Este documento fue creado como parte de los productos del Grupo de Trabajo del Consejo de Coordinación Gubernamental de Infraestructura Electoral sobre Desinformación y Errores del Consejo de Coordinación del Subsector. Este documento está destinado a ser utilizado por los funcionarios electorales estatales, locales, tribales y territoriales, y otros en la industria como parte de una estrategia de respuesta más amplia a la información errónea, la desinformación y la informacion maliciosa (MDM). Los funcionarios electorales de SLTT deben consultar con sus oficiales legales y otros funcionarios necesarios en su jurisdicción antes de crear un programa de respuesta de MDM.

Información Errónea, Desinformación e Información Maliciosa

Guía de planificación y respuesta a incidentes para funcionarios electorales

DESCRIPCIÓN GENERAL

Los funcionarios electorales estatales, locales, tribales y territoriales (SLTT) pueden tomar pasos proactivos para prepararse y responder a las amenazas de información errónea, desinformación e información maliciosa (MDM). Esta guía está destinada a ayudar a los funcionarios electorales a comprender, prepararse y responder a las amenazas de MDM que pueden afectar la capacidad de realizar elecciones.

¿QUÉ ES MDM?

CISA define información errónea, la desinformación y la información maliciosa (MDM) como "actividades de información". Este tipo de contenido se denomina influencia nacional o extranjera según su origen.

La **información errónea** es falsa, pero no se crea ni se comparte con la intención de causar daño.
La **desinformación** se crea deliberadamente para engañar, dañar o manipular a una persona, grupo social, organización o país.
La **información maliciosa** se basa en hechos, pero se usa fuera de contexto para engañar, dañar o manipular.

Combinado con la falta de conocimiento público acerca de los procesos electorales, el panorama cambiante de la tecnología y las comunicaciones crea nuevos riesgos y vectores en evolución para la propagación de MDM.

Esto incluye información inexacta sobre el proceso electoral, rumores sin fundamento e informes de resultados incompletos o falsos.

¿DE DÓNDE VIENE MDM?

MDM puede originarse a partir de una variedad de fuentes a través de medios digitales, sociales y tradicionales, y surgen continuamente nuevos temas de MDM. Los actores extranjeros han utilizado MDM para dirigirse a los votantes estadounidenses durante décadas. MDM también puede tener su origen en fuentes internas con el objetivo de sembrar divisiones y reducir la cohesión nacional. Los actores nacionales y extranjeros pueden usar campañas de MDM para causar ansiedad, miedo y confusión. En última instancia, estos actores buscan interferir y socavar nuestras instituciones democráticas.

Incluso MDM que no está directamente relacionado con las elecciones puede tener un impacto en el proceso electoral, reduciendo la confianza de los votantes.
El MDM relacionado con la infraestructura electoral ocurre todo el año; **no es solo una preocupación en los meses previos al día de las elecciones.**
Las narrativas falsas erosionan la confianza y representan una amenaza para las transiciones democráticas, especialmente, entre otras, las narrativas sobre los procesos electorales y la validez de los resultados electorales.

Definiciones adaptadas de la MDM Resource Library. Para obtener una descripción general de las tácticas utilizadas por las campañas de desinformación, como la manipulación de audio y videos, la realización de falsificaciones y el desarrollo de sitios web proxy para socavar la confianza del público y sembrar confusión, consulte Tools of Disinformation: Inauthentic Content.

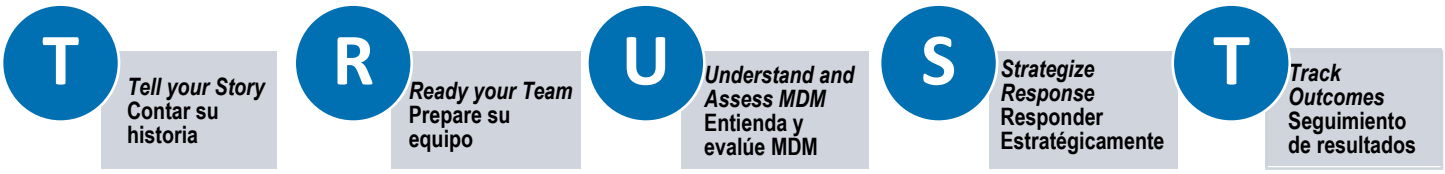
¿CÓMO IMPACTA MDM LA SEGURIDAD DE LAS ELECCIONES?

