10 recomendaciones para proteger las infraestructuras tecnológicas en las elecciones regionales

- *MinTIC y Colcert entregan pasos clave para proteger a su empresa de ciber ataques.*
- *Para reportar un incidente de seguridad digital, puede comunicarse a través de los siguientes canales: Bogotá: +57 601 344 22 22, o al correo contacto@colcert.gov.co.*

Bogotá, 27 de octubre de 2023 (@Ministerio_TIC). Con el propósito de mantener la tranquilidad y seguridad cibernética durante las Elecciones de Autoridades Territoriales 2023, que se realizarán en el país este próximo domingo 29 de octubre, el MinTIC, a través del Grupo de Respuestas a Emergencias Cibernéticas de Colombia (Colcert), entrega 10 recomendaciones para que entidades públicas y privadas fortalezcan sus canales digitales.

"*Las entidades y organizaciones deben establecer una postura de seguridad digital orientada a la prevención, protección y reacción para la gestión de sus incidentes, y para ello, una de las estrategias que deben adoptar es conocer el ciclo de vida de los ataques (Cyber Kill Chain), lo cual permite detectar, detener e interrumpir las acciones de los actores maliciosos, gracias a la identificación de indicadores de ataque*", señaló el ministro TIC, Mauricio Lizcano, (@MauricioLizcano).

La principal recomendación es reportar los incidentes de seguridad digital, clasificados por la entidad u organización como 'Muy graves' y 'Graves', a la línea del Colcert para el apoyo y coordinación de los primeros pasos en el restablecimiento de las operaciones, así como en el ciclo de gestión de los incidentes.

Recomendaciones Generales

1. Establecer una política de gestión de contraseñas y de control de acceso.
2. Actualizar el inventario de activos de información, incluyendo los de nube.
3. Activar un plan de capacitación para la entidad.
4. Recomendar a los usuarios no descargar software ni aplicaciones ilegales, que puedan afectar la seguridad de la infraestructura tecnológica de la entidad.
5. Evitar conectarse a redes inalámbricas Wi-Fi abiertas, que puedan capturar credenciales y exfiltrar información.
6. Realizar análisis de vulnerabilidades plataformas expuestas en internet y planes de mitigación de éstas.
7. Hacer pruebas de continuidad de la operación, para cada una de las copias de seguridad generadas.
8. Actualizar o implementar soluciones de antivirus para tener mayor visibilidad como soluciones EDR (Endpoint Detection and Response) para proteger

dispositivos y XDR (Extensive Detection and Response) para redes, aplicaciones y datos

9. Revisar, atender y gestionar los boletines y alertas emitidos por las instancias Ciber del Estado, así como de organismos internacionales en lo respectivo a vulnerabilidades críticas y altas que se deban atender.
10. Validar el despliegue de los agentes de antivirus en computadores y servidores, en la consola para validar el cubrimiento total de la infraestructura tecnológica de la entidad.

Durante el fin de semana de comicios, el MinTIC y el Colcert, estarán atentos para garantizar la realización de una jornada electoral donde prime la seguridad digital. Puede comunicarse a través de los siguientes canales: Bogotá: +57 601 344 22 22, o al correo contacto@colcert.gov.co.