RIESGO DE VOTACIÓN POR CORREO: INFRASTRUCTURA Y PROCESO

RIESGO	CONTROLES DE COMPENSACIÓN
Todas las formas de votación, en este caso, el voto por correo, conllevan una serie de riesgos cibernéticos y de infraestructura.	Los riesgos del voto por correo pueden manejarse mediante diversas políticas, procedimientos y controles, que crean niveles de protección para defender el proceso de la manipulación.
La implementación de infraestructura y procesos de votación por correo dentro de un cronograma condensado también puede presentar un nuevo riesgo.	Los funcionarios electorales deben evaluar los riesgos de introducir una nueva infraestructura con los riesgos operativos asociados con hacerlo en un cronograma reducido antes de tomar una determinación. La planificación, la preparación, la capacitación y la redundancia generarán resiliencia.
Para la votación por correo, parte del riesgo bajo el control de los funcionarios electorales durante la votación en persona se traslada a entidades externas, como impresoras de boletas, instalaciones de procesamiento de correo y el Servicio Postal de los Estados Unidos.	Los socios del sector privado están implementando las mejores prácticas técnicas y de procedimiento y compartiendo información a través de EI-ISAC. USPS tiene un programa de correo electoral dedicado que incluye un sistema de código de barras de correo inteligente que permite el seguimiento de las boletas y la cadena de custodia.
Los ataques a la integridad de los datos y sistemas de registro de votantes representan un riesgo comparativamente mayor en un entorno de votación por correo en comparación con un entorno de votación en persona.	Muchas jurisdicciones tienen un proceso de corrección que permite a los votantes corregir un paquete de boletas rechazado. Un votante que no recibe una boleta por correo puede ir a un lugar de votación y votar con una boleta provisional.
El procesamiento entrante y saliente de las boletas enviadas por correo introduce infraestructura y tecnología adicionales, lo que aumenta la potencial escalabilidad de los ataques cibernéticos.	Los controles de compensación para infraestructura adicional son los mismos que para otras tecnologías e infraestructuras electorales, por lo que los funcionarios electorales deben centrarse en las mejores prácticas de manejo de riesgos cibernéticos para generar resiliencia en el proceso electoral general.
Los procesos de votación por correo entrante y la tabulación tardan más que el procesamiento en persona, lo que hace que la tabulación de los resultados se produzca más lentamente y resulte en más papeletas para tabular después de la noche de las elecciones.	Algunas jurisdicciones han implementado tecnología e infraestructura electoral para acelerar el proceso. Algunas jurisdicciones tienen legalmente la oportunidad de comenzar a procesar la solicitud de boletas y las boletas antes del día de las elecciones. Los funcionarios electorales, los medios de comunicación, los candidatos y las ONG están educando a los votantes y creando la expectativa de que tomará días, si no semanas, determinar el resultado de muchas contiendas.
El riesgo de desinformación para la infraestructura y los procesos de votación por correo es similar al de la votación en persona mientras se utiliza un contenido diferente. Los actores maliciosos pueden aprovechar la comprensión limitada con respecto a los procesos de votación por correo para engañar y confundir al público.	Los funcionarios electorales, los medios de comunicación, los candidatos y las ONG están educando a los votantes sobre el proceso de votación por correo. La Asociación Nacional de Secretarios de Estado lanzó #TrustedInfo2020 para destacar a los funcionarios electorales estatales y locales como fuentes confiables y verificadas de información electoral.