EVALUACIÓN DE RIESGO CIBERNÉTICO A LA INFRAESTRUCTURA ELECTORAL

Las elecciones justas y libres son un sello distintivo de la democracia estadounidense. La confianza del pueblo estadounidense en el valor de su voto depende de su confianza en la seguridad y resiliencia de la infraestructura que hace posible las elecciones nacionales. Por lo tanto, un proceso electoral que sea seguro y resistente es de sumo interés nacional y una de las principales prioridades de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés), del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) de Estados Unidos. CISA está trabajando de manera conjunta y coordinada con nuestros socios [nuestras contrapartes] federales, con quienes están al frente de las elecciones tales como gobiernos estatales y locales, funcionarios electorales y proveedores- con el fin de manejar riesgos a la infraestructura electoral de la nación. En este documento, CISA evalúa el riesgo a la infraestructura electoral con el fin de ayudar a la comunidad electoral a comprender y controlar el riesgo en sus sistemas críticos.

Para llevar a cabo este trabajo, el Centro Nacional de Gestión de Riesgos (NRMC, por sus siglas en inglés) de CISA evaluó múltiples criterios que cuantifican la escala del riesgo cibernético a infraestructura electoral, incluyendo la preparación de las máquinas, la red de dispositivos y la centralización de los componentes de infraestructura. El NRMC de CISA también evaluó criterios de riesgo adicionales relacionados con la inscripción de votantes, las máquinas de votación y la presentación electrónica de las boletas/boletas/papeletas electorales de votación.

CONCLUSIONES PRINCIPALES

Violaciones a la integridad de los sistemas de inscripción de votantes a nivel estatal, la preparación de los datos electorales (por ejemplo, la programación de las boletas/boletas/papeletas electorales de votación), los sistemas para tabulación de votos y los sitios web electorales presentan un riesgo específico en la capacidad que tienen las jurisdicciones para llevar a cabo las elecciones.

Cuando adecuados planes de control y de respuesta a incidentes no se ponen en práctica, los ataques cibernéticos a la disponibilidad de los sistemas estatales o locales que permiten la inscripción de votantes en el día de las elecciones, el registro en los centros de votación o el voto provisional, también pueden potencialmente convertirse en un riesgo significativo a la capacidad de las jurisdicciones para llevar a cabo las elecciones.

Aunque los sistemas de votación son un blanco de alta importancia para los agentes amenazantes, los ataques a escala tienen poca probabilidad de éxito, lo que significa que hay un menor riesgo de incidentes en comparación con otros componentes de la infraestructura del proceso electoral.

Los sistemas electorales de los Estados Unidos están compuestos por diversas infraestructuras y controles de seguridad, y muchos sistemas invierten significativamente en su seguridad. Sin embargo, incluso aquellas jurisdicciones que aplican las mejores prácticas de seguridad cibernética son potencialmente vulnerables a los ataques cibernéticos por parte de actores cibernéticos sofisticados, como actores a nivel nacional.

Las campañas de desinformación en conjunto con ataques cibernéticos a la infraestructura electoral pueden entorpecer los procesos electorales y debilitar la confianza del público en los resultados de las elecciones.

NOTA DE ALCANCE: El Centro Nacional de Gestión de Riesgos (NRMC, por sus siglas en inglés) de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) preparó esta evaluación de riesgos con el fin de apoyar los esfuerzos de CISA para ayudar a los gobiernos estatales y locales en los Estados Unidos a mitigar las vulnerabilidades de los sistemas electorales, y respaldar la ciberseguridad y la resiliencia del sistema dentro de los sistemas electorales. Este producto proporciona un análisis fundamental que los funcionarios electorales pueden utilizar para priorizar y adaptar los esfuerzos de gestión de riesgos con el fin de manejar las vulnerabilidades específicas en los componentes de alto riesgo en el sistema electoral, y para promover la seguridad cibernética y la resiliencia del sistema dentro de los sistemas electorales. Dar prioridad a la acción de mitigar el riesgo de posibles ataques cibernéticos a la integridad de los componentes del sistema electoral puede producir el mayor beneficio marginal en el mejoramiento de los perfiles de riesgo estatales.

El NRMC de CISA coordinó este análisis con la División de Ciberseguridad de CISA (CSD, por sus siglas en inglés) y el Centro de Misión Cibernética (CYMC, por sus siglas en inglés) de la Oficina de Inteligencia y Análisis (I&A por sus siglas en inglés) de DHS.

ANÁLISIS DE LOS SISTEMAS DE INFRAESTRUCTURA ELECTORAL

La infraestructura electoral se compone de un conjunto diverso de sistemas, redes y procesos. El sistema electoral de Estados Unidos no se refiere a un único sistema, sino a un conjunto de múltiples sistemas diferentes. El ecosistema de infraestructura electoral de cada jurisdicción es un conjunto de componentes diferentes, algunos interconectados electrónicamente y otros no, y que deben funcionar en conjunto para llevar a cabo las elecciones. Aunque realizan las mismas funciones, los procesos y la infraestructura del sistema varían de un estado a otro, y a menudo difieren incluso entre condados, parroquias, pueblos o ciudades dentro de un estado o territorio.[1]

La figura 1 ofrece una idea general del funcionamiento de un ecosistema electoral estadounidense.

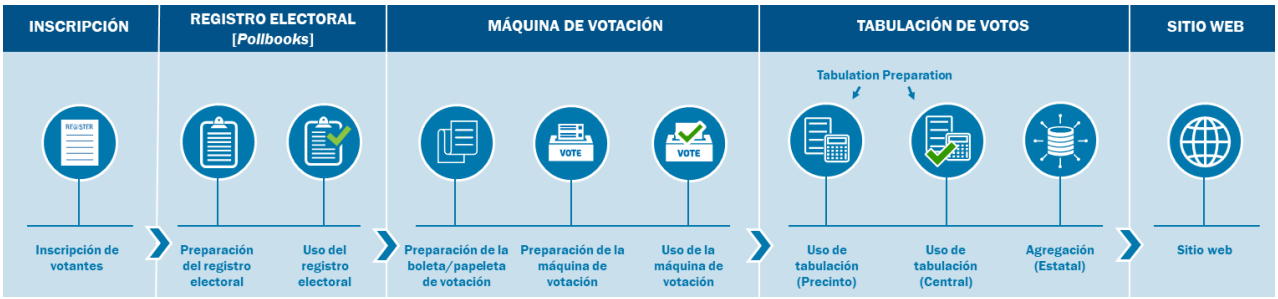

FIGURA 1- ECOSISTEMA FUNCIONAL DEL SISTEMA ELECTORAL

Los sistemas electorales hacen uso de diversas infraestructuras y controles de seguridad. Incluso las jurisdicciones que implementan las mejores prácticas de seguridad cibernética son potencialmente vulnerables a los ataques de actores cibernéticos sofisticados, como actores avanzados a nivel estatal o nacional. Por lo tanto, los métodos de detección y de recuperación son tan importantes como las medidas de prevención.