Dependiendo de la narrativa, MDM puede tener varios impactos en la seguridad electoral. Las categorías pueden incluir:

Impacto	Descripción	Ejemplo (Página CISA Control de rumores)
Interferencia en procedimiento	Narrativas o contenido relacionado con los procedimientos electorales que causan confusión e interfieren con la capacidad de los funcionarios para administrar una elección sin problemas.	✓ Realidad: Existen salvaguardas para evitar que se cuenten las boletas enviadas por correo impresas en casa o fotocopiadas. ✗ Rumor: un actor malicioso puede defraudar fácilmente una elección imprimiendo y enviando boletas adicionales por correo.
Interferencia en participación	Contenido que pueda intimidar o disuadir a los votantes de participar en el proceso electoral.	✓ Realidad: Las leyes estatales y federales protegen a los votantes de las amenazas o la intimidación en las urnas, incluso de parte de los observadores electorales. ✗ Rumor: Se permite que los observadores en el lugar de votación intimiden a los votantes, hagan campaña e interfieran con la votación.
Deslegitimación de resultados electorales	Narrativas o contenidos que deslegitiman resultados electorales o siembran desconfianza en la integridad del proceso basados en afirmaciones falsas o engañosas.	✓ Realidad: La información sobre los resultados de las elecciones puede ocurrir más lentamente de lo que esperan algunos votantes. Esto por sí solo no indica un problema con el proceso de conteo o los resultados, o que haya problemas que afecten la integridad de la elección. Los resultados oficiales no se certifican hasta que se hayan contado todas las papeletas válidamente emitidas, incluidas las papeletas que se han contado legalmente después de la noche de las elecciones. ✗ Rumor: si los resultados informados en la noche de las elecciones cambian en los días o semanas siguientes, el proceso está pirateado o comprometido, por lo que no puedo confiar en los resultados.
Personal de Seguridad	Narrativas o contenido que afirma falsamente que los funcionarios electorales o los trabajadores electorales son el "mal actor" que intenta interferir en los resultados o procesos electorales.	✓ Realidad: Sólidas salvaguardas que incluyen procedimientos de escrutinio y auditoría ayudan a garantizar la precisión de los resultados oficiales de las elecciones. ✗ Rumor: un mal actor podría cambiar los resultados de las elecciones sin ser detectado.

RESPONDING TO MDM

En el entorno actual de medios e información, los funcionarios electorales deben desempeñar un papel proactivo para responder a MDM. Si bien cada narrativa de MDM será diferente, aprovechar la CONFIANZA (TRUST en inglés) El modelo para la respuesta de MDM puede ayudar a reducir el riesgo y proteger a los votantes.



Es importante reconocer las oportunidades y limitaciones de la intervención de MDM liderada por el gobierno, particularmente donde la desconfianza en el gobierno puede estar alimentando la narrativa. Concentre las respuestas donde su equipo tenga evidencia, experiencia o autoridad para contrarrestar el MDM. Además, reclute socios comunitarios confiables para amplificar sus mensajes.

Categorías adaptadas del informe final del Proyecto de Integridad Electoral (EIP) reportfinal sobre información errónea y las elecciones de 2020 (revisado en marzo de 2021).

1. CONTAR TU HISTORIA

La resiliencia pública aumenta a medida que su equipo construye relaciones con los votantes y las partes interesadas. Informe a sus comunidades sobre los procesos electorales y las amenazas relacionadas con MDM antes de que ocurran.

Educar a los votantes: Educar a los electores sobre cómo participar en el proceso electoral y promover el aprendizaje cívico es fundamental para contrarrestar el MDM. **Comunicarse con claridad en el tono, el idioma y el medio, así como aprovechar las voces creíbles en las que confía su audiencia** ayudará a llegar e involucrar a los electores para transmitir información sobre fechas/fechas límite importantes, lugares de votación, procesos para cambiar la votación y dónde encontrar información confiable sobre las elecciones. y resultados electorales. Pre-bunk MDM: Brindar a los electores información y recursos antes de que surja la actividad de MDM prepara mejor a los estadounidenses para identificar y cuestionar narrativas falsas. En algunos casos, al aprovechar los conocimientos de su personal, puede anticipar dónde pueden surgir narrativas de MDM, por ejemplo, cómo los funcionarios electorales aseguran las elecciones mediante el uso de auditorías posteriores a las elecciones y salvaguardas similares. Abordar estos temas con los votantes antes de las elecciones y explicar cómo se utilizan en las narrativas de MDM puede aumentar la resiliencia y la confianza entre los votantes.

La alfabetización mediática incluye la verificación de fuentes, la búsqueda de puntos de vista alternativos y la búsqueda de fuentes de información confiables. La Asociación Nacional para la Educación en Alfabetización en Medios tiene miembros en todos los estados que pueden trabajar con funcionarios electorales para desarrollar contenido de alfabetización en medios. Las novelas gráficas de la serie Resiliencia de CISA son un gran ejemplo de un recurso destinado a desarrollar la alfabetización mediática y el pensamiento crítico para contrarrestar la desinformación.

