



Guía de Planificación de Notificación y Detección de Incidentes Cibernéticos para Seguridad Electoral

Julio 2020



Contenido

Introducción	1
Organización del documento	2
Guía para el desarrollo del plan	3
Descripción general	3
Tabla 1: Niveles de criticidad de los síntomas	3
Desarrollo e implementación	4
Paso 1: Identificar a las partes interesadas	4
Paso 2: Desarrollar planes de notificación	5
Paso 3: Desarrollar tablas de criticidad de los síntomas	5
Paso 4: Revisar y finalizar Plan	6
Paso 5: Distribuya e integre el plan	7
Paso 6: Utilice los servicios y recursos disponibles	8
Apéndice A: Partes interesadas clave e información de contacto Hojas de trabajo	A-1
Apéndice B: Plantilla del plan de notificación y detección de incidentes cibernéticos	B-1

Esta página se dejó intencionalmente en blanco

Introducción

La Agencia de Seguridad de la Infraestructura y Ciberseguridad (CISA) brinda orientación y asistencia técnica a los funcionarios responsables de salvaguardar la infraestructura electoral, previa solicitud. Varios funcionarios estatales y locales han identificado la necesidad de asistencia para mejorar la respuesta a incidentes cibernéticos. La respuesta efectiva a incidentes cibernéticos requiere que aquellos con acceso a los sistemas electorales y los responsables de responder a un incidente comprendan cómo detectar un incidente potencial, su papel en informar y/o responder al incidente, y qué procedimientos deben seguir para mitigar los impactos potenciales. Un plan de respuesta a incidentes cibernéticos, junto con suficientes recursos, capacitación y ejercicio del plan, es una herramienta esencial para que las jurisdicciones permitan esta comprensión entre los usuarios del sistema y los respondedores de incidentes.

No existe un enfoque único para todos para desarrollar un plan de respuesta a incidentes cibernéticos. Si bien algunas oficinas electorales son directamente responsables de una gran parte de la capacidad de respuesta a incidentes de sus sistemas, muchas (particularmente en jurisdicciones pequeñas y medianas) dependen de proveedores u otras agencias para actividades tales como monitoreo, análisis, contención, erradicación y recuperación. La estructura, el alcance y el nivel de detalle requerido para un plan de respuesta a incidentes varía ampliamente en función de estos y otros factores. Independientemente, **todas las oficinas electorales desempeñan un papel fundamental en la detección de posibles incidentes cibernéticos, según las observaciones de los usuarios del sistema, y la notificación a las partes involucradas correspondientes**.

Soporte Técnico

CISA ofrece una gama de recursos y servicios, como evaluaciones, capacitaciones, ejercicios y asistencia de planificación, para ayudar a los funcionarios electorales estatales y locales a evaluar las prácticas de ciberseguridad e identificar oportunidades para fortalecer la seguridad y la resiliencia a las amenazas. Estos servicios voluntarios están disponibles bajo petición sin costo alguno. Consulte la [Guía de recursos de seguridad de la infraestructura electoral](#) de [CISA](#) para obtener detalles adicionales.

Esta *Guía de planificación de notificación y detección de incidentes cibernéticos* se enfoca en la necesidad común compartida en toda la comunidad electoral para reconocer y responder de manera efectiva a posibles incidentes cibernéticos. Específicamente, la guía se basa en los materiales existentes ofrecidos por los líderes de opinión en seguridad electoral de la Nación para ayudar a las oficinas electorales a determinar y documentar lo siguiente:

- **Partes relevantes e información de contacto** para la notificación y respuesta de
- **incidentes Planes de notificación** proporcionan procedimientos estandarizados para notificar a las partes interesadas apropiadas de un posible incidente cibernético basado en los síntomas observados y el nivel de criticidad
- **indicadores de incidentes ("síntomas")** pueden consultar para detectar posibles incidentes cibernéticos e iniciar el plan de notificación apropiado para escalar e informar

Las oficinas electorales pueden usar esta información como un plan básico de respuesta a incidentes cibernéticos o integrar la información en un plan más amplio basado en sus necesidades específicas.

Organización del documento

Este documento consta de las siguientes cuatro secciones:

- **La Guía para el desarrollo del plan** brinda contexto e instrucciones para desarrollar un *Plan de notificación y detección de incidentes cibernéticos* utilizando las plantillas y herramientas provistas en los apéndices
- **Apéndice A: Hojas de trabajo de información de contacto y partes clave involucradas** proporciona una serie de hojas de trabajo para identificar a las partes interesadas que se incluirán en el *Plan de notificación y detección de incidentes cibernéticos* y su información de contacto
- **Apéndice B: Plantilla del plan de notificación y detección de incidentes cibernéticos** proporciona una plantilla rellenable que las oficinas electorales pueden completar siguiendo las instrucciones de esta guía. La plantilla incluye tablas de criticidad de síntomas rellenas previamente que brindan descripciones de ejemplo de los indicadores que observaría un usuario del sistema, los planes de notificación correspondientes y las posibles soluciones de solución de problemas/mitigación para una variedad de posibles síntomas de incidentes. Los funcionarios electorales pueden utilizar, modificar o agregar estos ejemplos, según corresponda, al desarrollar la sección de tablas de criticidad de síntomas de su *Plan de notificación y detección de incidentes cibernéticos*

La plantilla completa sirve como un producto "desprendible" independiente que las jurisdicciones pueden distribuir a las partes interesadas en formato electrónico o impreso, o como referencia para informar planes más amplios de respuesta a incidentes. Las oficinas electorales pueden modificar y actualizar estos planes a medida que cambian el personal y los procesos para adaptarse al entorno electoral dinámico.

