
**Plan de respuesta a incidentes**

**Propietario de la política: VICTOR ACOSTA LOPEZ**

**Fecha de entrada en vigencia: 09/09/20**

**Objetivo**

Este documento establece el plan para administrar incidentes y eventos de seguridad de la información, y ofrece orientación para empleados o equipos de respuesta a incidentes que creen que han descubierto o respondido a un incidente de seguridad.

**Alcance**

Esta política cubre todos los eventos o incidentes de seguridad de la información o privacidad de datos.

**Definiciones de incidentes y eventos**

Un evento de seguridad es una ocurrencia observable relevante para la confidencialidad, disponibilidad, integridad o privacidad de los datos, sistemas o redes controlados por la empresa.

Un incidente de seguridad es un evento de seguridad que resulta en pérdida o daño a la confidencialidad, disponibilidad, integridad o privacidad de los datos, sistemas o redes controlados por la empresa.

**Informes y documentación de incidentes**

**Informes**

Si un empleado, contratista, usuario o cliente de D3M3NT SA DE CV se da cuenta de un incidente o evento de seguridad de la información, posible incidente, incidente inminente, acceso no autorizado, infracción de políticas, vulnerabilidad de seguridad o actividad sospechosa, deberá informar de inmediato la información mediante uno de los siguientes canales de comunicación:

- Enviar un correo electrónico a seguridad@dmente.mx información o informes sobre el suceso o incidente

Los periodistas deben actuar como un buen testigo y comportarse como si estuvieran denunciando un delito. Los informes deben incluir detalles específicos sobre lo que se ha observado o descubierto.

**Severidad**

el equipo de soporte de D3M3NT SA DE CV supervisará los *tickets* de incidentes y eventos y asignará una gravedad de *ticket* en función de las siguientes categorías.

**S3/S4: Gravedad baja y media**

Los problemas que alcanzan esta gravedad son simplemente sospechas o comportamientos extraños. No están verificadas y requieren más investigación. No hay un indicador claro de que los sistemas tengan un riesgo tangible y no requieren una respuesta de emergencia. Esto incluye la pérdida o robo de una computadora portátil con encriptación de disco, correos electrónicos sospechosos, cortes de energía, actividad extraña en una computadora portátil, entre otros.

**S2: Gravedad alta**

Los problemas de gravedad alta se relacionan con problemas en los que aún no se ha probado un adversario o una explotación activa, y puede que no haya ocurrido, pero es probable que suceda. Esto puede incluir una computadora portátil perdida o robada sin encriptación, vulnerabilidades con riesgo directo de explotación, amenazas con riesgo o persistencia adversaria en nuestros sistemas (p. ej.: puertas traseras, *malware*), acceso malicioso a datos comerciales (p. ej.: contraseñas, datos de vulnerabilidad, información de pagos).

**S1: Gravedad crítica**

Los temas críticos se relacionan con riesgos vulnerados activamente e involucran a un actor malintencionado o amenazas que ponen a cualquier individuo en riesgo de sufrir daño físico. Se requiere la identificación de la explotación activa para cumplir con esta categoría de gravedad.

**Escalamiento e informes internos**

Los contactos de escalamiento de incidentes se encuentran a continuación en el Apéndice A.

*S1. Gravedad crítica:* los problemas de gravedad S1 requieren notificación inmediata a la gerencia de TI y también se debe notificar al administrador correspondiente (consulte S1 arriba) a través del correo electrónico con una referencia al número de ticket.

*S3/S4. Gravedad media y baja*: se debe crear un *ticket* de soporte con el tipo s3 o s4 y asignarlo al departamento correspondiente para su respuesta.

**Documentación**

Todos los eventos de seguridad, incidentes y actividades de respuesta informados se documentarán y se protegerán adecuadamente en <describe dónde se documentará, por ejemplo, el sistema de *tickets* ServiceDesk o Salesforce>.

Se podrá realizar un análisis de la causa raíz en todos los incidentes de seguridad verificados de S1 . Se documentará un informe de análisis de causa raíz y se hará referencia al mismo en el ticket del incidente. Dicho análisis será revisado por el <revisor del análisis de la causa raíz, por ejemplo, el vicepresidente de soporte, el vicepresidente de ingeniería o el director de TI, quien determinará si se convocará una reunión a posteriori.