Pre-bunk MDM: Brindar a los electores información y recursos antes de que surja la actividad de MDM prepara mejor a los estadounidenses para identificar y cuestionar narrativas falsas. En algunos casos, al aprovechar los conocimientos de su personal, **puede anticipar dónde pueden surgir narrativas de MDM,** por ejemplo, cómo los funcionarios electorales aseguran las elecciones mediante el uso de auditorías posteriores a las elecciones y salvaguardas similares. Abordar estos temas con los votantes antes de las elecciones y explicar cómo se utilizan en las narrativas de **MDM** puede aumentar la resiliencia y la confianza entre los votantes.

Establezca relaciones con los medios: Comuníquese con periódicos locales, radio, televisión, podcasts y otros medios de comunicación para **establecer relaciones de trabajo antes de los ciclos electorales.** Invítelos a obtener más información sobre cómo los procesos electorales aseguran los resultados electorales y detalles clave de educación electoral. Asegúrese de que tengan un contacto en su oficina. Establecer relaciones de trabajo con medios de comunicación y periodistas ayuda a desacreditar o exponer de forma rápida y preventiva la actividad de MDM. También puede ayudar a informar informes precisos sobre las elecciones, lo que limita la propagación de información.

2. PREPARA TU EQUIPO

La efectividad de su respuesta dependerá de cuánta preparación se lleve a cabo internamente antes de la actividad de MDM.
Establece tu protocolo de respuesta: Establecer un procedimiento claro para responder a MDM y educar a los miembros del equipo sobre el proceso.

- Comprenda los procedimientos para informar o marcar posibles MDM en línea en las plataformas de redes sociales que suelen utilizar sus electores. Consulte con su asesor legal para asegurarse de respetar los derechos constitucionales y las protecciones de privacidad y cumplir con las restricciones legales.
- El Centro para la Seguridad en Internet (CIS) se estableció para respaldar las necesidades de seguridad cibernética del subsector electoral. El CIS se puede aprovechar para informar MDM en tiempo real por correo electrónico a misinformation@cisecurity.org. Asegúrese de incluir enlaces y capturas de pantalla, así como detalles sobre la información errónea y su jurisdicción.
- Determine las funciones y responsabilidades internas, incluido un proceso de escalamiento dentro de su jurisdicción para garantizar que los equipos correctos se comunican entre sí mientras responden a la actividad de MDM. Tenga claro que esto no es “solo” un problema de comunicación; requiere la participación de todos los departamentos para garantizar que las respuestas sean precisas y comprensibles.
- Designe a una persona para que sea responsable de garantizar que este proceso se establezca, actualice y comparta tanto internamente como con las partes interesadas relevantes a nivel local, estatal, tribal, territorial y federal, incluyendo su Oficina Regional CISA.
- Realice o participe en ejercicios de simulación para aumentar la conciencia y la comprensión de su equipo sobre las amenazas de MDM, evalúe su preparación general, identifique deficiencias en su plan de respuesta a incidentes y aclare roles y responsabilidades durante un incidente. CISA puede asistir en el desarrollo y ejecución de estos ejercicios, o el recurso CISA de Tabletop in abox ambién puede ayudarlo a hablar sobre posibles escenarios con su equipo y las partes interesadas.

Cree canales creíbles para compartir información: El MDM puede prosperar en la ausencia de información creíble y de fácil acceso. Asegúrese de que el sitio web de su agencia, las cuentas de redes sociales y otros canales de información estén actualizados y activos para que pueda responder directamente a MDM. Esto puede ayudar a su comunidad a tener confianza en que los mensajes que sus organizaciones difunden tienen autoridad y puede generar aún más confianza pública en la administración electoral.

- Registre su sitio web con una dirección .gov para que el público no tenga que adivinar si sus sitios web y correos electrónicos son genuinos. CISA hace que los dominios .gov estén disponibles únicamente para organizaciones gubernamentales con sede en los EE. UU. y entidades controladas públicamente **sin costo alguno.**

- Muchas plataformas sociales (p. ej., Facebook, Twitter) también permitirán que las organizaciones gubernamentales y los usuarios soliciten insignias de verificación. Los funcionarios electorales locales deben comunicarse con su estado para obtener más información sobre cómo verificar sus cuentas.

