Nombre del documento: Procedimiento para la revisión de la gestión

Número de documento: 08-ISMS

Nombre de la empresa:	D3M3NT SA DE CV
Propietario(s) de la política:	Víctor Acosta
Fecha de entrada en vigencia:	15/04/2024

Objetivo

El objetivo de este documento de procedimiento es definir el proceso de gestión para la revisión y evaluación periódica de la Política del Sistema de Gestión de Seguridad de la Información ("SGSI") de D3M3NT SA DE CV para garantizar su idoneidad, adecuación y eficacia continuas, tal como se define en la sección 9.3 deL ISO/IEC 27001 ("ISO 27001").

Frecuencia y calendario de las revisiones

En D3M3NT SA DE CV, las revisiones de gestión del SGSI deben llevarse a cabo al menos una vez al año para garantizar su idoneidad, adecuación y eficacia continuas.Para los SGSI más nuevos o menos maduros, se programarán revisiones más frecuentes.

Metodología de revisión de la gestión

La metodología de revisión incluirá los siguientes pasos:

No.	Lista de tareas	Responsabilidad
1	Planificar y programar la revisión de la gestión e informar al Consejo de Gobernanza del SGSI	Líder en Gestión de Seguridad de la Información
2	Recopila y analiza las entradas de revisión para identificar elementos de interés (es decir, tendencias, problemas, evaluaciones, informes, actualizaciones de proyectos, incidentes, etc.)	Líder en Gestión de Seguridad de la Información
3	Revise los puntos de interés con el Consejo de Gobernanza del SGSI para identificar decisiones y acciones	Líder en Gestión de Seguridad de la Información
4	Aceptar y aprobar los resultados de la revisión, incluidos los resultados finales (decisiones y acciones)	Consejo de Gobernanza del SGSI
5	Documentar y mantener los resultados de la revisión de la gestión	Líder en Gestión de Seguridad de la Información
6	Integrar los resultados de la revisión (decisiones y acciones) en el SGSI	Líder de Gestión de la Seguridad de la Información/Equipo de Seguridad de la Información

Establecimiento de la agenda para las revisiones

La agenda para las revisiones de la gestión incluirá la revisión y consideración de los siguientes puntos: :

1. estado de las acciones de revisiones de la gestión anteriores;
2. cambios en cuestiones externas e internas (consulte 4.1) que sean relevantes para el SGSI;
3. información sobre el rendimiento de la seguridad de la información, incluyendo tendencias, en:
    1. las no conformidades y acciones correctivas
    2. resultados de monitoreo y medición;
    3. resultados de auditorías; y
    4. cumplimiento de los objetivos de seguridad de la información.
4. comentarios de las partes interesadas, incluyendo sugerencias de mejora, solicitudes de cambio y quejas;
5. resultados de la evaluación o evaluaciones, así como el estado, de los riesgos para la seguridad de la información
6. plan de tratamiento
7. oportunidades de mejora continua, incluyendo las mejoras de la eficacia tanto del SGSI como de los controles de seguridad de la información.

Entrada de revisión de la gestión

Las revisiones de la gestión pueden incluir las siguientes entradas según lo determine el Líder de Gestión de Seguridad de la Información:

- Cambios en el contexto interno o externo de la organización

- Comentarios de las partes interesadas
- Cambios en la práctica líder y la orientación
- Cambios en los requisitos legales, regulatorios o contractuales
- Estado de los objetivos del SGSI
- Criterios de aceptación de riesgos
- Resultados de la evaluación de riesgos
- Estado del plan de tratamiento de riesgos y del plan de implementación
- Monitoreo de la eficacia y resultados de medición
- Resultados de la auditoría interna
- Estado de los elementos de acción de revisiones de la gestión previas
- Observaciones de auditoría externa de terceros (por ejemplo, auditoría externa de certificación)
- Estado de los casos de incumplimiento abiertos, acciones correctivas y planes de mejora
- Tendencias en los casos de incumplimiento y las acciones correctivas
- Los resultados del programa de capacitación utilizado para evaluar el nivel de concienciación sobre la seguridad de la información dentro de la organización
- Incidentes de alto riesgo y los planes de acción y análisis de causa raíz relacionados
- Tendencias en incidentes internos de seguridad de la información
- Resultados de cualquier penetración u otras pruebas técnicas
- Resultados de cualquier consulta relacionada con la privacidad y la respuesta de la empresa
- Contactos de seguridad de la información, consultas, advertencias o sanciones de un organismo gubernamental o regulatorio
- Otros elementos a exclusivo criterio del Líder de Seguridad de la Información o del Consejo de Gobernanza del SGSI
- Estado o resultados de cualquier auditoría relacionada con la seguridad de la información (es decir, certificación, cliente, etc.)

