Política de gestión de riesgos

Tipo de directiva: Política de gestión de riesgos

Número de política: 6

Nombre de la empresa:	D3M3NT SA DE CV	
Propietario(s) de la política:	VICTOR ACOSTA LOPEZ	Teléfono:526144272392
Fecha de entrada en vigencia:	09/04/2024	Fecha de revisión: 09/04/2024
Última revisión:	24/05/2023	Próxima revisión: 09/04/2025

Objetivo:

Definir acciones para abordar los riesgos y oportunidades de seguridad de la información de D3M3NT SA DE CV. Definir un plan para la consecución de los objetivos de seguridad y privacidad de la información.

Alcance:

- Todos los sistemas de TI de D3M3NT SA DE CV que procesan, almacenan o transmiten datos confidenciales, privados o críticos para el negocio.
- Se deben considerar los riesgos que podrían afectar los objetivos a mediano y largo plazo de D3M3NT SA DE CV, así como los riesgos que se encontrarán en la prestación diaria de servicios.
- Los sistemas y procesos de gestión de riesgos de D3M3NT SA DE CV se ajustarán para lograr el máximo beneficio sin aumentar la carga burocrática y, en última instancia, sin afectar a la prestación de servicios básicos a la organización.
- Por lo tanto, D3M3NT SA DE CV considerará la relevancia del riesgo en el desarrollo de sistemas y procesos para administrar el riesgo .
- Esta política se aplica a todos los empleados de D3M3NT SA DE CV y a todas las partes externas, incluyendo pero no limitado a consultores y contratistas, socios comerciales, vendedores, proveedores de servicios externos y otras entidades de terceros de D3M3NT SA DE CV con acceso a redes y recursos del sistema de D3M3NT SA DE CV.

Declaración de gestión de riesgos

La gestión inadecuada de los riesgos de TI expone a D3M3NT SA DE CV a riesgos que incluyen el compromiso delos sistemas, servicios e información de la red, ciberataques, problemas contractuales o legales del cliente o de D3M3NT SA DE CV. D3M3NT SA DE CV garantizará que la gestión de riesgos desempeñe un papel integral en la gobernanza y gestión de la organización a nivel estratégico y operativo. El propósito de una política de gestión de riesgos consiste en garantizar que logre las metas y objetivos establecidos en el plan de negocio.

Estrategia para la gestión de riesgos

D3M3NT SA DE CV ha desarrollado procesos para identificar aquellos riesgos que obstaculizarán el logro de sus objetivos estratégicos y operativos. Por lo tanto, D3M3NT SA DE CV se asegurará de contar con los medios para identificar, analizar, controlar y monitorear los riesgos estratégicos y operativos que enfrenta utilizando esta política de gestión de riesgos basada en las mejores prácticas.

D3M3NT SA DE CV se asegurará de que la estrategia y la política de gestión de riesgos se revisen periódicamente y de que las funciones de auditoría interna sean responsables de garantizar:

- La política de gestión de riesgos se aplica a todas las áreas pertinentes de D3M3NT SA DE CV
- La política de gestión de riesgos y su aplicación operativa se revisan regularmente
- los incumplimientos se comuniquen a los funcionarios y autoridades competentes de la empresa.

Aplicación práctica de la gestión de riesgos

D3M3NT SA DE CV ha adoptado un formato estándar para su uso en la identificación de riesgos, clasificación y evaluación.

El formato se basa en las siguientes normas y marcos de NIST e ISO:

- ISO 27005
- NIST 800-30
- NIST 800-37

Los riesgos se evalúan y clasifican según su impacto y su probabilidad de ocurrencia. Se realizará una evaluación de riesgos formal y pruebas de penetración en la red al menos una vez al año, y se tendrán en cuenta los resultados de cualquier actividad de gestión de vulnerabilidades técnicas realizada de acuerdo con la Política de Seguridad de las Operaciones.