Guía para el desarrollo del plan

Descripción general

La detección temprana de un incidente de seguridad y la notificación a las partes interesadas apropiadas pueden ser vitales para mitigar los impactos del incidente. La *del plan de notificación y detección de incidentes cibernéticos* que se proporciona en esta guía está diseñada para acelerar la detección de incidentes en función de las observaciones de los usuarios del sistema y la notificación mediante la aplicación de dos conceptos clave

Síntoma de incidente de seguridad

Para los propósitos de este documento, un "síntoma" se define como algo que los usuarios pueden observar o reportar evidencia que puede ser indicativa de una posible amenaza o incidente de seguridad

- **Detección de incidentes basada en síntomas** se enfoca en detectar los "síntomas" que experimentarían un usuario durante un incidente de seguridad u otra falla relacionada con IT; no requiere que el usuario diagnostique la causa de una anomalía del sistema, solo que notifique a las partes interesadas correspondientes. Esto es importante por dos razones: (1) es posible que muchos usuarios de sistemas electorales no tengan la experiencia para diagnosticar o mitigar adecuadamente un incidente como un ataque cibernético, y (2) un síntoma que por sí solo suele indicar un problema rutinario o inocuo puede revelar una criticidad más grave si se informa y observa adecuadamente en múltiples sistemas o en combinación con otros síntomas
- **Los procedimientos de notificación basados en la criticidad** distinguen los procedimientos y canales de notificación apropiados en función de si los síntomas indican un ciber incidente rutinario, sospechoso o potencialmente crítico. Esto ayuda a proporcionar una vía para realizar un seguimiento de todos los incidentes, evita que las partes interesadas clave y los responsables de la toma de decisiones se vean abrumados con informes y solicitudes de soporte para incidentes de bajo riesgo, y agiliza la presentación de informes y la respuesta a incidentes críticos. La Tabla 1 describe los tres niveles de criticidad utilizados en el *Plantilla de Plan de Detección y Notificación de Incidentes Cibernéticos*

Tabla 1: Niveles de criticidad¹

Nivel de criticidad	Descripción
Rutinario	El incidente puede causar interrupciones menores en el sistema que probablemente no serán visibles para el público o afectarán el proceso electoral
Sospechoso	Posiblemente debido a un incidente cibernético que provocó una interrupción en el proceso electoral, pero es posible que no se activen las obligaciones de notificación formal. El problema comienza a hacerse público

¹Niveles de criticidad de incidentes cibernéticos rutinarios, sospechosos y críticos adaptados de los niveles de gravedad de incidentes cibernéticos (bajo, medio, alto) descritos en Belfer Center's *Election Cyber Incident Communications Plan Template*

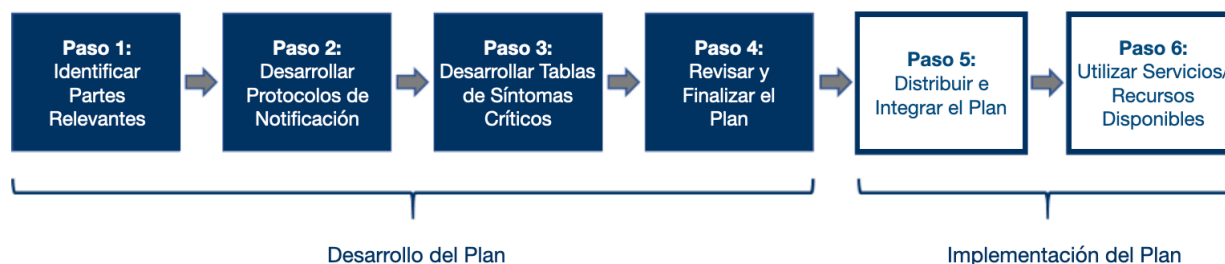
Nivel de criticidad	Descripción
Crítico	Es muy probable que sea indicativo de un incidente cibernético que desencadene obligaciones de presentación de informes a nivel nacional, afecte una gran cantidad de información de los votantes y/o sea destructivo para las operaciones electorales

Desarrollo e implementación

Esta guía describe un proceso de seis pasos (Figura 1) que las oficinas electorales pueden usar para desarrollar e implementar un *Plan de notificación y detección de incidentes cibernéticos* utilizando los conceptos anteriores. Se prevé que este proceso sea dirigido por un funcionario electoral de la jurisdicción o su designado, y cada paso está diseñado para llevarse a cabo en colaboración con el Equipo de Respuesta a Incidentes y el Equipo de Comunicaciones de Respuesta a Incidentes correspondientes, denominados en conjunto como el **Equipo de Planificación**. Si estos equipos aún no han sido designados para la jurisdicción, el funcionario electoral que lidere este esfuerzo debe identificar un Equipo de planificación compuesto por personas como personal electoral estatal y local, administradores de IT y representantes de proveedores que deben participar en la determinación de las partes interesadas y los procedimientos apropiados para el reporte y respuesta de incidentes.

Además de identificar al Equipo de Planificación, el Funcionario Electoral debe determinar cómo y cuándo (p.ej., un taller) el Equipo de Planificación colaborará para llevar a cabo cada paso del proceso. Puede solicitar recursos de CISA y asistencia directa de expertos en la materia para facilitar este proceso comunicándose con su funcionario electoral estatal o representante regional de CISA (<https://www.cisa.gov/cisa-regional-offices>)

Figura 1: Pasos de desarrollo e implementación del plan



Paso 1: Identificar a las partes relevantes

Los funcionarios electorales deben coordinarse con el personal electoral estatal y local aplicable y el personal de IT para completar el *Apéndice A: Partes interesadas clave y hojas de trabajo de información de contacto*. La hoja de trabajo captura los nombres y la información de contacto de las personas y organizaciones que deben ser notificadas sobre posibles incidentes de seguridad para facilitar la notificación y la respuesta efectivas y oportunas.

Es una buena práctica identificar y capacitar a los puntos de contacto principales y de respaldo; como tal, la hoja de trabajo proporciona espacio para registrar información para ambos, según corresponda. La información recopilada a través de este proceso se utilizará para respaldar la creación de procedimientos de notificación de incidentes en el Paso 2.

Instrucciones:

- € utilizando las tablas del *Apéndice A: Partes interesadas clave y hojas de trabajo de información de contacto*, designe a las partes interesadas clave que deben ser notificadas sobre posibles incidentes de seguridad No necesita identificar a alguien para cada categoría si no corresponde, y puede agregar filas/categorías adicionales según sea necesario Complete una hoja de trabajo específica del sistema/proveedor para cada sistema relacionado con las elecciones que tenga personas no gubernamentales que crea que deberían incluirse Puede modificar y actualizar estos planes a medida que cambia el personal y los procesos para adaptarse al entorno electoral dinámico

Paso 2: Desarrollar Protocolos de Notificación

Cada jurisdicción desarrolla planes de notificación de incidentes para proporcionar a los usuarios del sistema electoral y otras partes interesadas instrucciones paso a paso sobre a quién contactar y cómo contactarlos cuando se observa un síntoma que puede indicar un incidente de seguridad Los funcionarios electorales deben trabajar con el Equipo de planificación para personalizar los planes de notificación de incidentes para su jurisdicción La sección de planes de notificación de incidentes del *Apéndice B: Plantilla de plan de notificación y detección de incidentes cibernéticos* proporciona una plantilla para crear planes escalonados basados en el nivel de criticidad (Rutinario, sospechoso o crítico) de los síntomas observados