**Proceso de respuesta a incidentes**

En el caso de que haya problemas críticos, el equipo de respuesta seguirá un proceso de respuesta iterativa diseñado para investigar, contener la vulnerabilidad, erradicar la amenaza, recuperar el sistema y los servicios, solucionar vulnerabilidades y documentar un análisis retrospectivo con las lecciones de un incidente.

**Resumen**

- Evento notificado
- Triaje y análisis
- Investigación
- Contención y neutralización (corto plazo/triaje)
- Recuperación y reparación de vulnerabilidades
- Mejoras en el desarrollo y la detección (lecciones aprendidas, respuesta a largo plazo)

**Detallado**

- El gerente de TI o vicepresidente de soporte administrará el esfuerzo de respuesta a incidentes
- Si es necesario, se designará una"Sala de Guerra" central, que puede ser una ubicación física o virtual (es decir, canal de Slack)
- Se celebrará una reunión periódica de respuesta ante incidentes a intervalos regulares hasta que se resuelva el incidente.
- Se informará al personal jurídico y ejecutivo como se requiera

**Agenda de la reunión de respuesta a incidentes**

- Actualizar el *ticket* del incidente y los plazos
- Documentar nuevos indicadores de compromiso (OCI)
- Realizar preguntas y respuestas de investigación
- Aplicar mitigaciones de emergencia
- Informes externos / Informes de violaciones
- Planificar mitigaciones a largo plazo
- Documentar análisis de causa raíz (RCA)

- Elementos adicionales según sea necesario

**Consideraciones especiales**

**Problemas internos**

Los problemas en los que el actor malicioso es un empleado interno, contratista, proveedor o socio requiere un manejo sensible. El gerente de incidentes se pondrá en contacto directamente con la junta directiva y no lo debatirá con otros empleados. Estos son problemas críticos en los que se debe realizar un seguimiento.

**Comunicaciones comprometidas**

Los equipos de respuesta a incidentes deben tener método de comunicación oficial y organizados antes de anunciarse como miembros del incidente. Si hay riesgos de comunicación de TI, se elegirá una solución en privado y se comunicará a los equipos de respuesta a incidentes a través de cómo se comunicarán los cambios en la comunicación si es necesario, por teléfono celular.

**Vulnerabilidad de la cuenta raíz**

Si se conoce o se espera una vulnerabilidad de la cuenta raíz de AWS, consulte el manual del Apéndice D.

**Requisitos adicionales**

- Los eventos e incidentes sospechosos y reportados deben documentarse.
- Los incidentes sospechosos se evaluarán y clasificarán como un suceso o un incidente.
- La respuesta a incidentes se realizará de acuerdo con este plan y cualquier procedimiento asociado.
- Todos los incidentes se documentarán formalmente y se realizará un análisis de causa raíz documentado.
- Los equipos de respuesta ante incidentes deben recopilar, almacenar y preservar las pruebas relacionadas con incidentes de conformidad con los lineamientos de la industria y las prácticas recomendadas como NIST SP 800-86 "Guía para integrar técnicas forenses en la respuesta ante incidentes"
- Los eventos sospechosos y confirmados de acceso no autorizado serán revisados por el Equipo de Respuesta ante Incidentes. Las determinaciones de la violación solo serán realizadas por Gerente TI y junta directiva
- D3M3NT SA DE CV deberá notificar de inmediato y de forma adecuada a los clientes, socios, usuarios, partes afectadas y agencias reguladoras sobre incidentes o violaciones relevantes de conformidad con las políticas, obligaciones contractuales y requisitos regulatorios de D3M3NT SA DE CV, según lo determine el Junta directiva y el área legal.
- Este Plan de Respuesta ante Incidentes se revisará y formalmente se evaluará, al menos, anualmente. Los resultados de las actividades de prueba del Plan de Respuesta ante Incidentes, incluidos los hallazgos y las lecciones aprendidas, se documentarán formalmente y se mantendrán para respaldar los requisitos de seguridad, cumplimiento y auditoría.

**Comunicaciones externas y reportes de infracciones**

El personal legal y ejecutivo deberá consultar a los equipos técnicos en el caso de acceso no autorizado a los sistemas, redes o datos de la empresa o del cliente. El personal legal junto con el CEO determinará si se requieren informes de violaciones o comunicaciones externas. Las violaciones se informarán a los clientes, consumidores, interesados y reguladores sin retrasos indebidos y de conformidad con todas las obligaciones contractuales y la legislación aplicable.

Ningún miembro del personal puede divulgar información sobre incidentes o posibles infracciones a terceros o personas no autorizadas sin la aprobación de la gerencia legal o ejecutiva.