- Considere preinstalar MDM en su sitio web respondiendo preguntas comunes relevantes para sus responsabilidades. La Guía de puesta en marcha de Rumor Control brinda más orientación sobre cómo establecer esta página web y cómo evaluar qué temas incluir.

Prepárese para las preguntas: Asegúrese de que su oficina tenga métodos para responder a las preguntas y comentarios del público, incluida **la capacidad de manejar una gran afluencia de llamadas o mensajes.** Considere crear una bandeja de entrada de correo de voz y correo electrónico compartida para que ninguna persona se sienta abrumada, con un registro para rastrear consultas y respuestas. Estos buzones deben revisarse regularmente y debe haber un proceso establecido para determinar quién responderá. Esto permitirá que su equipo descubra el MDM que está circulando y mantenga los sistemas y las líneas telefónicas en funcionamiento durante los períodos críticos de actividad de MDM. Asegúrese de que el personal esté al tanto de los procedimientos de su oficina para denunciar amenazas y acoso y, si es posible, alterne las responsabilidades para responder a llamadas y correos electrónicos para evitar el agotamiento.

Listado del equipo

- ✓ **Comprender los mecanismos de denuncia para marcar MDM en las redes sociales.**
- ✓ **Determinar roles y responsabilidades para la respuesta de MDM.**
- ✓ **Designe a una persona para que supervise el proceso de respuesta de MDM.**
- ✓ **Registre su sitio web para una dirección .gov.**
- ✓ **Solicite insignias de verificación de las plataformas de redes sociales.**
- ✓ **Desarrolle una lista de temas y preguntas comunes vulnerables a MDM.**
- ✓ **Asegúrese de que sus sistemas de comunicación estén configurados para manejar las preguntas entrantes.**
- ✓ **Comprometerse con un abogado y, si corresponde, con su oficina de privacidad para garantizar la protección de los derechos constitucionales y la privacidad.**

3. COMPRENDER Y EVALUAR

Es importante comprender, en la medida de sus posibilidades, la naturaleza completa y el alcance de la actividad de MDM.

Identificar la actividad de MDM: Si bien cada jurisdicción electoral tiene diferentes recursos y capacidades, debe establecer un sistema para identificar y evaluar MDM en su oficina. Determine si es apropiado que su oficina se comprometa con organizaciones o herramientas externas para comprender mejor el panorama de riesgos y monitorear MDM, incluido su proveedor de sistemas técnicos. El monitoreo puede ser proactivo, a través de herramientas analíticas, o reactivo, a través de canales de retroalimentación pública.

- **Identificar y actualizar continuamente una lista de procesos clave relacionados con las elecciones y problemas vulnerables a MDM**, ya sean tendencias a corto plazo o narrativas a largo plazo. Asegúrese de que todos los miembros de su oficina tengan acceso a esta lista y se sientan cómodos contribuyendo a ella. Por lo tanto, la persona que responde a las consultas tendrá una buena idea de los temas sobre los que pregunta la gente y a quién contactar para obtener respuestas, incluso si no saben cómo responder a la pregunta por sí mismos.

- **Identificar los canales que utilizan los electores para recibir información**. El contenido de MDM se puede difundir a través de numerosos medios, incluidas las redes sociales, los principales medios de comunicación, el boca a boca, los foros en línea, las aplicaciones de mensajería y los correos electrónicos. Recuerde que las narrativas de MDM también suelen moverse entre canales, por lo que el contenido que aparece en una plataforma también puede surgir en otra.

- Para los temas de alta prioridad en su lista, incluidos aquellos en los que trabajó para preparar la litera, es posible que **desee adoptar un enfoque más proactivo para monitorear las narrativas de MDM, en la medida permitida por la ley.** Considere el uso de herramientas analíticas para buscar palabras clave relacionadas con el contenido de MDM. Evalúe el alcance del contenido (cuántas personas lo ven), el compromiso (a cuántas personas les gusta, lo comparten o reaccionan al contenido), en cuántos canales está presente y si ha llegado a los medios principales. Consulte con su asesor legal para determinar qué monitoreo está permitido según la ley y los términos de servicio de las plataformas.

Evaluar el riesgo: El equipo debe identificar qué riesgos plausibles están asociados con las narrativas de MDM y cómo pueden afectar la infraestructura electoral. Mapear las narrativas de MDM existentes y su impacto en la infraestructura electoral ayudará al equipo a estar preparado para las consecuencias en línea y fuera de línea y el impacto en la infraestructura electoral.

4. ESTRATEGIA DE RESPUESTA

Una vez que haya identificado MDM, es importante elaborar una respuesta eficaz, teniendo en cuenta cómo puede evolucionar el entorno de la información y la tecnología relacionada.