Categorías de riesgo

D3M3NT SA DE CV considerará y evaluará los riesgos en toda la organización. Las categorías de riesgo que deben considerarse para la evaluación incluyen:

- Reputacional
- Contractual
- Regulatorio/cumplimiento
- Económico/financiero
- Fraude
- Privacidad
- Medio ambiente y sustentabilidad
- Impacto en las personas
- Uso de servicios en la nube
- Capacidad operacional

Cada riesgo será evaluado en cuanto a su probabilidad e impacto. Tanto el impacto como la probabilidad se evalúan en una escala del 1 al 5. El impacto puede variar de 1 ("Impacto muy bajo") a 5 ("Impacto muy alto") y la probabilidad puede variar de 1 ("Muy improbable") a 5 ("Muy probable").

Criterios de riesgo

Los criterios para determinar el riesgo son la probabilidad y el impacto combinados de un evento que afecte negativamente la confidencialidad, disponibilidad, integridad o privacidad de la información de la organización y del cliente, la información de identificación personal (PII) o los sistemas de información del negocio.

Para todas las entradas de riesgo, como evaluaciones de riesgo, análisis de vulnerabilidades, pruebas de penetración, programas de recompensas por errores, etc., la dirección de D3M3NT SA DE CV se reservará el derecho de modificar las clasificaciones de riesgo en función de la evaluación de la naturaleza y criticidad del procesamiento del sistema, así como de la naturaleza, criticidad y capacidad de explotación (u otros factores y consideraciones relevantes) de la vulnerabilidad identificada.

Respuesta al riesgo, tratamiento y seguimiento

Los riesgos se priorizarán y mantendrán en un registro de riesgos donde se organizarán y mapearán con base en el enfoque de esta política. Se deberán emplear las siguientes respuestas al riesgo:

- **Mitigar**: D3M3NT SA DE CV puede tomar medidas o emplear estrategias para reducir el riesgo.
- **Aceptar**: D3M3NT SA DE CV puede aceptar y monitorear el riesgo en el momento actual. Esto puede ser necesario para algunos riesgos que surgen de eventos externos.
- **Transferencia**: D3M3NT SA DE CV puede decidir transferir el riesgo a otra parte. Por ejemplo, se pueden acordar términos contractuales para garantizar que el riesgo no sea asumido por D3M3NT SA DE CV o un seguro puede ser apropiado para protegerse contra pérdidas financieras.
- **Evitar**: el riesgo puede ser tal que D3M3NT SA DE CV podría decidir cesar la actividad o modificarla de tal manera que acabe con el riesgo.

Cuando D3M3NT SA DE CV elige una respuesta de riesgo que no sea "Aceptar" o "Evitar", desarrollará un Plan de tratamiento de riesgos.

Procedimientos de gestión de riesgos

El procedimiento de gestión de riesgos cumplirá los siguientes criterios:

1. D3M3NT SA DE CV mantendrá un Registro de Riesgos y un Plan de Tratamiento.
2. Los riesgos se clasificaron por probabilidad y gravedad/impacto, como críticos, altos, medios, bajos e insignificantes.
3. El riesgo general se determinará gracias a una combinación de probabilidad e impacto.
4. Los riesgos pueden valorarse para calcular las pérdidas monetarias cuando sea posible.
5. D3M3NT SA DE CV responderá a los riesgos de manera priorizada. La prioridad de reparación considerará la probabilidad de riesgo y el impacto, el costo, el esfuerzo laboral y la disponibilidad de recursos. Se pueden realizar múltiples correcciones simultáneamente
6. Se presentarán informes periódicos a la alta dirección de D3M3NT SA DE CV para garantizar que los riesgos se mitiguen de forma adecuada y según las prioridades y objetivos del negocio.

Seguridad de la información en la gestión de proyectos

D3M3NT SA DE CV considerará el riesgo de seguridad de la información como parte de todos los proyectos que sean de naturaleza técnica o que puedan representar un riesgo para la empresa, independientemente del tamaño, la duración o el dominio. Desde la planificación inicial, hasta la finalización de un proyecto, es esencial evaluar y mitigar adecuadamente los riesgos de seguridad de la información, lo que implica:

- evaluaciones iniciales de los riesgos para la seguridad de la información,
- identificación y tratamiento tempranos de los requisitos de seguridad de la información, y
- evaluación y gestión continuas de los riesgos, especialmente en lo que respecta a las comunicaciones internas y externas del proyecto.

Funciones y responsabilidades

La siguiente tabla describe las actividades y responsabilidades específicas de gestión de riesgos asociadas con cada rol.