**Mitigación y remediación**

El personal jurídico y ejecutivo determinará las medidas de mitigación o corrección inmediatas o a largo plazo que deban adoptarse como consecuencia de un incidente o una violación. En el caso de que se necesiten mitigaciones o medidas correctivas, el personal ejecutivo deberá dirigir al personal con respecto a la planificación, comunicación y ejecución de dichas actividades.

**Cooperación con clientes, controlador de datos y autoridades**

Según sea necesario y determinado por el personal legal y ejecutivo, la empresa cooperará con clientes, Controladores de Datos y reguladores para cumplir con todas sus obligaciones en caso de un incidente o una violación de datos.

**Funciones y responsabilidades**

Cada empleado y usuario de cualquier recurso de información de D3M3NT SA DE CV tiene responsabilidades con respecto a la protección de los recursos de información. La siguiente tabla establece las responsabilidades específicas de las funciones de respuesta ante incidentes.

**Miembros del equipo de respuesta**

| Función | Responsabilidad |
|---|---|
| GERENTE DE TI | El Gestor de Incidentes es el responsable de la toma de decisiones principal y final durante el período de respuesta. El Gestor de Incidentes es, en última instancia, responsable de resolver el incidente y de cerrar formalmente las medidas de respuesta ante incidentes. Consulte el Apéndice A para obtener información de contacto del Gestor de Incidentes.<br><br>Estas responsabilidades incluyen:<br><br>• Garantizar que las personas adecuadas de todas las funciones participen activamente, según corresponda<br>• Comunicar actualizaciones de estado a la persona o los equipos adecuados a intervalos regulares<br>• Resolución de incidentes en el plazo inmediato<br>• Determinar las medidas de seguimiento necesarias<br>• Asignar actividades de seguimiento a las personas adecuadas<br>• Informar de inmediato los detalles del incidente que pueden desencadenar el informe de violación, por escrito a la GERENTE DE TI |
| GERENTE DE TI | Las personas que se han comprometido y están trabajando activamente en el incidente. Todos los miembros del IRT permanecerán comprometidos en la respuesta a incidentes hasta que el incidente se resuelva formalmente, o sean formalmente liberados de la obligación por el gestor de incidentes. |
| GERENTE DE TI | Los ingenieros calificados se colocarán en la rotación de guardia y pueden actuar como gestor de incidentes (si los recursos primarios no están disponibles) o como un miembro del IRT cuando se comprometan a responder a un incidente. Los ingenieros son responsables de comprender las tecnologías y los componentes de los sistemas de información, los controles de seguridad implementados, incluidas las herramientas de registro, monitoreo y alerta, los canales de comunicación apropiados, los protocolos de respuesta ante incidentes, los procedimientos de escalamiento y los requisitos de |

| | |
|---|---|
| | documentación. Cuando los ingenieros participan en la respuesta ante incidentes, se convierten en miembros del IRT. |
| **Usuarios** | Los empleados y contratistas de D3M3NT SA DE CV. Los usuarios son responsables de seguir las políticas, informar de problemas, sospechas de problemas, debilidades, actividades sospechosas e incidentes y eventos de seguridad. |
| **Clientes** | Los clientes son responsables de reportar problemas con el uso de los servicios de D3M3NT SA DE CV. Los clientes son responsables de verificar que se resuelvan los problemas reportados. |
| **Asesor legal** | Responsable, junto con el CEO y la gerencia ejecutiva, de determinar si un incidente presenta exposición legal o regulatoria, así como de si un incidente se considerará una violación denunciable. El asesor legal deberá revisar y aprobar por escrito todas las notificaciones de violación externas antes de que se envíen a cualquier parte externa. |
| **Dirección ejecutiva** | Responsable, en conjunto con el director general y asesor legal, de determinar si un incidente se considerará incumplimiento denunciable. Un funcionario de la empresa correspondiente revisará y aprobará por escrito todos los avisos de incumplimiento externo antes de que se envíen a cualquier parte externa.<br><br>D3M3NT SA DE CV buscará consenso de las partes interesadas al determinar si se ha producido una infracción. El CEO de D3M3NT SA DE CV tomará una determinación final de la infracción en caso de que no se pueda alcanzar ese consenso. |

**Compromiso de la gerencia**

La gerencia de D3M3NT SA DE CV ha aprobado esta política y se compromete a proporcionar los recursos, las herramientas y la capacitación necesarios para responder razonablemente a los eventos e incidentes de seguridad identificados con el potencial de afectar negativamente a la empresa o a sus clientes.