Instrucciones:

- € complete todos los campos correspondientes en la sección de planes de notificación del *Apéndice B* utilizando las partes interesadas clave y la información de contacto documentada en el Paso 1 Las jurisdicciones pueden personalizar los planes de notificación para reflejar su capacidad para gestionar incidentes en varios niveles de criticidad
- € Revise y practique todos los planes con las partes interesadas correspondientes para garantizar su conocimiento de las funciones y responsabilidades para la respuesta a incidentes y para validar los procedimientos antes de finalizar

Paso 3: Desarrollar tablas de síntomas críticos

Las tablas de síntomas críticos enumeran los comportamientos o actividades anormales del sistema que un usuario del sistema puede observar, y brindan al usuario una guía común para la clasificación inicial y la resolución de problemas de esas anomalías para que puedan iniciar el plan de notificación adecuado según el nivel de criticidad: Rutinario, sospechoso o crítico Utilizando el *Apéndice B: Plantilla del plan de notificación y detección de incidentes cibernéticos*, los funcionarios electorales deben trabajar con el Equipo de planificación para desarrollar tablas de criticidad de síntomas para cada sistema electoral o tipo de sistema utilizado por su jurisdicción

Las tablas de criticidad de síntomas incluidas como parte del *Apéndice B: Plantilla del plan de notificación y detección de incidentes cibernéticos* se han llenado previamente para proporcionar ejemplos que el equipo de planificación puede usar como inspiración para el desarrollo de tablas de criticidad de síntomas personalizadas o pueden hacer referencia, utilizar, modificar o agregar directamente a estos ejemplos según corresponda para desarrollar las tablas de su plan Las tablas de ejemplo proporcionan algunos síntomas comunes que pueden observarse si ocurre un incidente cibernético Las tablas están diseñadas para ayudar a los usuarios a reconocer el nivel de criticidad, distinguir el plan de notificación correcto y realizar los pasos iniciales de solución de problemas para síntomas específicos que pueden observar en los sistemas electorales

Las jurisdicciones pueden optar por utilizar los ejemplos completados previamente, pero deben revisar y personalizar el contenido para alinear las políticas de la organización y los procedimientos operativos estándar de IT y los requisitos de notificación

Nota: Los ejemplos no representan todas las amenazas potenciales a la infraestructura de tecnología electoral, y los funcionarios y el personal electoral deben informar cualquier actividad sospechosa en el sistema o en la red de acuerdo con las políticas de su organización

Instrucciones:

- € Revise las Tablas de criticidad de síntomas rellenas previamente en el Apéndice B que proporcionan ejemplos de observaciones, sugerencias para la solución de problemas y planes de notificación para síntomas comunes que un usuario puede experimentar para varios activos, sistemas o tipos de sistemas
- € Utilice los ejemplos como referencia para ayudar a identificar cada activo, sistema o tipo de sistema crítico para el cual se desarrollarán tablas de criticidad de síntomas para su jurisdicción
- € Desarrolle una lista de posibles síntomas de incidentes que un usuario puede observar para cada uno de los activos, sistemas o tipos de sistemas identificados Utilice los ejemplos comunes proporcionados de síntomas como inspiración al desarrollar listas de síntomas o aprovéchelos directamente y modifíquelos según corresponda
- € En coordinación con el equipo de planificación, cree una tabla de criticidad de síntomas para cada síntoma utilizando la *Plan de notificación y detección de incidentes cibernéticos* en el Apéndice B El equipo puede optar por aprovechar las tablas de ejemplo rellenas previamente en el Apéndice B según corresponda Cada tabla de criticidad de síntomas debe proporcionar lo siguiente:
 - **Observaciones:** Comportamientos o actividades específicos del sistema que el usuario puede observar que describen el síntoma con más detalle para ayudar a determinar el nivel de criticidad
 - **Plan de notificación:** El plan específico que el usuario debe iniciar en función del nivel de criticidad indicado por la observación
 - **Posible resolución de problemas:** Acciones adicionales que la entidad que detecta el incidente o la primera línea de respuesta deben tomar para mitigar potencialmente los impactos del incidente y/o permitir que el usuario brinde información adicional útil para los respondedores de incidentes

Paso 4: Revisar y finalizar el plan

Una vez que los planes de notificación y las tablas de síntomas estén completos, los funcionarios electorales deben completar los campos personalizables restantes en el *Apéndice B: Plantilla del plan de notificación y detección de incidentes cibernéticos*

Se anima a las jurisdicciones a insertar su *Guía de respuesta a emergencias el día de las elecciones (EDERG)* donde se indica en la plantilla si ya tienen una, o trabajar con CISA para desarrollar un EDERG que se pueda incluir Un EDERG puede servir como una herramienta para desarrollar sus equipos de planificación y planes de notificación, por lo que su jurisdicción puede querer desarrollar este producto antes o junto con el desarrollo del *Plan de notificación y detección de incidentes cibernéticos*

Guía de Respuesta de Emergencia el Día de las Elecciones (EDERG)

Un EDERG proporciona pasos de respuesta e información de contacto para una variedad de incidentes de seguridad electoral Este producto personalizado puede ser desarrollado por funcionarios electorales estatales y locales con el apoyo gratuito de CISA

Los funcionarios electorales deben revisar el plan completo con cada miembro del equipo de planificación, incorporar comentarios y finalizar el documento

Instrucciones:

- € Complete los campos personalizables restantes en el Apéndice B
- € Inserte EDERG donde se indica en el Apéndice B Comuníquese con CISA si su jurisdicción no tiene un EDERG actual (consulte el Paso 6 para obtener más información)
- € Revise el borrador del plan con las partes interesadas correspondientes, incorpore los comentarios y finalice el documento

Paso 5: Distribuir e integrar el plan

Apéndice B: La plantilla del plan de notificación y detección de incidentes cibernéticos está diseñada para imprimirse o compartirse electrónicamente como un documento independiente una vez completada, y/o la información puede integrarse en otros documentos de planificación de respuesta a incidentes políticas y procedimientos según corresponda. Los funcionarios electorales deben proporcionar copias del plan completo a los usuarios del sistema, a los que responden a incidentes y a otras partes interesadas. Los funcionarios electorales deben capacitar a los usuarios y otras partes interesadas sobre cómo implementar el plan, ejercitar el plan regularmente y actualizar el plan después de completar los ejercicios para incorporar las lecciones aprendidas en el ejercicio.