Los ataques cibernéticos a la integridad de la inscripción de los votantes a nivel estatal, al registro electoral y a los sitios web electorales, así como a la preparación de las boletas/papeletas electorales, las máquinas de votación y los sistemas de tabulación, tienen el potencial de causar el mayor impacto funcional a la capacidad de las jurisdicciones para llevar a cabo las elecciones, basándose en el análisis[i] de errores de los componentes del sistema electoral en cada fase del proceso electoral. La siguiente infraestructura electoral

[i] El análisis de errores es un método muy utilizado en el análisis de la fiabilidad, el mantenimiento y la seguridad de los sistemas. Se trata de un procedimiento deductivo utilizado para determinar las combinaciones de errores en el hardware y el software y los errores humanos que podrían causar resultados no deseados a nivel del sistema.

representa los sistemas, redes y procesos más críticos para la seguridad, la integridad y la resiliencia de las elecciones estadounidenses:

- **Las bases de datos del registro electoral** se utilizan para ingresar, almacenar y editar la información del registro electoral, tales como los servidores donde permanecen las bases de datos y los portales en línea que proporcionan acceso. La inscripción de votantes es un proceso continuo de creación de nuevos registros, actualización de los existentes y eliminación de los obsoletos. Las bases de datos de registro de votantes reciben información de forma automática e indirecta (es decir, a través del ingreso manual) de una variedad de fuentes, incluyendo otras agencias gubernamentales (por ejemplo, del Departamento de Vehículos y Motores) y organizaciones que ayudan en el proceso de registro (por ejemplo, las campañas de inscripción de votantes). Las bases de datos contienen la información relacionada con el derecho que una persona tiene de votar o no, dónde pueden votar y en qué estilo de boleta/papeleta única votarán, basándose en la ubicación geográfica del votante dentro de múltiples círculos de distritos políticos y fiscales.
- **Los registros electorales electrónicos y de papel** contienen información sobre los votantes registrados en los centros de votación, y pueden utilizarse para inscribir a los votantes cuando así lo permita la ley. Antes de su utilización, los registros electorales deben prepararse transfiriendo la información en la base de datos de registro electoral. Los registros electorales tienen componentes tecnológicos y de procesamiento para ver, editar y modificar dichos registros de votantes. Los registros electorales pueden estar o no conectados en red. Los registros electorales en red están conectados a una base de datos externa y pueden incluir una conexión directa a la base de datos del registro de votantes o a un servidor independiente. Los registros electorales no conectados a la red se encuentran en papel o son archivos digitales estáticos localizados en computadores.
- **La preparación de las boletas/papeletas electorales** es el proceso de conectar las geopolíticas con las contiendas y los candidatos específicos de cada distrito, para luego traducir esos diseños en combinaciones únicas de datos de las boletas/papeletas electorales. Los datos de preparación de las boletas/papeletas electorales adoptan diversas formas, como las imágenes de las boletas/papeletas electorales (tanto en papel como en formato electrónico), los archivos de datos necesarios para construir las imágenes de las boletas/papeletas electorales, los archivos de audio para las boletas/papeletas electorales de uso especial y los archivos específicos para la exportación a sistemas externos, como sitios web o sistemas digitales usados de acuerdo a la Ley de Voto en Ausencia para Personal Uniformado y Ciudadanos Residentes en el Exterior (UOCAVA, por sus siglas en inglés). La preparación de las boletas/papeletas electorales también genera datos necesarios para la tabulación de los votos en una máquina de votación y la tabulación de los votos contados en una jurisdicción o en un estado. Este proceso suele completarse en un sistema de gestión electoral.
- **Los sistemas de máquinas de votación** consisten en tecnología y procesos utilizados para emitir y, en algunos casos, generar las boletas/papeletas electorales de los votantes de todo tipo (sistemas en papel, y sistemas electrónicos, como dispositivos de marcado de boletas/papeletas electorales y máquinas electrónicas de registro directo con o sin una auditoría de papel verificada por el votante). Las máquinas de votación abarcan tanto la tecnología como los procesos utilizados por los funcionarios electorales para preparar las máquinas de votación para la tabulación de las boletas/papeletas electorales y, en algunos casos, para su presentación. Específicamente, incluye la carga de los archivos de las boletas/papeletas electorales creados durante la preparación de éstas en las máquinas de votación. Las máquinas de votación se almacenan bajo la custodia de funcionarios electorales, pero tras su entrega, se colocan en los centros de votación para su uso durante la votación anticipada y durante el día de las elecciones. Las máquinas de votación son la forma de tecnología más visible con la que interactúan los votantes durante el proceso de votación.
- **Los sistemas centralizados de tabulación y conteo de votos** se utilizan para contabilizar los votos compartidos por sub-jurisdicciones tales como condados, distritos electorales y, en algunos casos, las máquinas individuales o incluso las boletas/papeletas electorales individuales. Estos sistemas recogen y procesan los datos para determinar el resultado de una contienda electoral. La tabulación comprende tanto la tecnología como los procesos utilizados para contar los votos y agregar los resultados. Los procesos de tabulación de votos incluyen el recuento manual, el escaneo óptico de

boletas/papeletas electorales y la tabulación electrónica directa. La tabulación de los votos puede realizarse a nivel de distrito electoral, además de la tabulación centralizada.