**Excepciones**

Las solicitudes de excepción a esta Política deben ser presentadas y autorizadas por el GERENTE DE TI para su aprobación. Se documentarán las excepciones.

**Infracciones y cumplimiento**

Cualquier infracción conocida de esta política debe ser reportada a los GERENTE DE TI Y/O OFICIAL DE CUMPLIMIENTO. Las infracciones de esta política pueden dar lugar al retiro o suspensión inmediata de los privilegios del sistema y la red o medidas disciplinarias de acuerdo con los procedimientos de la empresa, incluido el despido.

| Versión | Fecha | Descripción | Autor | Aprobado por |
|---|---|---|---|---|
| 1.1 | 09/04/2024 | AJUSTES POR TRADUCCION | VICTOR ACOSTA | MARCO VILLANUEVA |
| | | | | |

**Apéndice A. Información de contacto**

Los contactos para la gestión de TI e ingeniería, así como para el personal ejecutivo, se pueden encontrar en la siguiente liga https://intra.dmente.mx/

**Apéndice B. Formulario de recopilación de incidentes**

| | | | | |
|---|---|---|---|---|
| **Información general** | | | | |
| **Información del detector de incidentes** | | | | |
| **Nombre:** | | | **Fecha y hora detectada:** | |

| | | | | |
|---|---|---|---|---|
| **Título:** | | | | |
| **Teléfono:** | | | **Incidente de ubicación detectado desde:** | |
| **Correo electrónico:** | | | | |
| | | | **Información adicional:** | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| **Resumen del incidente** | | | | |
| **Tipo de incidente detectado:** | | | | |
| Denegación de servicio | Uso no autorizado | Espionaje | Investigación | Engaño |
| Código malicioso | Acceso no autorizado | Otros: | | |
| | | | | |
| **Ubicación del incidente:** | | | | |
| **Sitio:** | | | | |
| **Punto de contacto del sitio:** | | | | |
| **Teléfono:** | | | | |
| **Correo electrónico:** | | | | |
| | | | | |
| **Cómo se detectó el incidente**: | | | | |
| | | | | |
| **Información adicional:** | | | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| **Ubicación de los sistemas afectados:** | | | | |
| | | | | |
| **Fecha y hora de llegada de los responsables del incidente al lugar:** | | | | |
| | | | | |
| **Describir sistemas de información afectados (se recomienda un formulario por sistema):** | | | | |
| **Fabricante de *hardware*:** | | | | |
| **Número de serie:** | | | | |
| **Número de propiedad corporativa (si corresponde):** | | | | |
| | | | | |
| **¿El sistema afectado está conectado a una red?** | Sí | No | | |
| | | | | |
| **Describa la seguridad física de la ubicación de los sistemas de información afectados (bloqueos, alarmas de seguridad, acceso al edificio, entre otros):** | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Aislar los sistemas afectados:** | | | | |
| **¿Aprobación para eliminar de la red?** | Sí | No | | |
| **Si la respuesta es SÍ, nombre del aprobador:** | | | | |
| Fecha y hora de eliminación: | | | | |
| Si la respuesta es NO, indique el motivo: | | | | |
| | | | | |
| | | | | |
| **Copia de seguridad de los sistemas afectados:** | | | | |

| | | | | |
|---|---|---|---|---|
| **¿La última copia de seguridad del sistema se realizó correctamente?** | Sí | No | | |
| **Nombre de las personas que hicieron una copia de seguridad:** | | | | |
| | | | | |
| **Fecha y hora en que se iniciaron las últimas copias de seguridad:** | | | | |
| **Fecha y hora de las últimas copias de seguridad completadas:** | | | | |
| **Ubicación del almacenamiento de las copias de seguridad:** | | | | |
| | | | | |
| **Erradicación de incidentes:** | | | | |
| **Nombre de las personas que realizan análisis forenses:** | | | | |
| **Se identificó la vulnerabilidad (causa raíz):** | Sí | No | | |
| **Describir:** | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Cómo se validó la erradicación:** | | | | |
| | | | | |
| | | | | |
| | | | | |

**Apéndice C: Procedimientos de violación de la HIPAA para Información de Salud Protegida (PHI)**

**Procedimientos**

En caso de que D3M3NT SA DE CV identifique una posible violación de la PHI, se deberán seguir los siguientes procedimientos.