Instrucciones:

- € Proporcione copias impresas y/o electrónicas de su *Plan final de notificación y detección de incidentes cibernéticos* a los usuarios del sistema, los encargados de responder a incidentes y otras partes interesadas que estén directamente involucradas en el proceso de detección y/o notificación
- € Integre la información documentada en el *Plan de notificación y detección de incidentes cibernéticos* en planes, políticas, procedimientos, etc relacionados (por ejemplo, Planes de respuesta a incidentes existentes), según corresponda
- € Desarrolle e implemente un plan de capacitación para garantizar que los usuarios del sistema y otras partes interesadas entiendan cómo y cuándo usar el *Plan de notificación y detección de incidentes cibernéticos*. Comuníquese con su representante de CISA para obtener información adicional o asistencia según sea necesario
- € Desarrolle e implemente un plan de ejercicios para reconocer las brechas de recursos y capacitación y para garantizar que los usuarios del sistema y otras partes interesadas estén preparados para usar el *Plan de notificación y detección de incidentes cibernéticos*. Comuníquese con su representante de CISA para obtener información adicional o asistencia según sea necesario. El equipo de ejercicios CISA también puede ayudar en el desarrollo e implementación de un ejercicio personalizado (consulte el Paso 6 para obtener más información)

Paso 6: Utilizar los servicios y recursos disponibles

CISA y otras entidades a nivel nacional y estatal brindan una variedad de servicios y recursos para ayudar a las jurisdicciones estatales y locales con sus necesidades de seguridad electoral, a menudo sin cargo.

Además de esta guía, CISA ofrece varios servicios y recursos para ayudar a los funcionarios electorales con la planificación de respuesta a incidentes, incluido el desarrollo de EDERG, la capacitación y los ejercicios del plan de respuesta, e información sobre los servicios federales de respuesta a incidentes. Para obtener una lista completa de los servicios y recursos de CISA para funcionarios electorales, visite <https://www.cisagov/protect2020>

Apéndice A: Plantilla de partes relevantes e información de contacto

Contactos de partes gubernamentales relevantes

Guías del sistema INTERNO de la División Electoral

socio/ parte relevante	Nombre	información de contacto de (número telefónico y correo electrónico)
Director	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Director adjunto	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Funcionario electoral	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Gerente de programa	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Tecnología de la información	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Comunicaciones	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
CISO	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Líder del sistema de votación	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Líder de E-Pollbook (Registro electrónico)	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Líder Sitio Web	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Líder ENR	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]

socio/ parte relevante	Nombre	información de contacto de (número telefónico y correo electrónico)
Centro de comando del día de las elecciones	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
UOCAVA MOVE	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]

NOTAS:

Otras partes relevantes a nivel del condado

socio/ parte relevante	Nombre	información de contacto de (número telefónico y correo electrónico)
Informática IT del condado	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
CISO del condado	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Comunicaciones del condado	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Ejecutivos del condado	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Departamento legal del condado	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Ley del condado	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]

NOTAS:

Partes Relevantes a nivel Estatal

socio/ parte relevante	Nombre	información de contacto de (número telefónico y correo electrónico)
SOS POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
POC Dr Electoral Estatal	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Elecciones SOC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Otro Emer Man POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Centro de análisis e intercambio de información estatal	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Informática IT	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Estado legal	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Ley estatal	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]

:

Socios a nivel federal

socio/ parte relevante	Nombre	información de contacto de (número telefónico y correo electrónico)
Reportes generales de CISA	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
POC CISA Regional	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
POC de redes sociales	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]

EI-ISAC POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
POC local del FBI	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]

NOTAS:

Plantilla específica para proveedor/sistema

Sistema:	[Insertar nombre del sistema]
Proveedor y versión:	[Insertar proveedor y versión]
Componentes:	[Insertar componentes]

socio/ parte relevante	Nombre y afiliación	información de contacto de (número telefónico y correo electrónico)
Web Host del condado POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Técnico del condado POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Ejecutivo del condado POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
POC del proveedor	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Técnico del proveedor POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]
Ejecutivo del proveedor POC	Primario: [Insertar nombre y afiliación primarios] Suplente: [Insertar nombre y afiliación secundarios]	Primario: [Insertar número telefónico y correo electrónico primarios] Suplente: [Insertar número telefónico y correo electrónico secundarios]

NOTAS:

Esta página se dejó en blanco intencionalmente

Apéndice B: Plantilla del plan de notificación y detección de incidentes cibernéticos

La siguiente plantilla puede ser completada por jurisdicciones electorales siguiendo las instrucciones en esta guía. La plantilla completa está destinada a servir como un producto independiente que las jurisdicciones pueden distribuir a las partes interesadas en formato electrónico o impreso, o como referencia para informar planes más amplios de respuesta a incidentes. Los funcionarios electorales pueden modificar y actualizar estos planes a medida que cambian el personal y los procesos para adaptarse al entorno electoral dinámico.

Se puede solicitar apoyo adicional para desarrollar, capacitar o poner en práctica el plan a través de su funcionario electoral estatal o representante regional de CISA (<https://www.cisa.gov/cisa-regional-offices>)

Esta página se dejó en blanco intencionalmente

[Insertar nombre de jurisdicción]

Seguridad electoral

Plan de notificación y detección de incidentes cibernéticos

Versión [Insertar número de versión]

Publicado [Insertar fecha de publicación]

Aprobado por [Insertar autoridad de aprobación]

La seguridad electoral es una responsabilidad compartida entre los administradores electorales estatales y locales, otras entidades gubernamentales estatales y locales, proveedores, trabajadores electorales, socios federales y ciudadanos estadounidenses. Cada uno de nosotros desempeña un papel fundamental para garantizar que la infraestructura electoral de la Nación, incluidos sus sistemas, redes, espacios físicos y procesos, esté protegida de adversarios y amenazas de seguridad cibernética.

El propósito de este plan es proporcionar al personal electoral, a los usuarios del sistema electoral, a los respondedores de incidentes y a los respondedores de comunicaciones de incidentes un plan común para (1) la detección de posibles incidentes de seguridad y (2) la notificación oportuna a las partes interesadas correspondientes.