- **Los sitios web oficiales son** utilizados por los funcionarios electorales para comunicar información al público, incluyendo cómo registrarse para votar, dónde votar (por ejemplo, herramientas de búsqueda de precintos), y para transmitir los resultados de las elecciones (por ejemplo, sistemas de informes durante la noche de las elecciones). A veces, los sitios web electorales se encuentran bajo infraestructuras que son propiedad del gobierno, pero a menudo se encuentran bajo empresas comerciales.
- **Instalaciones de almacenamiento**, que pueden estar situadas en una propiedad pública o privada, y pueden utilizarse para almacenar la infraestructura del sistema electoral y de votación antes de la jornada electoral.
- **Los colegios electorales** (incluidos los lugares de votación anticipada) son lugares donde los individuos emiten su voto y pueden estar ubicados físicamente en una propiedad pública o privada.
- **Las oficinas electorales** son lugares donde los funcionarios electorales llevan a cabo sus actividades oficiales, incluidos los espacios de trabajo compartidos, como las bibliotecas públicas, los edificios municipales, los domicilios particulares y las zonas públicas de las jurisdicciones que no disponen de un espacio de trabajo específico.

CONSECUENCIAS DEL ATAQUE CIBERNÉTICO A LA INFRAESTRUCTURA ELECTORAL

El análisis determinó que los ataques cibernéticos en cada componente del ecosistema de la infraestructura electoral pueden tener diferentes consecuencias, según el tipo de impacto cibernético y del componente específico del sistema electoral al que van dirigidos. Esta evaluación utilizó el modelo[ii] de seguridad de la información Confidencialidad-Integridad-Disponibilidad (CIA, por sus siglas en inglés) para analizar tres tipos de ataque cibernéticos:

- Ataques a la confidencialidad, el robo de información.
- Ataques a la integridad, la modificación de la información o de la funcionalidad de un sistema.
- Ataques a la disponibilidad, la interrupción o la privación de uso del sistema.

Los riesgos también pueden ser diferentes para el mismo componente durante la preparación y durante el uso (por ejemplo, las máquinas de votación pueden ser más accesibles a los ataques cibernéticos durante la preparación que el día de las elecciones). Además, un ataque cibernético exitoso en una máquina de votación también podría atacar consecutivamente a un sistema de tabulación o agregación si el programa informático maligno [malware] se transfiere después de la votación.

La tabla 1 ofrece una visión general de alto nivel con referencia a las posibles consecuencias de un ataque cibernético exitoso contra cada componente del sistema. Esta tabla no aborda directamente los ataques cibernéticos destinados a disminuir la confianza del público en las elecciones, aunque los tres tipos de ataques podrían tener como objetivo principal o secundario el disminuir dicha confianza.

TABLA 1- CONSECUENCIA POTENCIAL DE UN CIBERATAQUE ELECTORAL SEGUN COMPONENTE

COMPONENTE ELECTORAL	CONSECUENCIAS EN CONFIABILIDAD	CONSECUENCIAS EN INTEGRIDAD	CONSECUENCIAS EN DISPONIBILIDAD
Inscripción de votantes	Exponer información no pública del registro electoral	Cambiar la información del registro electoral	Impedir el acceso a la información del registro electoral

[ii] Para más información sobre la tríada de CIA, consulte: Centro para la Seguridad en Internet, "EI-ISAC Cybersecurity Spotlight - CIA Triad", 2019, https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/. Consultado el 28 de julio de 2020.

COMPONENTE ELECTORAL	CONSECUENCIAS EN CONFIABILIDAD	CONSECUENCIAS EN INTEGRIDAD	CONSECUENCIAS EN DISPONIBILIDAD
Preparación del registro electoral	Exponer la información no pública del registro electoral	Cambiar la información del registro electoral	Impedir el acceso a la información del registro electoral
Preparación de la boleta/papeleta electoral	Exponer la información de la boleta/papeleta electoral	Cambiar la información de la boleta/papeleta electoral durante la preparación	Impedir la preparación de la boleta/papeleta electoral
Preparación de la máquina de votación	Cambiar la funcionalidad de la máquina de votación para exponer las selecciones del votante	Cambiar la funcionalidad de la máquina de votación (presentación de la boleta electoral /registro de selecciones)	Impedir la funcionalidad de la máquina de votación
Preparación de la tabulación	Cambiar la funcionalidad de la máquina de conteo para exponer los resultados	Cambiar la funcionalidad de la máquina de tabulación	Impedir la funcionalidad de la máquina de tabulación
Uso del registro electoral	Exponer información no pública del registro electoral	Cambiar la información del registro electoral	Impedir el acceso a la información del registro electoral
Uso de la máquina de votación	Exponer las selecciones del votante	Cambiar la funcionalidad de la máquina de votación	Impedir la funcionalidad de la máquina de votación
Tabulación (Precinto)	Exponer los resultados de la tabulación antes de lo previsto	Cambiar los resultados de la tabulación de los votos	Impedir la tabulación de los votos
Tabulación (Centralizada)	Exponer los resultados de la tabulación de los votos antes de lo previsto (Agregación)	Cambiar los resultados de la tabulación de los votos (Agregación)	Impedir la tabulación de los votos (Agregación)
Agregación (Estatal)	Exponer los resultados de la tabulación de los votos antes de lo previsto	Cambiar los resultados de la tabulación de los votos	Impedir la tabulación de votos
Sitio web	Exponer información no supuesta para la divulgación pública	Cambiar los resultados comunicados	Impedir la comunicación de resultados
Sitio web	Exponer información no supuesta para la divulgación pública	Cambiar la información del registro electoral y del distrito electoral (en el buscador de votantes)	Evitar la búsqueda de información sobre el registro y la inscripción de los votantes

INFRAESTRUCTURA ELECTORAL CONJUNTA Y ATAQUES DE DESINFORMACIÓN

Los actores extranjeros estatales y no estatales aprovechan las actividades de información como parte de amplias campañas para sembrar la discordia, manipular el discurso público y desacreditar el sistema electoral

para debilitar los pilares de la democracia. En el contexto de las elecciones, las entidades extranjeras tienen como objetivo:

- Disuadir al público objetivo de participar en el proceso electoral a través de contenidos que sugieran que sus votos no importan, que abstenerse de votar es la acción más democrática, o a través de contenidos que engañen a los votantes acerca del proceso de votación.
- Influir en la selección de candidatos mediante, entre otras actividades, la difusión de contenidos inventados y favorables acerca de los candidatos favoritos, y de contenidos inventados o denigrantes sobre los candidatos no favoritos..
- Dañar la percepción pública de unas elecciones justas y libres mediante la difusión de contenidos falsos o engañosos sobre los procesos y resultados electorales.