**Paso 1: Identificación (descubrimiento)**

Una violación de la PHI se considerará "descubierta" a partir del primer día en que D3M3NT SA DE CV tenga conocimiento del incumplimiento o, ejerciendo una diligencia razonable, hubiera o debiera haber tenido conocimiento del incumplimiento.

Si se descubre una posible violación ante la que se deba actuar con rapidez, debe informarse de inmediato.

A continuación, se describe completamente lo que constituye la PHI

- PHI es cualquier información de salud que pueda estar vinculada a una persona e incluye lo siguiente:

1. Nombres (nombre completo o apellido e inicial)
2. Todos los identificadores geográficos menores que un estado, excepto los tres dígitos iniciales de un código postal si, de acuerdo con los datos actuales disponibles públicamente de la Oficina del Censo de los Estados Unidos: la unidad geográfica formada al combinar todos los códigos postales con los mismos tres dígitos iniciales contiene más de 20 000 personas; y los tres dígitos iniciales de un código postal para todas las unidades geográficas que contienen 20 000 o menos personas se cambian a 000
3. Fechas (distintas del año) directamente relacionadas con un individuo, incluida la fecha de nacimiento, la fecha de admisión, la fecha de alta, la fecha de muerte; y todas las edades mayores de 89 años y todos los elementos de fechas (incluido el año) indicativos de dicha edad, excepto que dichas edades y elementos pueden agregarse en una sola categoría de 90 años o más
4. Números de teléfono

5. Números de fax
6. Direcciones de correo electrónico
7. Números de Seguro Social
8. Números de historia clínica
9. Números de beneficiarios del seguro médico
10. Números de cuenta
11. Números de certificado/licencia
12. Identificadores de vehículo (incluidos números de serie y números de matrícula)
13. Identificadores y números de serie de dispositivo
14. Localizadores uniformes de recursos web (URL)
15. Números de dirección de protocolo de Internet (IP)
16. Identificadores biométricos, incluido huellas de dedos, retinas y voz
17. Imágenes fotográficas de rostro completo y cualquier imagen comparable
18. Cualquier otro número, característica o código de identificación únicos, excepto el código único asignado por el investigador para codificar los datos

También existen estándares y criterios adicionales para proteger la privacidad de las personas contra la reidentificación. Cualquier código utilizado para sustituir los identificadores en los conjuntos de datos no puede derivarse de ninguna información relacionada con el individuo y los códigos maestros, ni puede revelarse el método para derivar los códigos. Por ejemplo, las iniciales de un sujeto no se pueden usar para codificar sus datos porque las iniciales se derivan de su nombre. Además, el investigador no debe tener conocimiento real de que el sujeto de la investigación podría volver a identificarse a partir de los identificadores restantes en la PHI utilizada en el estudio de investigación. En otras palabras, la información seguiría considerándose identificable si hubiera una forma de identificar a la persona, aunque se eliminaran los 18 identificadores.

**Paso 2: Informes iniciales y escalamiento**

Si se cree que se ha producido una posible violación de la PHI, se debe notificar de inmediato al responsable de la seguridad o privacidad designado, o a su representante designado.

Proporcione toda la información disponible en el momento de la inicial con respecto a la posible violación, debe incluir lo siguiente:

- Nombres
- Fechas
- La naturaleza de la PHI potencialmente violada
- La forma de la divulgación (fax, correo electrónico, correo, verbal)
- Todos los empleados implicados
- El destinatario
- Todas las otras personas con conocimiento
- Cualquier documentación escrita o electrónica asociada que pueda existir

La notificación y la documentación asociada pueden contener PHI y solo debe entregarse al responsable de la seguridad o privacidad designado, o a su representante designado.

No discuta la posible violación con nadie más, y no intente llevar a cabo una investigación, ya que estas tareas las realizará el responsable de la seguridad o privacidad designado, o su representante designado.

**Paso 3: Investigación**

Una vez recibida la notificación de una posible violación, el responsable de la seguridad o privacidad designado, o su representante designado, llevará a cabo una investigación de inmediato.

La investigación incluirá las siguientes actividades:

- Entrevistar a los empleados implicados
- Recopilar documentación escrita
- Completar toda la documentación adecuada
- Investigación forense (opcional en función del incidente)

El responsable de la seguridad o privacidad designado, o su representante designado, conservará toda la documentación relacionada con posibles investigaciones de violación, de conformidad con los requisitos de retención de registros establecidos, o durante un mínimo de seis años, lo que sea mayor.