Función	**Responsabilidad**
Junta Directiva	Area responsable de la aceptación o tratamiento de cualquier riesgo de la organización.
Gerente de TI	Puede aprobar la evitación, corrección, transferencia o aceptación de cualquier riesgo citado en el Registro de Riesgos.
Gerente de TI / SOPORTE DE TI	Será responsable de la identificación y desarrollo del plan de tratamiento de todos los riesgos relacionados con la seguridad de la información. Esta persona será responsable de comunicar los riesgos a la alta dirección y de adoptar tratamientos de riesgo de acuerdo con la dirección ejecutiva.

Otros recursos

04-Política de Evaluación y Tratamiento de Riesgos SGSI

Para consultar el Registro de riesgos actual, consulte https://intra.dmente.mx/risk-register

Cobertura ISO 27001/27701

ISO 27001 6.1; 6.2

Versión	Fecha	Descripción	Autor	Aprobado por
1.0	25/05/2023	Implementación inicial	Víctor Acosta	Marco Villanueva
2.0	05/06/2023	Segunda Implementación	Víctor Acosta	Marco Villanueva
2.1	09/04/2024	Ajuste por traducción	Víctor Acosta	Marco Villanueva

APÉNDICE A - Proceso de evaluación de riesgos

A continuación, se muestra una descripción general de alto nivel del proceso utilizado por D3M3NT SA DE CV para evaluar y administrar los riesgos relacionados con la seguridad de la información.

El proceso que se analiza a continuación se basa en el NIST 800-30 y proporciona orientación a D3M3NT SA DE CV sobre cómo:

- Preparar y llevar a cabo una evaluación de riesgos eficaz.
- Comunicar y compartir los resultados de la evaluación y la información relacionada con el riesgo.
- Gestionar y mantener los riesgos de forma continua.

El proceso de evaluación de riesgos se compone de los siguientes pasos:

1. Prepararse para la evaluación
2. Realizar la evaluación
3. Comunicar la evaluación
4. Mantener la evaluación

Paso 1: Prepararse para la evaluación

En este paso, el objetivo es establecer el contexto para la evaluación de riesgos. Esto se puede lograr de la siguiente manera:

- Identificar el propósito de la evaluación
  - Determinar la información que la evaluación pretende producir y las decisiones que la evaluación pretende respaldar.
- Identificar el alcance de la evaluación
  - Determinar la función o el proceso organizativo aplicable, el marco temporal asociado y cualquier consideración arquitectónica o tecnológica aplicable.
- Identificar cualquier suposición o restricción asociada con la evaluación.
  - Determinar los supuestos en áreas clave relevantes para la evaluación de riesgos, incluyendo:
    - Prioridades de la organización
    - Objetivos de negocio
    - Disponibilidad de recursos
    - Habilidades y experiencia del equipo de evaluación de riesgos.
- Identificar fuentes de información.
  - Diagramas arquitectónicos/tecnológicos y configuraciones del sistema.
  - Requisitos legales y reglamentarios
  - Fuentes de amenazas
  - Eventos de amenaza
  - Vulnerabilidades y condiciones que influyen
  - Impactos potenciales
  - Controles existentes

Paso 2: Realizar la evaluación

En este paso, el objetivo es elaborar una lista de riesgos relacionados con la seguridad de la información que pueda priorizarse por nivel de riesgo y utilizarse para fundamentar las decisiones de respuesta al riesgo. Esto puede lograrse realizando lo siguiente:

- Identificar las fuentes de amenazas
  - Determinar y caracterizar las fuentes de amenazas relevantes y de interés para D3M3NT SA DE CV , incluyendo, entre otras cosas:
    - Humano (intencional o no intencional / interno o externo)
    - Medio ambiente
    - Natural
    - Sistema o equipo
  - Considere lo siguiente al identificar fuentes de amenazas:
    - Capacidad
    - Motivo/Intención
    - Personas dirigidas intencionadamente a personas, procesos y/o tecnologías
    - Personas, procesos y/o tecnologías dirigidos involuntariamente
- Identificación de eventos de amenazas
  - Determinar qué eventos de amenaza podrían ser producidos por las fuentes de amenaza identificadas que tienen potencial para afectar a D3M3NT SA DE CV .
  - Considerar la relevancia de los acontecimientos y las fuentes que pudieron iniciarlos.
- Identificar vulnerabilidades
  - Determinar las vulnerabilidades asociadas a personas, procesos y/o tecnologías que podrían ser explotadas por las fuentes y los eventos de amenazas identificados.
  - Considerar cualquier condición influyente que pudiera afectar y ayudar al éxito de la explotación.
- Determinar la probabilidad
  - Determinar la probabilidad de que las fuentes de amenaza identificadas inicien los eventos de amenaza identificados y puedan explotar con éxito cualquier vulnerabilidad identificada.
  - Tenga en cuenta lo siguiente a la hora de determinar la probabilidad:
    - Características de las fuentes de amenaza que podrían iniciar los acontecimientos.
      - Capacidad
      - Motivo/Intención
      - Oportunidad
    - Las vulnerabilidades y/o condiciones que influyen en las identificadas
    - La exposición de D3M3NT SA DE CV basada en cualquier salvaguarda/contramedida planeada o implementada para prevenir o mitigar tales eventos.
- Determinar el impacto
  - Determinar el impacto para los objetivos empresariales, las operaciones, los activos, las personas, los clientes y/u otras organizaciones de D3M3NT SA DE CV teniendo en cuenta lo siguiente:
    - Impactos comerciales y operativos
    - Daños financieros
    - Daño a la reputación
    - Cuestiones legales o regulatorias
  - Al determinar el impacto, tenga también en cuenta las salvaguardas/contramedidas previstas o implementadas por D3M3NT SA DE CV que pudieran mitigar o disminuir sus efectos.
- Determinar el riesgo
  - Determinar los riesgos generales relacionados con la seguridad de la información para D3M3NT SA DE CV al combinar lo siguientes:

        - La probabilidad de que ocurra el evento.
        - El impacto que resultaría del evento.
    - El riesgo para D3M3NT SA DE CV es proporcional a la probabilidad y al impacto de un evento.
        - Evento de mayor riesgo: es más probable que suceda y el impacto resultante será mayor.
        - Evento de menor riesgo: es menos probable que suceda y el impacto resultante será mínimo, si es que lo hay.

Paso 3: Comunicar y compartir los resultados de la evaluación de riesgos

En este paso, el objetivo es garantizar que los responsables de la toma de decisiones en D3M3NT SA DE CV y la dirección ejecutiva dispongan de la información adecuada relacionada con los riesgos, necesaria para informar y orientar las decisiones sobre los mismos.

- Comunique los resultados
    - Comunique los resultados de la evaluación de riesgos a los responsables de la toma de decisiones y a la dirección ejecutiva de D3M3NT SA DE CV para ayudar a tomar decisiones basadas en el riesgo y obtener el apoyo necesario para la respuesta al riesgo.
    - Comparta la evaluación de riesgos y la información relacionada con los riesgos con el personal apropiado de D3M3NT SA DE CV para ayudar a apoyar los esfuerzos de respuesta a los riesgos.

Paso 4: Mantener la evaluación

En este paso, el objetivo es mantener actualizados los conocimientos específicos relacionados con los riesgos en los que incurra D3M3NT SA DE CV. Los resultados de las evaluaciones informan e impulsan decisiones basadas en riesgos y guían los esfuerzos continuos de respuesta a riesgos.

- Vigilar los factores de riesgo
    - Llevar a cabo un monitoreo continuo de los factores de riesgo que contribuyen a los cambios en el riesgo para los objetivos comerciales, de operaciones, activos, individuos, clientes y/u otras organizaciones de D3M3NT SA DE CV.
- Mantener y actualizar la evaluación
    - Actualizar las evaluaciones de riesgo existentes utilizando los resultados del monitoreo continuo de los factores de riesgo y realizando evaluaciones adicionales, como mínimo una vez al año.