Estas campañas de desinformación, llevadas a cabo en conexión con los ataques cibernéticos a la infraestructura electoral, pueden entorpecer los procesos electorales y debilitar la confianza del público en los resultados de las elecciones. El acceso no autorizado a la red permite hacer vigilancia y seguimiento, y ofrece oportunidades para realizar ataque cibernéticos devastadores. La información robada o falsificada puede transmitirse estratégicamente para dar forma a narrativas falsas. El secuestro de personas en línea y la desconfiguración o alteración de sitios web usados por el público, pueden aprovecharse para influir en la opinión pública. El ataque a los sistemas gubernamentales (incluso sin compromiso alguno) puede ser utilizado para formar narrativas que conduzcan a la desconfianza en el gobierno como administrador de la información de los ciudadanos.

CRITERIOS DE RIESGO DE LA INFRAESTRUCTURA ELECTORAL

Basándose en estas consecuencias, la evaluación aplicó múltiples criterios que valoran la escala del riesgo cibernético asociado a la infraestructura electoral. La escala potencial de un ataque cibernético a la infraestructura electoral se basa en factores que incluyen si la infraestructura está siendo preparada para su uso o si está en uso, si la tecnología de la infraestructura está en red y el grado de centralización de los componentes de la infraestructura. Las consideraciones de los criterios de riesgo no son mutuamente excluyentes.

CISA también evalúa criterios de riesgo adicionales relacionados con el registro de votantes, las máquinas de votación y la presentación electrónica de las boletas/papeletas electorales.

Escala de ataque: Preparación del sistema

La escala potencial de un ciberataque a la infraestructura electoral será más amplia si un ataque cibernético sucede durante la preparación o programación de la infraestructura electoral para su uso inmediato. Mientras que un ataque cibernético a la integridad de una sola máquina de votación en un recinto electoral afectaría a esa máquina o recinto, los ataques cibernéticos ocurridos durante la preparación o programación central de las máquinas de una jurisdicción pueden afectar a toda una jurisdicción que utilice esas máquinas. Si la preparación de las máquinas se lleva a cabo a nivel estatal, los ataques cibernéticos durante proceso de preparación tienen el potencial de afectar a todo un estado. Esto es el caso para una única elección. Sin embargo, el malware colocado en una sola máquina durante su uso podría propagarse al sistema de tabulación y de preparación, y a todas las otras máquinas para futuras elecciones si las jurisdicciones no implementan mejores prácticas para utilizar una arquitectura de sistemas de software electoral segura.

Durante la preparación del sistema, las jurisdicciones electorales dependen de archivos de fuentes externas, como bases de datos de registro, proveedores de sistemas de votación, impresoras de boletas/papeletas electorales o programadores de boletas/papeletas electorales.

La importación de datos de fuentes externas supone un riesgo, ya que las fuentes pueden utilizar sistemas conectados al Internet y que no implementan prácticas de ciberseguridad sólidas. Además, una fuente externa

puede presentar un vector de ataque cibernético contra una amplia variedad de jurisdicciones electorales si una única fuente presta servicio a múltiples jurisdicciones o estados.

Escala de ataque: Red de sistemas

La escala de un ataque cibernético a la infraestructura electoral tiene el potencial de ser más amplia si un ataque compromete su infraestructura en red. Por ejemplo, en algunas jurisdicciones los registros electorales electrónicos están conectados en red a lo largo de toda la jurisdicción para facilitar el funcionamiento de los centros de votación, mientras que en otras jurisdicciones los registros electorales electrónicos no están conectados en red. Un ataque cibernético a un colegio electoral individual no conectado en red tiene menos posibilidades de propagarse si la máquina permanece aislada de la red. Un ataque a la integridad de un registro electoral electrónico en la red tiene el potencial de afectar a toda la jurisdicción, mientras que un ataque a la integridad de un registro de votación local, no conectado a la red, puede quedar aislado en ese lugar de votación especifico.

Por ello, consideramos que la conectividad en la red para los sistemas de votación es de alto riesgo. La creación y el mantenimiento de un espacio aéreo para los sistemas críticos, como los sistemas de emisión o tabulación de votos, es una práctica recomendable.[iii]

Escala de ataque: Centralización

La escala potencial de un ataque cibernético será más amplia si un ataque se dirige a un proceso centralizado frente a un proceso localizado. Algunas jurisdicciones tabulan los votos en cada lugar de votación antes de agregar los resultados en una locación central, mientras que otras sólo tabulan los votos en una locación central. Un ataque a la integridad de los sistemas o procesos centrales de tabulación puede tener un mayor alcance que un ataque a la integridad del proceso de tabulación local.

El cuadro 2 ofrece un breve resumen de los criterios utilizados para evaluar el riesgo cibernético asociado a la escala potencial de un ataque cibernético a las elecciones, evaluado para cada componente de la infraestructura electoral. Clasificamos la escala de un ataque en una de las siguientes tres categorías:

- Baja: Afecta a un subconjunto de una jurisdicción
- Media: Afecta a toda una jurisdicción
- Alta: Afecta a todo un estado o a varias jurisdicciones

Para un análisis más detallado del riesgo cibernético por componente, consulte la "Tabla 3-Matriz de prioridad de riesgos en la infraestructura electoral" en la página 10.

TABLA 2- ESCALA POTENCIAL DE UN ATAQUE CIBERNÉTICO ELECTORAL POR COMPONENTE

COMPONENTE ELECTORAL	VECTOR DE ATAQUE	ESCALA
Inscripción de votantes	Base de datos del registro jurisdiccional	Media
Inscripción de votantes	Base de datos del registro estatal	Alta

[iii] Un espacio de aire es una separación física entre sistemas que requiere que los datos se muevan mediante algún procedimiento manual externo.