El plan está organizado en las siguientes secciones:

- 1. Cómo usar este Plan (Páginas [Insertar número(s) de página])**
Instrucciones para funcionarios electorales, personal y usuarios del sistema electoral para mantener e implementar este plan.
- 2. Tablas de síntomas de incidentes (páginas [Insertar número(s) de página])**
El personal electoral y los usuarios de los sistemas deben consultar estas tablas cada vez que se observe un comportamiento o actividad anormal o sospechosa (es decir, un síntoma) en un sistema relacionado con las elecciones para determinar el nivel de criticidad.
- 3. Planes de Notificación de Incidentes (Páginas [Insertar número(s) de página])**
Todos los síntomas observados constituyen un incidente y deben informarse a las partes interesadas correspondientes utilizando los planes de notificación de esta sección. Los planes de notificación son específicos para el nivel de criticidad.
- 4. (OPCIONAL) Guía de respuesta a emergencias el día de las elecciones (Páginas [Insertar número(s) de página])**
Brinda pasos de respuesta e información de contacto para tipos de incidentes adicionales que incluyen clima severo, alarmas contra incendios e incidentes violentos.

1 Cómo usar este plan

Funcionarios electorales

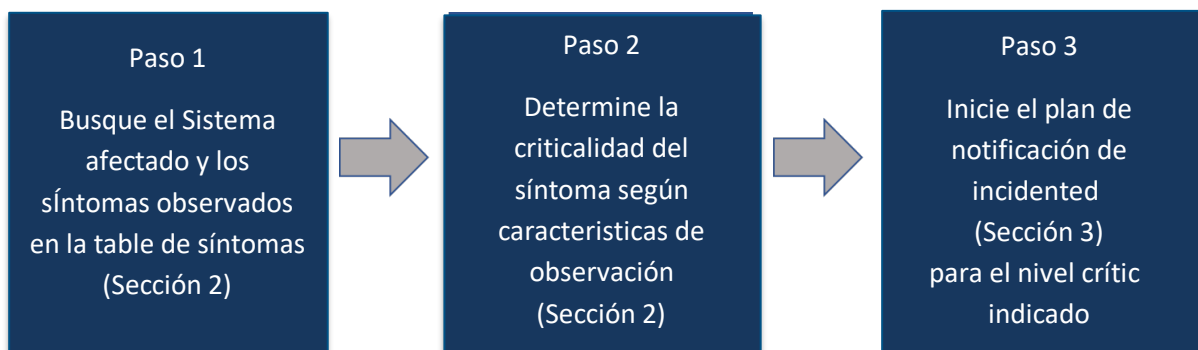
Revise este plan periódicamente para asegurarse de que esté actualizado y distribúyalo a todo el personal electoral, usuarios del sistema electoral, equipos de respuesta a incidentes y de comunicaciones de incidentes También asegúrese de que estas partes estén debidamente capacitadas en este plan y que el plan se practique regularmente Se puede solicitar apoyo adicional para actualizar, capacitar o ejecutar el plan a través de su funcionario electoral estatal o representante regional de CISA (<https://www.cisa.gov/cisa-regional-offices>)

Personal electoral y usuarios del sistema electoral

Revise este plan al recibirlo y al menos una vez al mes a partir de ese momento, con el fin de asegurarse de que está familiarizado con el contenido Consulte este plan cada vez que observe o tenga conocimiento de cualquier anomalía (es decir, síntoma) relacionada con un sistema electoral

Utilizando las Tablas de síntomas de incidentes en la Sección 2, ubique el síntoma y la(s) observación(es) específica(s) para determinar la gravedad del síntoma Con base en el nivel de criticidad indicado, inicie el Plan de Notificación de Incidentes correspondiente que se encuentra en la Sección 3 tan pronto como sea posible

Cada vez que observe o tenga conocimiento de cualquier anomalía (es decir, síntoma) relacionada con un sistema electoral, debe hacer lo siguiente:



Cómo usar las tablas de síntomas de incidentes

- Ubique la tabla de síntomas de incidentes para el sistema afectado y el síntoma que está experimentando
- Identifique la observación enumerada en la Tabla de síntomas que describe de manera más acertada lo que está experimentando para determinar el nivel de criticidad
- Inicie el Plan de notificación que se encuentra en la Sección 3 para el nivel de criticidad indicado

Nota: Los síntomas pueden tener explicaciones no relacionadas con la tecnología; sin embargo, es importante seguir el plan de notificación correspondiente para involucrar a las partes interesadas apropiadas en la revisión y evaluación de la situación. Siga siempre las políticas y los procedimientos internos y comuníquese con su administrador de IT si no está seguro de si debe seguir alguna de las acciones descritas en este documento

Índice de la tabla de criticidad de los síntomas: [Actualice los números de página a continuación según sea necesario]

Registro de votantes y observaciones de encuestas	5
Síntoma: Gran número de votantes no figuran en el libro de votación.	5
Síntoma: Número inusualmente alto de boletas provisionales distribuidas.	5
Observaciones sobre equipos y máquinas de votación	6
Síntoma: Equipo de la máquina de votación que no funciona correctamente	
Síntoma: El equipo de la máquina de votación no está aceptando/no lee las boletas	6
Síntoma: La máquina de votación no está marcando el voto seleccionado en la pantalla táctil	7
Síntoma: La selección del votante en la máquina de votación no coincide con la impresión en papel	7
Observaciones de sistemas y dispositivos de TI	
Síntoma: Archivos cifrados y rescate solicitado	8
Síntoma: La computadora no cargará aplicaciones de software basadas en web	8
Síntoma: Equipo lento para responder	9
Síntoma: Equipo lento al acceder a la red local	9
Síntoma: La computadora se bloquea o muestra con frecuencia "pantalla azul de la muerte" (BSOD)	10
Síntoma: El navegador te lleva a páginas web extrañas	
Síntoma: No se puede iniciar sesión en la cuenta	11
Síntoma: Error "El almacenamiento local está lleno"	
Síntoma: cuadros de diálogo con texto extraño, inesperado o sin sentido	12
Síntoma: Advertencia de que el software antivirus/antimalware está desactivado	12
Síntoma: Advertencia de que el equipo está infectado y se debe instalar un nuevo antivirus	13
Síntoma: advertencias extrañas del sistema o un gran número de ventanas emergentes	13
Síntoma: Su cursor se mueve por sí solo y / o los programas se inician por sí solos	13
Síntoma: No se puede acceder al Panel de control u otras herramientas del sistema en su computadora	14
Síntoma: Los iconos del escritorio han cambiado/movido o se han agregado nuevos iconos	14

[INSERTAR NOMBRE DE LA JURISDICCIÓN] PLAN DE DETECCIÓN Y NOTIFICACIÓN DE INCIDENTES CIBERNÉTICOS [INSERTAR FECHA]

Síntoma: Sitio web de la jurisdicción o cuenta de redes sociales que muestra información errónea	15
Síntoma: Las cuentas de redes sociales no oficiales presentan información errónea	15
Síntoma: correo electrónico sospechoso de una empresa legítima que solicita información confidencial	15