**Paso 4: Evaluación de riesgos y recomendación**

Una vez finalizada la investigación, el responsable de la seguridad o privacidad designado, o su representante designado, realizará una Evaluación de Riesgos para determinar si el uso o la divulgación de la PHI constituye una violación que requiera una notificación adicional a la Entidad Cubierta.

El responsable de la seguridad o privacidad designado, o su representante designado, documentará adecuadamente la Evaluación de Riesgos y formulará una recomendación a la gerencia ejecutiva o al asesor legal sobre si la notificación a la Entidad Cubierta de la posible violación sería prudente.

Al llevar a cabo la Evaluación de Riesgos, se aplicará una norma de "juicio razonado" al incidente que será específico de los hechos y se tendrán en cuenta los siguientes factores:

- ¿La divulgación involucró PHI no segura en primer lugar?
- ¿Quién usó o divulgó innecesariamente la PHI no segura?
- ¿A quién se le reveló la información sin autorización?
- ¿Se devolvió dicha información antes de que pudiera accederse para un propósito indebido?
- ¿Qué tipo de PHI no segura está involucrada y en qué cantidad?
- ¿Se hizo la divulgación con algún propósito indebido?
- ¿Existe la posibilidad de un riesgo significativo de ocasionar un daño financiero, de reputación u otro daño a la persona cuya PHI se divulgó?
- ¿Se tomaron medidas inmediatas para mitigar cualquier daño potencial?
- ¿Se aplica alguna de las excepciones de violación específicas?

**Paso 5: Determinación final**

La gerencia ejecutiva de D3M3NT SA DE CV en colaboración con el asesor legal, deberá, después de revisar las pruebas y la evaluación de riesgos, tener la autoridad final para determinar si se produjo una violación de la PHI y qué acciones adicionales, si las hubiera, están justificadas.

**Paso 6: Notificación**

En caso de que la gerencia ejecutiva y/o el asesor legal de D3M3NT SA DE CV determinen que se justifica la notificación a la Entidad cubierta, la gerencia ejecutiva y/o el asesor legal de D3M3NT SA DE CV prepararán y transmitirán sin demora una notificación a la Entidad cubierta.

1. **Hora de la notificación**

D3M3NT SA DE CV deberá notificar a la Entidad Cubierta "sin retraso injustificado" antes de los 60 días posteriores a la detección o notificación de la violación, según lo exija la ley.

Los Acuerdos de servicio y de socio comercial de D3M3NT SA DE CV establecen que D3M3NT SA DE CV es un contratista independiente; por lo tanto, el tiempo de la Entidad cubierta para

proporcionar la notificación requerida comienza a correr en la fecha en que D3M3NT SA DE CV notifica a la Entidad cubierta del incumplimiento.

1. **Retraso de la notificación**
2. ***Retraso injustificado***

Si el responsable de la seguridad designado, o el responsable de la privacidad, o su representante designado, considera que su investigación no se completará en un plazo razonable, se informará a la gerencia ejecutiva o al asesor jurídico para garantizar que se notifique a la Entidad Cubierta antes de que se complete la investigación.

1. ***Retraso en la aplicación de la ley***

Se permite un retraso en la notificación si un funcionario del orden declara que una notificación sobre una violación impediría una investigación penal o causaría daños a la seguridad nacional.

1. Si se recibe una solicitud policial, la declaración policial debe ser por escrito y debe especificar la duración de la demora requerida.
2. Si la solicitud de demora en la notificación es oral, D3M3NT SA DE CV debe documentar la declaración y solicitar una confirmación por escrito dentro de un plazo de 30 días. Si no se recibe una solicitud por escrito de demora dentro de ese plazo, D3M3NT SA DE CV debe enviar una notificación de la infracción a la Entidad cubierta.
3. **Contenido de la notificación**

Toda notificación a la Entidad Cubierta (CE, por su sigla en inglés) cursada por D3M3NT SA DE CV incluirá toda la información requerida por la ley, pero, como mínimo, tendrá el siguiente contenido:

- Identificación de cada individuo cuya PHI se cree que se ha infringido
- La fecha del descubrimiento del incidente
- La fecha de divulgación
- Los hechos y circunstancias que rodean la divulgación
- Toda la documentación asociada
- Toda otra información disponible conocida por D3M3NT SA DE CV que la Entidad cubierta deberá incluir en su propio Aviso a las personas.

Cualquier información adicional relacionada con la violación que D3M3NT SA DE CV detecte después de la notificación inicial a la Entidad Cubierta se proporcionará de inmediato a la Entidad Cubierta según lo exija la ley.