COMPONENTE ELECTORAL	VECTOR DE ATAQUE	ESCALA
Registro electoral	Preparación del registro electoral jurisdiccional	Media
Registro electoral	Preparación del registro electoral estatal	Alta
Registro electoral	Uso del registro electoral fuera de línea [registro físico]	Baja
Registro electoral	Uso del registro electoral jurisdiccional en línea	Media
Registro electoral	Uso del registro electoral estatal en línea	Alta
Preparación de las boletas/papeletas electorales	Preparación de las boletas/papeletas electorales a nivel jurisdiccional	Media
Preparación de las boletas/papeletas electorales	Preparación de las boletas/papeletas electorales a nivel estatal	Alta
Máquina de votación	Preparación de las máquinas de votación a nivel jurisdiccional	Media
Máquina de votación	Preparación de las máquinas de votación a nivel estatal	Alta
Máquina de votación	Uso de las máquinas de votación	Baja
Tabulación	Preparación del conteo	Media
Tabulación	Conteo de votos a nivel de precintos	Baja
Tabulación	Conteo de votos centralizado	Media
Tabulación	Agregación a nivel estatal	Alta

COMPONENTE ELECTORAL	VECTOR DE ATAQUE	ESCALA
Sitio web	Sitio web jurisdiccional	Media
Sitio web	Sitio web estatal	Alta

Número de votantes registrados

Las jurisdicciones electorales varían mucho de tamaño, ya que algunas tienen tan sólo 100 votantes, pero las más grandes contienen varios millones de votantes.[2] Las jurisdicciones con más votantes registrados asumen más riesgos que las jurisdicciones con poblaciones de votantes más pequeñas. El número de votantes registrados representa el número de individuos en cada jurisdicción que podrían tener información personal expuesta durante un ataque de confidencialidad o experimentar interrupciones en los centros de votación como resultado de ataque cibernéticos, o impactos consecutivos a las elecciones causados por incidentes físicos.

Configuración del sistema de registro electoral

Los estados con un sistema de registro de votantes descendente mantienen[3] los datos en una única plataforma central de hardware, que es mantenida por el estado con datos e información suministrados por las jurisdicciones locales. Los sistemas ascendentes incluyen datos ubicados en hardware local, compilados periódicamente para formar una lista de registro electoral a nivel estatal. Los sistemas híbridos son una combinación de las características descendentes y ascendentes. Desde el 2018, un total de 39 estados y territorios tienen sistemas de registro electorales con configuraciones[4] descendentes.

Los estados con sistemas de registro de votantes descendentes presentan a los atacantes un sistema único que al verse comprometido, podría interrumpir el proceso de votación a una escala más amplia que los sistemas a nivel de jurisdicción. Dado que los sistemas de registro de votantes descendentes mantienen toda la base de datos del registro electoral de un estado, presentan un único objetivo de ataque que podría afectar a muchos más votantes. Un sistema ascendente o híbrido requeriría atacar a un número diverso de sistemas en el estado para lograr resultados similares. Sin embargo, es más probable que la seguridad cibernética y física de los sistemas descendentes sea más fuerte que la de los sistemas ascendentes o híbridos, basándose en una revisión de los recursos y el apoyo general de la ciberseguridad a nivel estatal y local.

Inscripción de votantes en línea

La inscripción electoral en línea permite a los residentes llenar los formularios para registro de votantes en línea. Cuarenta estados y territorios ofrecen un portal de registro de votantes en línea en el que las personas pueden inscribirse por su cuenta, sin tener que presentar un formulario en papel.[5]

Los sistemas de inscripción electoral en línea proporcionan un punto adicional de vulnerabilidad que permite a los ciberactores acceder a las bases de datos de registro de votantes y llevar a cabo ataques[6] a la confidencialidad, la integridad o la disponibilidad. Los piratas informáticos, incluidos los actores de los estados nacionales, han explotado las bases de datos de votantes en el pasado para obtener acceso ilícito a la información del electorado.[7]

Es probable que medidas como el registro[iv] el mismo día y las boletas/papeletas electorales provisionales reduzcan el impacto de los ataques a la integridad de los sistemas de inscripción electoral, al proporcionar un mecanismo a prueba de errores que permita a los votantes elegibles corregir los datos manipulados o borrados, y votar utilizando los procesos establecidos. Los procesos de voto provisional requeridos por la Ley 'Ayuda a América a Votar' (Help America Vote Act) también proporcionan una medida de protección contra errores. Aunque el registro en el mismo día y los votos provisionales pueden proporcionar alguna protección, ambos tienen el potencial de causar interrupciones en los centros de votación debido a tiempos de procesamiento más largos que pueden ser necesarios para administrar los votos provisionales (aproximadamente un 15 por ciento más largo que el de los procesos de votación regulares, dependiendo de los procesos[v] específicos que los funcionarios electorales implementen). Además, muchos funcionarios electorales creen que la mejor implementación del registro en el mismo día utiliza tecnología conectada a la red, como los registros electorales electrónicos, lo que genera riesgos de conexión al sistema en la red, como se ha comentado anteriormente.

Máquinas de votación sin registro de papel auditable verificado por el votante

Las máquinas de votación electrónica de registro directo capturan los datos de la votación directamente en la memoria[8] electrónica. Muchas máquinas de votación electrónica de registro directo vienen equipadas con una función de registro de auditoría en papel verificado por el votante que proporciona una impresión, verificable por los votantes, para garantizar que sus votos se capturan correctamente. Desde 2016, muchos funcionarios electorales en todo el país reemplazaron los sistemas que no tienen un registro de papel auditable verificado por el votante con sistemas de votación que sí lo tienen. Basándose en la investigación, CISA estima que más del 90% de los votos emitidos en 2020 tendrán el correspondiente registro auditable.

Se cree que los sistemas de votación sin registro de papel auditable verificado por el votante presentan un riesgo adicional, basándonos en el análisis de la dificultad de identificar la manipulación electrónica para garantizar la integridad de las elecciones en caso de un ataque cibernético. La existencia de un registro de papel auditable verificado por el votante es el primer paso en la fomentar resiliencia, ya que puede permitir a los funcionarios electorales verificar que los resultados de la elección son correctos, independientemente de que se produzca un error o fallo no detectado en el sistema de votación. Sin embargo, para ofrecer a los votantes una amplia garantía de que se detectarán los errores, los funcionarios electorales también deben realizar auditorías periódicas de sus elecciones.

Las medidas para verificar la lógica y la exactitud, tales como el monitoreo[vi] paralelo y la verificación[vii] con el fin de garantizar la integridad del software, mejoran la capacidad de detección y recuperación de los sistemas de votación por parte de funcionarios electorales; especialmente de aquellos que carecen de un registro que no puede auditarse de otro modo, aunque ninguna de estas medidas puede sustituir el uso de copias de seguridad en papel para identificar irregularidades y reducir el riesgo.