Síntoma: [Inserte el nombre o tipo del sistema/activo, los síntomas y los números de página según sea necesario]

Registro de votantes y observaciones electorales

Síntoma: Un gran número de votantes no figuran en el libro de votación

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] Un gran número de votantes (autoidentificados o con tarjeta de registro) no figuran en el libro de votación	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Seguir las políticas y procedimientos de jurisdicción para un votante que no está en el libro de votación Reportar el incidente a la Oficina Electoral, que verificará el registro en la Base de Datos de Registro de Votantes
[Inserte la observación, si procede]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: Número inusualmente alto de papeletas provisionales distribuidas

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] Alta demanda y distribución de papeletas provisionales	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Adquirir boletas provisionales adicionales y continuar distribuyéndolas según sea necesario
[Inserte la observación, si procede]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Observaciones de máquinas y equipos de votación

Síntoma: El equipo de la máquina de votación no funciona correctamente

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] La máquina o el equipo de votación no muestra información o no funciona como debería, pero previamente no funcionaba normalmente	Rutinario	<ul style="list-style-type: none"> • Confirme que la máquina está enchufada o que la batería está cargada • Consulte los protocolos estándar de solución de problemas • Busque soporte de experiencia en la materia (SME) o de proveedores según sea necesario
[Edite según sea necesario] La máquina o equipo de votación no muestra información o no funciona como debería. Anteriormente funcionaba como debería y está enchufado o tiene una batería cargada	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Busque soporte experto en la materia (SME) o proveedor según sea necesario
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]

Síntoma: La máquina de votación no acepta/no lee las boletas

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] El equipo de votación no acepta ni lee boletas	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Consulte los procedimientos estándar de operación de los equipos de votación • Confirme que el equipo está enchufado o tiene una batería cargada • Busque el apoyo de PYME o proveedor según sea necesario
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]

Síntoma: La máquina de votación no está marcando el voto seleccionado en la pantalla táctil

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] La máquina de votación no responde con precisión al tocar / no registra secciones como se indica	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Consulte los Procedimientos Estándar de Operación de la Máquina de Votación y siga los pasos para calibrar la máquina • Devolver la máquina al departamento de servicio si la recalibración solucionó el problema
[Edite según sea necesario] La máquina de votación no responde con precisión al tocar/no registrar secciones como se indica después de la recalibración	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Alertar POC de proveedor
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> • [Inserte posibles soluciones de problemas si corresponde]

Síntoma: La selección del votante en la máquina de votación no coincide con la impresión en papel

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] Los votantes reportan inconsistencias en las selecciones de votos y la impresión en papel generada para su envío desde una sola máquina	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Retirar del servicio el equipo afectado
[Edite según sea necesario] Los votantes reportan inconsistencias en las selecciones de votos y la impresión en papel generada para su envío desde varias máquinas	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Recurrir a planes de contingencia (es decir, boletas de papel) • Eliminar todos los equipos del servicio
[Edite según sea necesario] Los votantes reportan inconsistencias en las selecciones de votos y la impresión en papel generada para su envío desde varias máquinas, y no hay planes /	Crítico	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • No aplicable

[INSERTAR NOMBRE DE LA JURISDICCIÓN] PLAN DE DETECCIÓN Y NOTIFICACIÓN DE INCIDENTES CIBERNÉTICOS [INSERTAR FECHA]

procesos de contingencia para recolectar votos a través de otros métodos		
---	--	--

Observaciones de sistemas y dispositivos de IT

Síntoma: Archivos encriptados y rescate/multa solicitada

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] Ve una pantalla que dice que los archivos en la computadora están encriptados y que debe pagar una multa u otro pago para recuperar los archivos	Crítico	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Desconecte inmediatamente el cable de red del ordenador NO desenchufe ni apague la computadora

Síntoma: El equipo no carga aplicaciones de software basadas en web

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] Su navegador no cargará una página web	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Asegúrese de que todos los cables estén firmemente en sus enchufes Reiniciar el dispositivo Si usa Wi-Fi, asegúrese de estar en la red correcta
[Edite según sea necesario] Su navegador cargará algunas páginas web pero no otras	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Actualizar el sitio que no responde Comprobar si hay informes de otros usuarios que tienen problemas con el sitio Póngase en contacto con el servicio de atención al cliente para obtener información sobre interrupciones
[Edite según sea necesario] Su navegador no cargará ninguna página web	<ul style="list-style-type: none"> Suspiciou s 	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Asegúrese de que todos los cables estén firmemente en sus enchufes

[INSERTAR NOMBRE DE LA JURISDICCIÓN] PLAN DE DETECCIÓN Y NOTIFICACIÓN DE INCIDENTES CIBERNÉTICOS [INSERTAR FECHA]

		<ul style="list-style-type: none"> • Reiniciar el dispositivo • Si usa Wi-Fi, asegúrese de estar en la red correcta
[Inserte la observación, si aplica]	<ul style="list-style-type: none"> • Crítico 	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]

Síntoma: equipo lento para responder

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] Su computadora tarda en responder	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Reinicie el equipo • Compruebe cuántas aplicaciones se están ejecutando • Cerrar aplicaciones abiertas que no están en uso
[Edite según sea necesario] Reinició el equipo, pero sigue tardando en responder	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • No aplicable
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]

Síntoma: Equipo lento al acceder a la red local

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] El equipo es lento cuando intenta imprimir, abrir o guardar archivos, pero aún puede acceder a páginas web	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Reinicie el equipo • Asegúrese de haber iniciado sesión en la red • Asegúrese de que la impresora esté encendida y conectada
[Edite según sea necesario] El equipo es lento cuando intenta imprimir, abrir o guardar archivos, y no puede acceder a ninguna página web	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> • Reiniciar el equipo • Asegúrese de que todos los cables estén firmemente en sus enchufes

[INSERTAR NOMBRE DE LA JURISDICCIÓN] PLAN DE DETECCIÓN Y NOTIFICACIÓN DE INCIDENTES CIBERNÉTICOS [INSERTAR FECHA]

		<ul style="list-style-type: none"> • Asegúrese de que la impresora esté encendida y conectada • Asegúrese de haber iniciado sesión en la red • Asegúrate de estar conectado a la red Wi-Fi correcta
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]

Síntoma: La computadora se reinicia o muestra con frecuencia "pantalla azul de la muerte" (BSOD)