Cualquier notificación a la Entidad Cubierta se enviará por correo postal de primera clase con solicitud de un recibo de devolución, y el recibo de devolución, así como una copia de la Notificación a la Entidad Cubierta, se mantendrá con la documentación relacionada y se conservará de conformidad con los requisitos de retención de registros establecidos o durante un mínimo de seis años, lo que sea mayor.

**Paso 7: Documentación**

Todas las fases del proceso deben documentarse en detalle de manera específica para cada caso, de una manera suficiente para demostrar que se completaron todos los pasos adecuados. Toda la documentación de respaldo asociada con la posible violación se mantendrá registrada de acuerdo con los requisitos de retención de registros establecidos o durante un mínimo de seis años, lo que sea mayor.

**Lista de verificación de violación de la HIPAA**

- Después de cualquier incumplimiento real o sospechoso de información médica protegida electrónica no segura (ePHI), D3M3NT SA DE CV debe notificar a la Entidad cubierta (CE, por sus siglas en inglés) afectada.
- Notificar al responsable de la seguridad o al responsable de la privacidad, y al Departamento Legal de una presunta violación de ePHI, dentro de las cuatro (4) horas.
- El Equipo de Respuesta ante Incidentes investiga las sospechas de violación y lleva a cabo una Evaluación de Riesgos para verificar si los datos de la ePHI fueron comprometidos.
- El Equipo de Respuesta ante Incidentes completará un Informe de Notificación de Violación.
- El Equipo de Respuesta ante Incidentes proporciona el Informe de Notificación de Violación completado al responsable de la seguridad o al responsable de la privacidad para su revisión y aprobación.
- El responsable de la seguridad, o de la privacidad, revisa y aprueba el Informe de Notificación de Violación presentado.
- El responsable de la seguridad, o de la privacidad, proporcionará una copia del informe final de notificación de incumplimiento al departamento jurídico de D3M3NT SA DE CV dentro de un (1) día hábil después de la aprobación.
- El Departamento Legal revisa el Informe de Notificación de Violación y envía el informe a la Entidad Cubierta mediante canales de comunicación aprobados.
- El Departamento Legal se asegurará de que la notificación a la Entidad Cubierta ocurra en un plazo no superior a los sesenta (60) días calendario posteriores a la detección inicial de una violación o sospecha de violación, a menos que se retrase por un organismo del orden competente.

**Contenido y plantilla de notificación de violación de la HIPAA**

El Informe de Notificación de Violación a la Entidad Cubierta (CE) debe incluir la siguiente información:

- Identificación de cada persona asociada con la Entidad Cubierta afectada (CE) cuya ePHI se sospechaba que se había accedido, adquirido, utilizado o divulgado (en la medida de lo posible)
- Cualquier otra información que la Entidad Cubierta deba incluir en la notificación a la persona afectada de conformidad con CFR 164.404 (c) que incluya:
    - Una breve descripción de lo que sucedió, incluida la fecha de la violación y la fecha de descubrimiento de la violación, si se conoce
    - Una descripción de los tipos de información de salud protegida no segura involucrados en la violación (por ejemplo, si se involucró el nombre completo, número de seguro social, fecha de nacimiento, domicilio, número de cuenta, diagnóstico, código de discapacidad u otros tipos de información)
    - Cualquier medida que las personas deben tomar para protegerse de posibles daños que se deriven de la violación

**Plantilla de notificación de violación de la HIPAA**

| | |
|---|---|
| **Seguridad de la Información: Informe de Notificación de Violación de la HIPAA/ePhI** | |
| **Número de incidente:(generado automáticamente por sistema)** | |
| **Otros incidentes relacionados con este incidente:** | |
| **Estado del incidente de violación** | (es decir, Nuevo, En curso, Reenviado para investigación, Resuelto) |