El equipo de Seguridad de la Información analizará estos aportes para identificar problemas, elementos de atención, preguntas, entre otros para el Consejo de Gobernanza del SGSI. El equipo de Seguridad de la Información preparará un resumen de las entradas, un análisis de estas, y las decisiones y acciones clave propuestas que se necesitan según los resultados para mejorar el SGSI. Por ejemplo, un problema que puede identificarse durante el análisis de las entradas de revisión es que los elementos del Plan de Implementación están vencidos, y la acción propuesta para el Consejo de Gobernanza del SGSI sería reasignar recursos específicos o fondos necesarios para completar el Plan de Implementación.

Salidas de la revisión de la gestión

El Consejo de Gobernanza del SGSI revisará el resumen de los elementos de la revisión, el análisis de las entradas y las decisiones y acciones clave propuestas. El Consejo de Gobernanza del SGSI aprobará la revisión, los resultados y todas las decisiones o acciones finales necesarias. Estas decisiones y acciones pueden incluir lo siguiente:

- Cambios en el alcance y los límites del SGSI
- Elementos de acción para mejorar la efectividad del SGSI
- Modificaciones a las políticas, objetivos y procedimientos relacionados de seguridad de la información
- Actualizaciones de la evaluación de riesgos, el plan de tratamiento de riesgos y el plan de implementación
- Identificación o modificación de los requisitos de recursos o fondos necesarios para mejorar el SGSI o para ejecutar planes definidos (por ejemplo, plan de implementación, plan de acción correctiva, entre otros)

Procedimiento para la revisión de las medidas de eficacia

El Consejo de Gobernanza del SGSI revisará las medidas de efectividad de los controles del SGSI:

- El Consejo de Gobernanza del SGSI es responsable de revisar las medidas de efectividad del control al menos una vez al año.
- El equipo de Seguridad de la Información preparará la presentación de la reunión para el Consejo de Gobernanza del SGSI al describir las medidas y métricas y agregarlas al informe o presentación segun represente el caso
- El equipo de Seguridad de la Información identificará si la métrica actual excede los niveles definidos en los criterios de Medición y Métricas.
- Si una métrica excede sus criterios, entonces el Consejo de Gobernanza del SGSI debatirá acerca de las medidas que deben tomarse para corregir la deficiencia que permitió que el control se volviera ineficaz. Las medidas se registrarán en el Plan de Medida Correctiva y Preventiva.

Cobertura ISO 27001

ISO 27001 4.3; 6.1.3; 9.3

Historial de versiones

Versión	Fecha	Descripción	Autor	Aprobado por
1.0	25/05/2023	Política inicial	Víctor Acosta	Marco Villanueva
2.0	15/06/2024	ajustes por traduccion	Víctor Acosta	Marco Villanueva

27701 Anexo del Sistema de Gestión de Información de Privacidad (PIMS)

Este anexo se aplica automáticamente a las organizaciones que implementan la norma ISO 27701 y es opcional para las organizaciones que solo implementan la norma ISO 27001.

- Todas las referencias a "SGSI" en este documento se cambian a "SGSI&P".
- Todas las referencias a la norma ISO 27001 en este documento se cambian a "ISO 27001/27701".
- Todas las referencias al "Sistema de Gestión de Seguridad de la Información" se cambian a "Sistema de Gestión de Seguridad de la Información y la Privacidad".