[iv] La inscripción del mismo día es el procedimiento a través del cual las personas se registran para votar y emiten su voto el mismo día. Según la Encuesta de Administración Electoral y Votación de la Comisión de Asistencia Electoral de Estados Unidos, 26 estados ofrecen alguna forma de registro el mismo día, desde 2018.

[v] Los procesos de votación provisional, o el voto provisional, mantienen la intención de voto del individuo hasta que los funcionarios electorales determinan el estado de elegibilidad del individuo para emitir su voto en la elección. Todos los estados, excepto Minnesota, New Hampshire y Dakota del Norte, emiten votos provisionales a las personas el día de las elecciones, de acuerdo con la sección 302 de la ley Help America Vote.

[vi] El monitoreo paralelo es el proceso de poner a prueba un conjunto de máquinas de votación seleccionadas al azar para ser examinadas en modo electoral durante el período de votación. La intención es intentar "engañar" al sistema para que piense que está en un lugar de votación y que está siendo utilizado directamente en las elecciones. Las pruebas paralelas pueden así detectar si se ha desplegado un software malicioso para que sólo surta efecto en un modo específico (es decir, el modo electoral) o durante un tiempo determinado (es decir, el día de las elecciones).

[vii] Las pruebas de uniformidad [Hash checks] son útiles para verificar la integridad de los datos y se llevan a cabo comparando el valor uniforme de los datos recibidos con el valor de uniforme de los datos tal y como fueron enviados para detectar si los datos fueron alterados.

Boletas/Papeletas Electrónicas de conformidad con la Ley de Voto en Ausencia del Personal Uniformado y de Ciudadanos Residentes en el Exterior

Ciertos grupos de votantes, en particular la población militar y los votantes residentes en el exterior tienen dificultades para votar en persona o por correo. Todas las jurisdicciones están obligadas a ofrecer boletas/papeletas electorales electrónicas, según la ley federal. Muchos funcionarios electorales estatales y locales hacen uso de correo electrónico, fax y portales en línea para facilitar la devolución de las boletas/papeletas electorales por parte de estos grupos.[9, 10] Treinta[viii] y un estados, y el District of Columbia (D.C.) permiten a los votantes amparados por la Ley de Voto en Ausencia del Personal Uniformado y de Ciudadanos Residentes en el Exterior presentar sus boletas/papeletas electorales por al menos un medio electrónico, como el portal de Internet, el correo electrónico o el fax.[11] Cinco estados (Arizona, Colorado, Missouri, North Dakota y West Virginia) permiten a los votantes amparados por la Ley de Voto en Ausencia del Personal Uniformado y de Ciudadanos Residentes en el Exterior devolver las boletas/papeletas electorales a través de un portal o aplicación en la red. Además, varios condados de Utah, Colorado y Oregon llevaron a cabo una prueba piloto con una aplicación de voto por teléfono móvil y están determinando su uso en el futuro.[12] West Virginia utilizó una aplicación similar en elecciones anteriores. Diecinueve[ix] estados y el D.C. permiten a algunos votantes devolver las boletas/papeletas electorales por correo electrónico o fax, mientras que siete estados[x] permiten a algunos votantes devolver las boletas/papeletas electorales exclusivamente por fax.

Se considera que la devolución de las boletas/papeletas electorales electrónicas presenta un riesgo adicional, sea por correo electrónico, fax, portal en línea o aplicación móvil, debido a la dificultad de asegurar la transmisión electrónica de datos. Las boletas/papeletas electorales enviadas por medios electrónicos están sujetas a un mayor potencial de interrupción, manipulación o exposición.

Los riesgos para la devolución de las boletas/papeletas electorales electrónicas son similares a los de las boletas/papeletas electorales por correo, pero con el potencial de afectar a un mayor número de boletas/papeletas electorales. Por ejemplo, un ataque intrusivo "man-in-the-middle" en una papeleta física por correo requiere acceso físico, y la escala del ataque está limitada por los procedimientos implementados en la cadena de custodia. En cambio, un actor cibernético malintencionado puede llevar a cabo un ataque intrusivo contra las boletas/papeletas electorales electrónicas a mayor escala desde una amplia gama de ubicaciones globales.

MATRIZ DE PRIORIZACIÓN DE RIESGOS DE LA INFRAESTRUCTURA ELECTORAL

El CISA NRMC evalúa la diversidad relativa de riesgo cibernético agregado según cada componente de la infraestructura electoral, basándose en el análisis de errores. La matriz de priorización que se presenta a continuación se calcula sobre la base de la capacidad técnica necesaria para llevar a cabo un ataque[xi] cibernético, la escala potencial de impacto de un ataque cibernético y una puntuación de importancia[xii], para proporcionar una visión del riesgo en cada componente del sistema electoral. Dado que las implementaciones de los sistemas electorales varían ampliamente entre jurisdicciones, el CISA NRMC evaluó tanto el "mejor caso" como el "peor caso" de implementación del sistema para cada componente electoral. Esta visión del "mejor caso" y del "peor caso" afecta a la capacidad técnica necesaria para atacar cada componente, pero no altera la escala de ataque ni su importancia.

[viii] Los 31 estados son: Alaska, Arizona, California, Colorado, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Massachusetts, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Texas, Utah, Washington, and West Virginia.
[ix] Los 19 estados son: Delaware, Hawaii, Idaho, Indiana, Iowa, Kansas, Maine, Massachusetts, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, Oregon, South Carolina, Utah, and Washington.
[x] Los siete estados son: Alaska, California, Florida, Louisiana, Oklahoma, Rhode Island and Texas.
[xi] La capacidad técnica se determinó en función de la dificultad relativa de ataque al componente.
[xii] La puntuación de importancia se determinó a partir de las medidas de la escala de importancia agregada asignadas por un grupo de expertos de funcionarios electorales y proveedores de tecnología.

