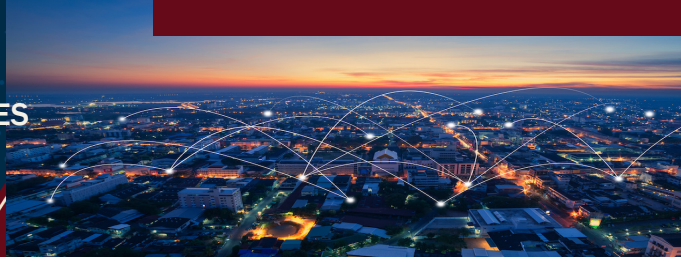
CICLO ELECTORAL GENERAL DE 2024: GUÍA PARA EL REPORTE VOLUNTARIO DE INCIDENTES DIRIGIDA A LAS PARTES INVOLUCRADAS EN LA INFRAESTRUCTURA ELECTORAL



VISIÓN GENERAL

Se anima a las partes involucradas en la infraestructura electoral a compartir información referente a incidentes de seguridad física y cibernética de acuerdo con sus planes de respuesta a incidentes. El intercambio de información posiblemente ha de incluir oficinas electorales locales y estatales, centros de fusión estatales, organismos de seguridad locales y estatales, y demás colaboradores a nivel federal. Compartir de manera voluntaria información sobre incidentes, facilita un acceso más rápido a los recursos para respuesta a incidentes, una mejor comprensión de las tácticas usadas por los actores maliciosos y alerta a otras partes involucradas en las elecciones acerca de las amenazas actuales y de las acciones para ayudarles a proteger su infraestructura.

REPORTE VOLUNTARIO DE INCIDENTES POR PARTE DE MIEMBROS DEL GOBIERNO FEDERAL: A QUIÉN CONTACTAR

INCIDENTES CIBERNÉTICOS

Para maximizar el conocimiento de la situación y el apoyo durante el ciclo electoral de 2024, reporte incidentes cibernéticos presuntos o reales a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Oficina Federal de Investigaciones (FBI) y el Centro de Análisis e Intercambio de Información de Infraestructura Electoral (EI-ISAC).

1. **Reporte incidentes cibernéticos sospechosos a CISA. Envíe un correo electrónico a report@cisa.dhs.gov, llame al 1-844-Say-CISA (1-844-729-2472) o reporte en línea a través de https://www.cisa.gov/report.** CISA puede ayudar en la respuesta a incidentes y la recuperación de incidentes cibernéticos sospechosos. CISA comparte información relevante sobre amenazas e incidentes cibernéticos con el IE-ISAC para que sea diseminado a lo largo de la comunidad electoral.

2. **Reporte incidentes cibernéticos sospechosos al FBI. Comuníquese con su oficina local del FBI: https://www.fbi.gov/contact-us/field-offices. También puede ponerse en contacto con el Centro para la Denuncia de Delitos en Internet del FBI: www.ic3.gov, la Línea Nacional de Información del FBI al 1-800-225-5324 o envíe información clave en línea: https://tips.fbi.gov/home.** El FBI es el principal brazo de investigación del Departamento de Justicia de los Estados Unidos y dirige las investigaciones del Gobierno de los Estados Unidos en cuestiones de actividad delictiva relacionada con las elecciones. El FBI tiene la responsabilidad de investigar actividad cibernética maliciosa y posibles delitos electorales, incluyendo la desinformación acerca de la hora, el lugar o la forma para votar.

3. **Reporte incidentes cibernéticos sospechosos al EI-ISAC. Envíe un correo electrónico soc@cisecurity.org o llame al 866-787-4722.** El EI-ISAC es el mayor mecanismo de intercambio de información para la comunidad electoral acerca de amenazas e incidentes cibernéticos. EI-ISAC es financiado parcialmente por CISA, a través de un acuerdo de cooperación con el fin de que funcione como un centro para análisis e intercambio de información 24 x 7 x 365 acerca de amenazas e incidentes cibernéticos y proporcione servicios gratuitos de ciberseguridad y respuesta a incidentes.

INCIDENTES DE SEGURIDAD FÍSICA

1. **Si hay una amenaza física inminente, llame al 911 de inmediato. Reporte las amenazas e incidentes de seguridad física a los organismos de seguridad a nivel estatal y local,** de acuerdo con sus planes de respuesta a incidentes y puntos de contacto previamente identificados.

2. **Denuncie amenazas e incidentes de seguridad física al FBI, incluyendo sospechas de amenazas o actos de violencia contra los trabajadores electorales.** Comuníquese con su Coordinador de Delitos Electorales o la oficina local del FBI: https://www.fbi.gov/contact-us/field-offices. También puede comunicarse con el Centro para la Denuncia de Delitos en Internet del FBI: www.ic3.gov, la Línea Nacional de Información del FBI al 1-800-225-5324 o envíe información clave en línea: https://tips.fbi.gov/home.

3. **Reporte incidentes que sucedan por correo y de correo sospechoso al Servicio de Inspección Postal de los Estados Unidos (USPIS). Llame a USPIS al 877-876-2455 o denuncie un delito postal en línea: uspis.gov/report.** El USPIS es el organismo de seguridad a nivel federal del Servicio Postal de los Estados Unidos (USPS) y protege el correo, incluyendo el correo electoral enviado desde y hacia los votantes tanto nivel nacional como internacional.

4. **Comparta información con CISA acerca de incidentes físicos que afecten la seguridad o el funcionamiento de la infraestructura electoral (cortes de energía, pérdida de servicios de comunicación u otras amenazas o peligros**). **Envíe un correo electrónico a report@cisa.dhs.gov, llame al 1-844-Say-CISA (1-844-729-2472) o reporte en línea a través de https://www.cisa.gov/report.** Los casos de actividad delictiva o de amenazas activas deben informarse primero al organismo policial local, estatal o federal correspondiente para obtener una respuesta adecuada. En el caso de incidentes físicos que afectan la infraestructura electoral, reportarlos a CISA permite notificar más ampliamente a las partes involucradas acerca de las tendencias en las amenazas a nivel nacional y orienta los análisis de riesgo a la seguridad física y las guías para la mitigación de riesgos emergentes.

EJEMPLOS

La siguiente lista proporciona algunos ejemplos de incidentes que las partes interesadas en la infraestructura electoral deben reportar.

Ejemplos de posibles incidentes cibernéticos	Ejemplos de posibles incidentes físicos
• Incidente de denegación de servicio en sitios web oficiales • Contraseñas de cuentas o claves de seguridad de la infraestructura de red comprometidas • Ataque exitoso de suplantación de identidad (*phishing*) • Incidente de programa malicioso (*malware*) o de secuestro de datos (*ransomware*) • Tráfico o actividad sospechosa en la red • Acceso no autorizado a los datos • Acceso no autorizado a la red • Degradación o suplantación de un sitio web	• Intimidación, hostigamiento o agresión de trabajadores electorales • Paquetes o correo sospechosos • Amenazas de violencia contra el personal o las instalaciones • Acceso no autorizado a instalaciones o equipos • Vandalismo en instalaciones o equipos electorales • Violencia en los lugares de votación o recintos electorales • Interrupciones de servicios públicos que afectan las instalaciones u operaciones electorales • Desastres naturales que afectan las instalaciones u operaciones electorales