| | |
|---|---|
| **Resumen del incidente** | Descripción de lo que ocurrió y se sabe hasta la fecha |
| **Descripción del incidente** | Fecha y hora en que se descubrió el incidente: |
| Fecha y hora en que se informó del incidente: | |
| Fecha y hora en que ocurrió el incidente: | |
| Lugar del incidente: | |
| Personal involucrado en el incidente: | |
| Tipo y volumen de información involucrada: | |
| Accesibilidad/vulnerabilidad de la ePHI / controles de protección establecidos: (por ejemplo, Cifrado, entre otros): | |
| Indicadores de compromiso relacionados con el incidente: | |
| Causa raíz del incidente: | |
| Conocimiento del incidente (quién lo sabe ahora): | |
| **Evaluación inicial de riesgos** | Número de personas potencialmente afectadas: |
| Posible violación de la privacidad (Sí/No): | |
| Riesgo para las personas (tipos y extensiones): | |
| Riesgo financiero para la organización: | |
| Riesgo legal o contractual para la organización: | |
| Riesgo regulatorio para la organización: | |
| Riesgo de relaciones públicas para la organización: | |
| ePHI accedida o modificada de manera no autorizada (Sí / No): | |
| **Pasos realizados** | Medidas actuales adoptadas: |
| Evidencia recopilada / Cadena de custodia: | |
| Personas contactadas: (p. ej.: propietarios de sistemas, administradores de sistemas, policía, asesores externos, investigadores forenses): | |
| Proveedor de servicios de violación de datos contactado: | |
| Agencias notificadas: | |
| Cerrar o pasar a la fase de investigación y por qué: | |
| **Notificación** | Entidades Cubiertas (CE) afectadas: |
| Fecha de notificación a Entidades Cubiertas (CE): | |
| Métodos utilizados para notificar a las Entidades Cubiertas (CE): | |
| Registro de notificaciones (n.° de *ticket* en donde se documenta la notificación): | |
| Lista generada por el sistema de personas afectadas adjunta (obligatorio): | |
| Detalles adicionales: | |
| **Recomendaciones** | Requisitos de notificación inmediata: las Entidades Cubiertas afectadas DEBEN ser notificadas dentro de los sesenta (60) días posteriores a la sospecha de una violación. |
| Prioridades y consideraciones para una investigación posterior | |

| | |
|---|---|
| Próximos pasos a seguir (por ejemplo, reconstruir el *host*, actualizar una aplicación, implementar controles adicionales, entre otros) | |
| Recomendaciones para personas afectadas: | |

**Apéndice D: Manual de vulnerabilidad de la cuenta raíz de AWS**

**Manual de Respuesta ante Incidentes: uso raíz**

**Objetivo**

El objetivo de este manual es brindar orientación específica sobre cómo administrar el uso de la cuenta raíz de AWS. Este manual no sustituye a una estrategia de Respuesta ante Incidentes en profundidad. Este manual se centra en el ciclo de vida de la Respuesta ante Incidentes:

- Establecer control
- Determinar el impacto
- Recuperar según sea necesario
- Investigar la causa raíz
- Mejorar

A continuación, se enumeran los Indicadores de Violación (IOC, por sus siglas en inglés), los pasos iniciales (detener el sangrado) y los comandos CLI detallados necesarios para ejecutar estos pasos.

**Suposiciones**

- CLI está configurado e instalado.
- El proceso de reporte ya está en marcha.
- El asesor de confianza está activo.
- El *hub* de seguridad está activo.

**Indicadores de Violación**

- Actividad anormal en la cuenta
  - Creación de usuarios de IAM
  - CloudTrail desactivado
  - Cloudwatch desactivado
  - SNS en pausa
  - Paso Funciones en pausa
- Lanzamiento de AMI nuevas o inesperadas
- Cambios en los contactos de la cuenta

**Pasos para remediar: establecer el control**

En la documentación de AWS para una posible cuenta vulnerada, se describen las tareas específicas que se enumeran a continuación. La documentación de una posible cuenta comprometida se puede encontrar en: *What do I do if I notice unauthorized activity in my AWS account? (¿Qué hago si observo una actividad no autorizada en mi cuenta de AWS?)*

1. Comuníquese con el equipo de soporte de AWS y TAM lo antes posible.
2. Cambie y rote la contraseña Root y agregue un dispositivo de autenticación multifactor asociado con Root.
3. Rote las contraseñas, las claves de acceso o secretas y los comandos CLI relevantes para los pasos de reparación.
4. Revise las medidas adoptadas por el usuario raíz.
5. Abra los manuales para esas medidas.

6. Cierre el incidente.
7. Revise el incidente y comprenda lo que sucedió.
8. Solucione los problemas subyacentes, implemente mejoras y actualice el manual, según sea necesario.

**Medidas adicionales: determinar el impacto**

Revise los elementos creados y las llamadas mutantes. Puede haber elementos que se hayan creado para permitir el acceso en el futuro. Algunas cosas que tener en cuenta:

- Roles de cuentas cruzadas de IAM
- Usuarios de IAM
- *Buckets* de S3
- Instancias de EC2
- AWS EC2