El cuadro 3 ofrece una visión detallada del riesgo cibernético relativo para los componentes electorales en el mejor caso (el más seguro) y en el peor caso (el más vulnerable) de implementación del sistema, evaluado por componente y por tipo de ataque cibernético. La tabla representa el cambio en la calificación del riesgo cuando se implementan los controles de seguridad recomendados en lugar de los controles de seguridad bajos. En el caso de aquellos sistemas de infraestructura electoral que implementan bajos niveles de controles de seguridad, asumimos que cualquier actor capaz de amenaza puede poseer la capacidad de realizar ataques exitosos contra los sistemas de infraestructura electoral. A su vez, la aplicación en la infraestructura electoral de controles de seguridad recomendados reduce significativamente el riesgo de un ataque cibernético exitoso. Algunos componentes, incluso al implementar los controles de seguridad recomendados, muestran un mayor riesgo de ataques a la disponibilidad, tal como se detalla en la siguiente tabla.

TABLA 3 MATRIZ DE PRIORIZACIÓN DE RIESGOS DE LA INFRAESTRUCTURA ELECTORAL

COMPONENTE	TIPO DE ATAQUE	ESCALA DE ATAQUE	Control bajo HABILIDAD DEL ATACANTE	Control bajo CLASIFICACIÓN DE RIESGO	Control recomendado HABILIDAD DEL ATACANTE	Control recomendado CLASIFICACIÓN DE RIESGO
Base de datos del registro jurisdiccional	Confiabilidad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Base de datos del registro jurisdiccional	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Base de datos del registro jurisdiccional	Disponibilidad	Media	Actor Nivel 3	Medio	Actor Nivel 2	Bajo
Base de datos del registro estatal	Confiabilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Base de datos del registro estatal	Integridad	Alta	Actor Nivel 3	Alto	Actor Nivel 1	Bajo
Base de datos del registro estatal	Disponibilidad	Alta	Actor Nivel 3	Alto	Actor Nivel 2	Medio
Preparación del registro electoral a nivel jurisdiccional	Confiabilidad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo

COMPONENTE	TIPO DE ATAQUE	ESCALA DE ATAQUE	Control bajo HABILIDAD DEL ATACANTE	Control bajo CLASIFICACIÓN DE RIESGO	Control recomendado HABILIDAD DEL ATACANTE	Control recomendado CLASIFICACIÓN DE RIESGO
Preparación del registro electoral a nivel jurisdiccional	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación del registro electoral a nivel jurisdiccional	Disponibilidad	Media	Actor Nivel 3	Medio	Actor Nivel 2	Bajo
Preparación del registro electoral a nivel estatal	Confiabilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación del registro electoral a nivel estatal	Integridad	Alta	Actor Nivel 3	Alto	Actor Nivel 1	Medio
Preparación del registro electoral a nivel estatal	Disponibilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 2	Medio
Uso del registro electoral fuera de línea	Confiabilidad	Baja	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Uso del registro electoral fuera de línea	Integridad	Baja	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Uso del registro electoral fuera de línea	Disponibilidad	Baja	Actor Nivel 3	Bajo	Actor Nivel 2	Bajo
Uso en línea del registro electoral a nivel jurisdiccional	Confiabilidad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo

COMPONENTE	TIPO DE ATAQUE	ESCALA DE ATAQUE	Control bajo HABILIDAD DEL ATACANTE	Control bajo CLASIFICACIÓN DE RIESGO	Control recomendado HABILIDAD DEL ATACANTE	Control recomendado CLASIFICACIÓN DE RIESGO
Uso en línea del registro electoral a nivel jurisdiccional	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Uso en línea del registro electoral a nivel jurisdiccional	Disponibilidad	Media	Actor Nivel 3	Medio	Actor Nivel 2	Bajo
Uso en línea del registro electoral a nivel estatal	Confiabilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Uso en línea del registro electoral a nivel estatal	Integridad	Alta	Actor Nivel 3	Alto	Actor Nivel 1	Bajo
Uso en línea del registro electoral a nivel estatal	Disponibilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 2	Medio
Preparación del registro electoral a nivel jurisdiccional	Confiabilidad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación del registro electoral a nivel jurisdiccional	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación del registro electoral a nivel jurisdiccional	Disponibilidad	Media	Actor Nivel 3	Medio	Actor Nivel 2	Bajo
Preparación de la boleta/papeleta electoral a nivel estatal	Confiabilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 1	Bajo

COMPONENTE	TIPO DE ATAQUE	ESCALA DE ATAQUE	Control bajo HABILIDAD DEL ATACANTE	Control bajo CLASIFICACIÓN DE RIESGO	Control recomendado HABILIDAD DEL ATACANTE	Control recomendado CLASIFICACIÓN DE RIESGO
Preparación de la boleta/papeleta electoral a nivel estatal	Integridad	Alta	Actor Nivel 3	Alto	Actor Nivel 1	Bajo
Preparación de la boleta/papeleta electoral a nivel estatal	Disponibilidad	Alta	Actor Nivel 3	Alto	Actor Nivel 2	Medio
Preparación de la máquina de votación a nivel jurisdiccional	Confiabilidad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación de la máquina de votación a nivel jurisdiccional	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación de la máquina de votación a nivel jurisdiccional	Disponibilidad	Media	Actor Nivel 3	Medio	Actor Nivel 2	Bajo

COMPONENTE	TIPO DE ATAQUE	ESCALA DE ATAQUE	Control bajo DEL ATACANTE	Control bajo CLASIFICACIÓN DE RIESGO	Control recomendado HABILIDAD DEL ATACANTE	Control recomendado CLASIFICACIÓN DE RIESGO
Preparación de la máquina de votación a nivel estatal	Confiabilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación de la máquina de votación a nivel estatal	Integridad	Alta	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Preparación de la máquina de votación a nivel estatal	Disponibilidad	Alta	Actor Nivel 3	Alto	Actor Nivel 2	Bajo
Uso de las máquinas de votación	Confiabilidad	Baja	Actor Nivel 3	Alto	Actor Nivel 1	Bajo
Uso de las máquinas de votación	Integridad	Baja	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Uso de las máquinas de votación	Disponibilidad	Baja	Actor Nivel 3	Bajo	Actor Nivel 2	Bajo
Preparación de la tabulación	Confiabilidad	Media	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Preparación de la tabulación	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo