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] La computadora, que es nueva y ha tenido nuevos programas instalados, se reinicia más de 1 vez al día sin previo aviso y / o muestra el BSOD	Rutinario	[Edite según sea necesario] <ul style="list-style-type: none"> • No aplicable
[Edite según sea necesario] La computadora se reinicia más de 1 vez al día sin previo aviso y/o muestra el BSOD El equipo no es nuevo y no se han instalado nuevos programas	Sospechoso	[Edite según sea necesario] <ul style="list-style-type: none"> • No aplicable
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]

Síntoma: El navegador te lleva a páginas web extrañas

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] El navegador web lo redirige a sitios que no escribió o eligió ir	Rutinario	[Edite según sea necesario] <ul style="list-style-type: none"> • NO haga clic en ningún enlace o archivo en el sitio al que el navegador lo lleva • NO visite sitios importantes mientras el navegador está actuando de manera extraña • El personal de IT puede eliminar lo que puede ser malware secuestrador del navegador
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none"> • [Inserte posibles soluciones al problema si corresponde]

[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
-------------------------------------	---------	--

Síntoma: No se puede iniciar sesión en la cuenta

Observación	Plan de notificación	Posible solución al problema
[Editar según sea necesario] Está bloqueado de su computadora; su nombre de usuario y contraseña actuales no funcionan Recientemente recibió una notificación de que su contraseña caducará pronto o un aviso para restablecerla	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Confirme con IT y haga que se restablezca la cuenta
[Edite según sea necesario] Está bloqueado de su computadora; su nombre de usuario y contraseña actuales no funcionan Ha recibido una notificación sobre una contraseña que caduca o se está cambiando, aunque la contraseña haya estado funcionando	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> IT ayudará a restablecer la cuenta y determinar si se necesita una investigación adicional Preste especial atención a cómo actúa la computadora durante la próxima semana e informe cualquier comportamiento extraño al departamento de TI
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: Error "El almacenamiento local está lleno"

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] Recibe una advertencia de que el almacenamiento local en la computadora está casi lleno después de almacenar grandes cantidades de datos en la computadora (por ejemplo, archivos de imagen o video)	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Mire el espacio que consumen los archivos grandes y mueva parte (o todo) a un dispositivo de respaldo si es posible
[Edite según sea necesario] Recibe una advertencia de que el almacenamiento local en el equipo está casi lleno, pero no está almacenando grandes cantidades de datos en el equipo	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> No aplicable
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: cuadros de diálogo con texto extraño, inesperado o galimatías

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] Recibe cuadros de diálogo con texto extraño, inesperado o galimatías	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> NO haga clic en ninguna parte del cuadro, ni siquiera en la 'X' en la esquina superior para cerrar el cuadro Tome una captura de pantalla del cuadro y haga clic con el botón derecho en la barra de herramientas en la parte inferior de la pantalla para cerrar solo si debe continuar trabajando Deje la computadora sola hasta que llegue el personal de TI
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: advertencia de que el software antivirus/antimalware está deshabilitado

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] Recibe una advertencia de que el software antivirus / antimalware está deshabilitado después de instalar recientemente un software legítimo que le pidió que deshabilitara la protección antivirus para la instalación	Rutinario	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> No aplicable
[Editar según sea necesario] Recibe una advertencia de que el software antivirus o antimalware está desactivado, pero no recuerda haber instalado recientemente un software legítimo que le pidió que	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> No aplicable

deshabilitara las protecciones antivirus para la instalación		
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: Advertencia de que el equipo está infectado y se debe instalar un nuevo antivirus

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] Recibe una advertencia de que su equipo está infectado y se debe instalar un nuevo programa antivirus para limpiar la infección	Crítico	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> NO haga clic en ningún lugar dentro o cerca del cuadro de diálogo, ventana emergente o cuadro de advertencia Si debe continuar trabajando, cierre la casilla haciendo clic derecho en la barra de herramientas en la parte inferior de la pantalla y seleccionando "cerrar"

Síntoma: advertencias extrañas del sistema o un gran número de ventanas emergentes

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] Recibe advertencias extrañas del sistema o una gran cantidad de ventanas emergentes	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> No aplicable
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: El cursor se mueve por sí solo y/o los programas se inician por sí solos

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none">[Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none">[Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] El cursor se mueve por sí solo y/o se inician programas que no ha abierto	Crítico	[Edite según sea necesario] <ul style="list-style-type: none">No aplicable

Síntoma: No se puede acceder al Panel de control u otras herramientas del sistema en el equipo

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] No puede acceder al panel de control u otras herramientas del sistema (por ejemplo, administrador de tareas, configuración) Sin embargo, no ha podido acceder a estos en el pasado reciente	Rutinario	[Edite según sea necesario] <ul style="list-style-type: none"> No aplicable
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] No puede acceder al panel de control u otras herramientas del sistema (por ejemplo, administrador de tareas, configuración), a las que ha podido acceder en el pasado reciente	Crítico	[Edite según sea necesario] <ul style="list-style-type: none"> No aplicable

Síntoma: Los iconos del escritorio han cambiado/movido o se han agregado nuevos iconos

Observación	Plan de notificación	Posible solución al problema
[Edite según sea necesario] Los iconos del escritorio han cambiado o se han movido, o se han agregado nuevos iconos y ha tenido problemas para iniciar sesión en el equipo	Rutinario	[Edite según sea necesario] <ul style="list-style-type: none"> Confirme que inició sesión con la cuenta correcta y que está conectado a la red
[Edite según sea necesario] Los iconos del escritorio han cambiado o se han movido, o se han agregado nuevos iconos Ha iniciado sesión con la cuenta correcta y está conectado a la red	Sospechoso	[Edite según sea necesario] <ul style="list-style-type: none"> No aplicable
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: sitio web de jurisdicción o cuenta de redes sociales que muestra información errónea

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] El sitio web de la jurisdicción o la cuenta oficial de redes sociales con información de votación (por ejemplo, fechas, ubicaciones, horarios) muestra información errónea	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> IT determinará la causa de la información errónea (maliciosa o accidental)
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: Las cuentas de redes sociales no oficiales presentan información errónea

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] Parece que las cuentas de redes sociales no controladas por una jurisdicción gubernamental están proporcionando maliciosa o accidentalmente información errónea relacionada con la votación	Sospechoso	<p>[Edite según sea necesario]</p> <ul style="list-style-type: none"> Póngase en contacto con IT y el enlace de redes sociales para coordinar con el proveedor de redes sociales para eliminar el contenido y / o la página
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: correo electrónico sospechoso de una empresa legítima que solicita información confidencial

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Edite según sea necesario] El correo electrónico no está dirigido al destinatario El correo electrónico se refiere a una	Sospechoso	[Edite según sea necesario]