Determina tu respuesta: En función de su evaluación de riesgos, priorice a qué narrativas de MDM responder. Al diseñar su estrategia de comunicación, considere tanto el tiempo como el medio de respuesta.

- **No toda la actividad de MDM garantiza una respuesta inmediata.** Decidir qué rumores hacen el corte es un ejercicio de juicio de una organización, y ese juicio puede cambiar a medida que evolucionan las narrativas de MDM y cambia la respuesta de la comunidad.

- **Comprenda a su audiencia** para la intervención de **MDM**. Su comunidad no es homogénea y su audiencia cambiará según el mensaje que intente transmitir y el medio que utilice. Adapte sus mensajes a las audiencias a las que intenta llegar, como nuevos votantes, veteranos, personas en regiones geográficas específicas o aquellos que hablan otros idiomas.

Los funcionarios electorales de todo el país están combatiendo el MDM en las elecciones.

- La oficina del Secretario de Estado de Colorado llevó a cabo actividades de divulgación digital y en las redes sociales para los votantes y creó un sitio web para educar sobre la información errónea sobre amenazas y responder a las narrativas de MDM.
- La oficina del Secretario de Estado de Kentucky lanzó una página de control de rumores en su sitio web para contrarrestar las narrativas de MDM sobre las elecciones.
- La Comisión Electoral de Wisconsin estableció una página de preguntas frecuentes para responder las preguntas de los votantes sobre las elecciones de 2020.
- El Departamento de Elecciones del condado de Maricopa, Arizona, lanzó un sitio web para abordar preguntas y conceptos erróneos sobre las elecciones de 2020 y se ha involucrado en esfuerzos de control de rumores en las redes sociales.

Aplicar las mejores prácticas de comunicación: En una crisis, las tácticas y el lenguaje específicos pueden ayudar a construir la credibilidad de su respuesta y tranquilizar a los votantes. Las tácticas también pueden verse diferentes según la actividad y la audiencia. Una estrategia de comunicación podría incluir **redes sociales, radio, noticias locales u otras plataformas de medios** para involucrar a los electores.

- Identifique dónde recibe información su audiencia y, si es posible y conveniente, establezca presencia en estas plataformas. Es probable que no sea realista que su oficina utilice activamente todas las plataformas. Concéntrese en usar una cantidad menor de plataformas de manera efectiva para establecer su identificador como una fuente confiable de información.
- Asegúrese de tener los hechos antes de responder.
- Indique los hechos primero, en lugar de repetir una falsedad en su titular.
- Tenga cuidado de no amplificar la fuente del MDM al vincularlo directamente o compartir imágenes o videos originales. Si hace referencia a una imagen, use una captura de pantalla con una superposición de texto que explique que la imagen no es auténtica o es engañosa. Considere qué protecciones de privacidad son necesarias para todos los medios compartidos.
- Considere la longitud de su respuesta. Las declaraciones más cortas son más fáciles de digerir y pueden ser útiles cuando el MDM se refuta fácilmente.
- No es necesario que responda a cada incidente de MDM individualmente. Señale las publicaciones, declaraciones o trabajos anteriores de su oficina si MDM recircula. Los mensajes inconsistentes pueden crear problemas de credibilidad.
- Aproveche las asociaciones y los mensajeros comunitarios confiables para contrarrestar las narrativas de MDM. **La repetición y consistencia son la clave.** Transmitir el mismo mensaje a través de múltiples medios y plataformas ayudará a llegar a la audiencia más amplia posible.

5. SEGUIMIENTO DE LOS RESULTADOS

Después de su respuesta, evalúe la prevalencia continua de MDM y evalúe formas de ajustar los procesos en el futuro.

Administrar y monitorear las repercusiones: Si bien las narrativas de MDM pueden abordarse de manera efectiva o las cuentas que difunden desinformación pueden eliminarse, los manipuladores a menudo encontrarán formas de eludir estos cambios. La creación de nuevas cuentas, la adaptación del lenguaje codificado, la alteración del material audiovisual y la iteración de narraciones ya identificadas como objetables por las plataformas son todos los ajustes posibles implementados para aumentar la eficacia de MDM. Es importante monitorear el entorno de MDM, según lo permitan los recursos, para estar al tanto de los cambios y ajustar las tácticas de respuesta en consecuencia.

Reevaluar la estrategia de respuesta: Después de un esfuerzo de respuesta de MDM, revise y reevalúe su proceso, incluida su lista de temas prioritarios para el monitoreo de los medios. En el entorno de información actual, las amenazas están en constante evolución y las ubicaciones, los medios y las narrativas de MDM también están cambiando.