APÉNDICE B - Matriz de evaluación de riesgos y clave descriptiva

RIESGO= PROBABILIDAD * IMPACTO	**PROBABILIDAD**				
IMPACTO	**Muy poco probable: 1**	**Poco probable: 2**	**Algo probable: 3**	**Probable: 4**	**Muy probable: 5**
Impacto muy alto: 5	**5**	**10**	**15**	**20**	**25**
Alto impacto: 4	**4**	**8**	**12**	**16**	**20**
Impacto medio: 3	**3**	**6**	**9**	**12**	**15**
Bajo impacto: 2	**2**	**4**	**6**	**8**	**10**
Impacto muy bajo: 1	**1**	**2**	**3**	**4**	**5**

NIVEL DE RIESGO	**DESCRIPCIÓN DEL RIESGO**
Bajo (1-4)	Se podría esperar que un evento de amenaza tenga un efecto adverso limitado en las operaciones organizacionales, capacidades de misión, recursos, individuos, clientes u

	otras organizaciones.
Medio (5-12)	Se podría esperar que un evento de amenaza tenga un efecto adverso grave en las operaciones organizacionales, capacidades de misión, recursos, individuos, clientes u otras organizaciones
Alto (15-25)	Se podría esperar que un evento de amenaza tenga un efecto adverso grave en las operaciones organizacionales, capacidades de misión, recursos, individuos, clientes u otras organizaciones

NIVEL DE PROBABILIDAD	DESCRIPCIÓN DE LA PROBABILIDAD	CLASIFICACIÓN (NUMÉRICA)
Muy poco probable (1)	Un evento de amenaza es tan poco probable que se puede suponer que no se producirá. Una fuente de amenaza no está motivada o no tiene capacidad, o existen controles para evitar o impedir de forma significativa que se explote la vulnerabilidad.	1
Poco probable (2)	Un evento de amenaza es poco probable, pero existe una ligera posibilidad de que se produzca. Una fuente de amenaza carece de motivación o capacidad suficientes, o existen controles para evitar o impedir que se explote la vulnerabilidad.	2
Algo probable (3)	Un evento de amenaza es probable y puede asumirse que es posible que ocurra. Una fuente de amenaza está motivada o tiene la capacidad, pero existen controles que pueden reducir significativamente o impedir la explotación exitosa de la vulnerabilidad.	3
Probable (4)	Un evento de amenaza es probable y puede asumirse que ocurra. Una fuente de amenazas está muy motivada o tiene la capacidad y los recursos suficientes, pero existen algunos controles que pueden reducir o impedir la explotación exitosa de la vulnerabilidad.	4
Muy probable (5)	Un evento de amenaza es altamente probable y puede asumirse que ocurra. Una fuente de amenazas está muy motivada o tiene la capacidad y los recursos suficientes, pero no hay controles o lo controles presentes no pueden reducir o impedir la explotación exitosa de la vulnerabilidad.	5

NIVEL DE IMPACTO	DESCRIPCIÓN DEL IMPACTO	CLASIFICACIÓN (NUMÉRICA)
Impacto muy bajo (1)	Se podría esperar que un evento de amenaza tenga un efecto adverso en las operaciones organizacionales, capacidades de misión, recursos, individuos, clientes u otras organizaciones	1
Bajo impacto (2)	Se podría esperar que un evento de amenaza tenga un efecto adverso limitado, lo que significa: degradación de la capacidad de la misión, pero aún se pueden realizar funciones principales; daños menores; pérdidas financieras menores; o el rango de efectos se limita a algunos recursos cibernéticos, pero no a recursos críticos.	2

Impacto medio (3)	Se podría esperar que un evento de amenaza tenga un efecto adverso grave, lo que significa: degradación significativa de la capacidad de la misión, pero las funciones principales aún se pueden realizar con una capacidad reducida; daños menores; pérdida financiera menor; o la variedad de efectos es importante para algunos recursos cibernéticos y algunos recursos críticos.	3
Alto impacto (4)	Se podría esperar que un evento de amenaza tenga un efecto adverso grave o catastrófico, es decir: degradación grave o pérdida de la capacidad de la misión y no se pueden realizar una o más funciones principales; daños importantes; pérdida financiera importante; o la variedad de efectos es extensa para la mayoría de los recursos cibernéticos y los recursos más críticos.	4
Impacto muy alto (5)	Cabe esperar que un evento de amenaza tenga múltiples efectos adversos graves o catastróficos sobre las operaciones de la organización, los activos, los individuos, otras organizaciones o la propia nación. La gama de efectos es amplia y afecta a casi todos los recursos cibernéticos.	5