[INSERTAR NOMBRE DE LA JURISDICCIÓN] PLAN DE DETECCIÓN Y NOTIFICACIÓN DE INCIDENTES CIBERNÉTICOS [INSERTAR FECHA]

acción que no ha realizado (es decir, excedió el número de intentos de inicio de sesión para una cuenta) El correo electrónico solicita información confidencial o de identificación personal (PII) por correo electrónico		<ul style="list-style-type: none"> No haga clic en ningún enlace ni ingrese PII confidencial o PII Póngase en contacto con IT e informe por correo electrónico IT determinará qué otros usuarios (si los hay) recibieron el mismo correo electrónico, si alguien fue víctima de él, etc, y bloqueará / compartirá los indicadores asociados
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

[Insertar nombre o tipo de sistema/activo adicional]

Síntoma: [Insertar síntoma adicional de incidente cibernético]

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: [Insertar síntoma adicional de incidente cibernético]

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none"> [Inserte posibles soluciones al problema si corresponde]

Síntoma: [Insertar síntoma adicional de incidente cibernético]

Observación	Plan de notificación	Posible solución al problema
[Inserte la observación, si aplica]	Rutinario	<ul style="list-style-type: none">[Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Sospechoso	<ul style="list-style-type: none">[Inserte posibles soluciones al problema si corresponde]
[Inserte la observación, si aplica]	Crítico	<ul style="list-style-type: none">[Inserte posibles soluciones al problema si corresponde]

Síntoma: [Agregar sistemas/activos adicionales y tablas de síntomas según sea necesario]

Planes de notificación de incidentes

Los siguientes planes de notificación de incidentes especifican los procedimientos que deben seguirse cuando se observa un síntoma de incidente y la información de contacto de las partes designadas con quienes se debe contactar.

Se proporcionan planes para los siguientes niveles de criticidad:

1. Observaciones Rutinarias de IT (página *[Insertar número(s) de página]]*)
2. Observaciones sospechosas de IT (página *[insertar número(s) de página)*
3. Observaciones críticas de IT (página *[Insertar número(s) de página]]*)

Cómo utilizar los planes de notificación de incidentes

Inicie el Plan de notificación de incidentes que corresponda al nivel de criticidad determinado a partir de las Tablas de síntomas de incidentes en la Sección 2.

El plan seleccionado debe completarse en su totalidad.

Plan de notificación de observación rutinaria de IT

Fase	Acción
Alertas Interna	1a Contactos iniciales de observadores Apoyo informático de la División Electoral: [Ingrese el nombre y la información de contacto]
Escalamiento de incidentes	2a Es probable que las acciones de escalamiento no sean aplicables Nota: El personal de soporte de IT puede determinar que es necesario ponerse en contacto con el líder de soporte de IT para el diagnóstico 2b Si el diagnóstico de IT resulta en un incidente sospechoso o crítico, proceda a implementar acciones de comunicación y escalamiento en tablas "Sospechosas" o "Críticas", según corresponda

Plan de notificación de observación sospechosa de IT

Fase	Acción
Interno Alertas	<p>1a Contactos de observadores División Electoral Soporte de TI: [Ingrese el nombre y la información de contacto]</p> <p>1b El Observador notifica a los supervisores inmediatos y al Oficial Electoral supervisor de la posible violación: [Ingrese el nombre y la información de contacto]</p> <p>1c El funcionario electoral identifica y evalúa los posibles impactos en los sistemas e inicia planes de continuidad según sea necesario: [Plan #1 – Consideraciones de ejecución de entrada] [Plan #2 – Consideraciones de ejecución de entrada]</p> <p>1d El funcionario electoral notifica a los líderes de los sistemas de división interna para que proporcionen instrucciones de mitigación de IT, según corresponda: [Sistema de entrada, nombre del POC e información de contacto] [Sistema de entrada, nombre del POC e información de contacto]</p>
Escalamiento de incidentes	<p>2a El funcionario electoral notifica a los líderes de los sistemas de división estatal que proporcionen instrucciones de mitigación de IT, según corresponda: [Ingrese el nombre y la información de contacto]</p> <p>2b El líder de soporte de IT determina, si es necesario, ponerse en contacto con IT del condado y del estado para obtener asistencia adicional para diagnosticar impactos y determinar una resolución: [Ingrese el nombre de IT del condado y la información de contacto] [Estado de entrada Nombre de IT e información de contacto]</p> <p>2C Si el líder de soporte de IT confirma que la observación sospechosa es crítica, el funcionario electoral notifica a los POC estatales y federales apropiados: [Ingrese el nombre de la autoridad electoral estatal y la información de contacto] [Ingrese el nombre de CISA POC y la información de contacto] [Ingrese el nombre del POC EI-ISAC y la información de contacto]</p>

Plan de notificación de observación crítica de IT

Fase	Acción
Interno Alertas	<p>1a Contactos de observadores Líder de Soporte de IT de la División de Elecciones: [Ingrese el nombre y la información de contacto]</p> <p>1b El observador notifica a los supervisores y al funcionario electoral supervisor del incidente crítico: [Ingrese el nombre y la información de contacto]</p> <p>1c El funcionario electoral identifica y evalúa los posibles impactos en los sistemas del negocio e inicia planes de continuidad del negocio según sea necesario: [Plan #1 – Consideraciones de ejecución de entrada] [Plan #2 – Consideraciones de ejecución de entrada]</p> <p>1d El Director de Comunicaciones coordina el equipo interno para revisar e implementar las estrategias aplicables de relaciones públicas de emergencia y comunicación con los medios</p>
Escalamiento de incidentes	<p>2a El funcionario electoral notifica inmediatamente a los socios estatales y federales apropiados sobre incidentes críticos: [Ingrese el nombre de la autoridad electoral estatal y la información de contacto] [Nombre del centro de análisis e intercambio de información de estado de entrada e información de contacto] [Ingrese el nombre de la administración de emergencias del estado y la información de contacto] [Ingrese el nombre de CISA POC y la información de contacto] [Ingrese el nombre del POC EI-ISAC y la información de contacto] [Ingrese el nombre del POC local del FBI y la información de contacto]</p> <p>2b Director de apoyo tecnológico contacta a sus homólogos del condado y del estado para implementar acciones de mitigación del sistema de IT: [Ingrese el nombre de IT del condado y la información de contacto] [Estado de entrada Nombre de IT e información de contacto]</p>

[Opcional – Insertar Guía de Respuesta de Emergencia del Día de las Elecciones]