COMPONENTE	TIPO DE ATAQUE	ESCALA DE ATAQUE	Control bajo HABILIDAD DEL ATACANTE	Control bajo CLASIFICACIÓN DE RIESGO	Control recomendado HABILIDAD DEL ATACANTE	Control recomendado CLASIFICACIÓN DE RIESGO
Preparación de la tabulación	Disponibilidad	Media	Actor Nivel 3	Medio	Actor Nivel 2	Bajo
Tabulación a nivel de precinto	Confiabilidad	Baja	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Tabulación a nivel de precinto	Integridad	Baja	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Tabulación a nivel de precinto	Disponibilidad	Baja	Actor Nivel 3	Bajo	Actor Nivel 2	Bajo
Tabulación centralizada	Confiabilidad	Media	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Tabulación centralizada	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Tabulación centralizada	Disponibilidad	Media	Actor Nivel 3	Medio	Actor Nivel 2	Bajo
Agregación a nivel estatal	Confiabilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Agregación a nivel estatal	Integridad	Alta	Actor Nivel 3	Alto	Actor Nivel 1	Bajo

COMPONENTE	TIPO DE ATAQUE	ESCALA DE ATAQUE	Control bajo HABILIDAD DEL ATACANTE	Control bajo CLASIFICACIÓN DE RIESGO	Control recomendado HABILIDAD DEL ATACANTE	Control recomendado CLASIFICACIÓN DE RIESGO
Agregación a nivel estatal	Disponibilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 2	Medio
Sitio web a nivel jurisdiccional	Confiabilidad	Media	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Sitio web a nivel jurisdiccional	Integridad	Media	Actor Nivel 3	Medio	Actor Nivel 1	Bajo
Sitio web a nivel jurisdiccional	Disponibilidad	Media	Actor Nivel 3	Bajo	Actor Nivel 2	Bajo
Sitio web a nivel estatal	Confiabilidad	Alta	Actor Nivel 3	Bajo	Actor Nivel 1	Bajo
Sitio web a nivel estatal	Integridad	Alta	Actor Nivel 3	Alto	Actor Nivel 1	Bajo
Sitio web a nivel estatal	Disponibilidad	Alta	Actor Nivel 3	Medio	Actor Nivel 2	Bajo

TIPO DE ATAQUE
Confiabilidad: Robo de información
Integridad: Modificación de la información o de la funcionalidad de un sistema
Disponibilidad: la interrupción o la negación del uso del sistema

ESCALA DE ATAQUE
Baja: Afecta a un subconjunto de una jurisdicción
Media: Afecta a toda una jurisdicción
Alta: Afecta a todo un estado o a varias jurisdicciones

HABILIDAD DEL ATACANTE - CONTROLES BAJOS/RECOMENDADOS
Cada puntuación de la capacidad se determinó basándose en la dificultad relativa de un ataque al componente en el peor caso y el mejor caso de implementación de los controles de seguridad del sistema, e indica la capacidad técnica que necesita un actor amenazante para ejecutar un ataque potencialmente exitoso.

Actor nivel 1: Actores amenazantes con la capacidad más alta para poder descubrir nuevas vulnerabilidades ("días cero"), desarrollar aplicaciones y herramientas personalizadas, y combinar actividades en línea con operaciones físicas cercanas. Los actores de nivel 1 incluyen tanto grupos a nivel estatal y nacional, como a grupos subnacionales sofisticados.

Actor nivel 2: Actores amenazantes con mediana capacidad que, con suficiente tiempo, pueden explotar la mayoría de las vulnerabilidades cibernéticas y pueden crear aplicaciones y herramientas personalizadas. Los actores de nivel 2 se limitan en gran medida a realizar operaciones a través del internet, aunque también pueden explotar el acceso cercano (por ejemplo, la búsqueda de redes inalámbricas Wi-Fi o "*wardriving*") o las normas de seguridad débiles en medios extraíbles.

Actor nivel 3: Actores amenazantes menos sofisticados que dependen de herramientas cibernéticas disponibles para explotar vulnerabilidades conocidas. Los actores de nivel 3 no crean sus propias aplicaciones o herramientas, pero pueden encontrarlos en la *dark-web* o en conjuntos de herramientas existentes.

CALIFICACIÓN DE RIESGO - CONTROL BAJO/RECOMENDADO
Cada calificación de riesgo global se determinó tanto en el peor caso como en el mejor caso de implementación de los controles de seguridad del sistema. Las calificaciones se basan en medidas de capacidad cibernética agregada y en evaluaciones realizadas por un grupo especializado de funcionarios electorales y proveedores de tecnología.

El Centro Nacional de Gestión de Riesgos (NRMC, por sus siglas en inglés) de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés), es el centro de planificación, análisis y colaboración que trabaja en estrecha coordinación con la comunidad de infraestructuras críticas con el fin de Identificar; Analizar; Priorizar; y Manejar los riesgos más estratégicos a las Funciones Críticas Nacionales. Estas son funciones del gobierno y del sector privado tan vitales para los Estados Unidos que su interrupción, corrupción o disfunción podrían tener un impacto debilitante en la seguridad, la estabilidad económica nacional, la salud pública nacional o el bienestar, o cualquier combinación de las mismas. Para más información, póngase en contacto con Central@cisa.gov o visite https://www.cisa.gov/national-risk-management.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.

---

[1] RAND Corporation Homeland Security Operational Analysis Center, "Election System Risk Prioritization Report," August 2019, page 1.
[2] David C. Kimball and Brady Baybeck, "Are All Jurisdictions Equal? Size Disparity in Election Administration," Election Law Journal (Vol. 12, No. 2), 2013, pp.130-145.
[3] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 119.
[4] Ibid.
[5] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 122.
[6] National Conference of State Legislatures, "Online Voter Registration," October 25, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx. Accessed July 28, 2020.
[7] Report of the U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure,* page 22.
[8] Verified Voting Foundation, "Voting Equipment in the United States," 2019, https://www.verifiedvoting.org/resources/voting-equipment/. Accessed July 28, 2020.
[9] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 15.
[10] National Conference of State Legislatures, "Electronic Transmission of Ballots," September 5, 2019. https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx. Accessed July 28, 2020.
[11] Ibid.
[12] Associated Press, "2 Oregon counties offer vote-by-mobile to overseas voters," 2019, https://apnews.com/8ce0fbc400514f55839fa84fb364d7f4. Accessed July 28, 2020.