.co

Centro Cibernético Policial
Twitter y Facebook: @caivirtual
(+571) 5159700 Ext 309727
caivirtual@policia.gov.co

Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT)
(+571) 2959897
contacto@colcert.gov.co

Equipo de Respuesta incidentes de Seguridad Digital del Gobierno (CSIRT-GOBIERNO)
csirtgob@mintic.gov.co
(+571) 5159728
01800910742 opción 4

Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional (CSIRT-PONAL)
https://cc-csirt.policia.gov.co/
ponal.csirt@policia.gov.co

El futuro digital es de todos

MinTIC

¡Muchas gracias!

CIBERSEGURIDAD
EN EL PROCESO ELECTORAL
COLOMBIANO

Consejo Nacional Electoral COLOMBIA

REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

POLICÍA NACIONAL DIOS Y PATRIA

+MásTIC MejorPaís

Gráficos: freepik