Nombre del documento: Funciones, responsabilidades y autoridades

Número de documento: 03-ISMS

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

Objetivo

El objetivo de este documento es definir claramente las funciones, responsabilidades y autoridades que son esenciales para el establecimiento, la implementación, el mantenimiento y la mejora continua de la Política del Sistema de Gestión de Seguridad de la Información ("SGSI") de D3M3NT SA DE CV.

Alcance

Esta política se aplica a toda la alta gerencia y al personal asociado con el SGSI en toda la organización.

Funciones y responsabilidades

La alta gerencia deberá revisar periódicamente el SGSI y garantizar la asignación adecuada de responsabilidades y autoridades. LaD3M3NT SA DE CV identificó las siguientes funciones y responsabilidades de alto nivel:

- Alta gerencia: responsable de la revisión y delegación adecuada de las funciones y responsabilidades del SGSI.Las funciones principales y sus funcionalidades deben ser sancionados por este nivel.
- Coordinación del SGSI: encargada de supervisar el establecimiento, el mantenimiento regular, el análisis del rendimiento y la mejora del SGSI.
- Asesoramiento del SGSI: dedicado a proporcionar orientación sobre las evaluaciones de riesgos y los tratamientos asociados a la seguridad de la información.
- Diseño: encargado del desarrollo de procesos y sistemas de seguridad de la información adaptados a las necesidades de la organización.
- Establecimiento de estándares: implicado en la formulación y el ajuste de los estándares y controles de seguridad de la información dentro de la organización.
- Gestión de incidentes: participa en la gestión rápida y eficaz de los incidentes de seguridad de la información que se produzcan.
- Revisión y auditoría: es responsable del examen y la evaluación periódicos y exhaustivos de la eficacia y el cumplimiento del SGSI.

Funciones del SGSI

Consejo de Gobernanza del SGSI

El Consejo de Gobernanza del SGSI está presidido por el Líder en Gestión de Seguridad de la Información y compuesto por la gerencia ejecutiva o sus delegados necesarios para respaldar la seguridad de la información o impulsar la visión futura de la seguridad de la información. Los miembros del Consejo de Gobernanza del SGSI están compuestos por las siguientes funciones:

- CIO (líder de gestión de seguridad de la información y responsable de protección de datos)
- COO
- Director de Operaciones
- Delegados de las empresas de D3M3NT SA DE CV .
- Líderes de TI

Líder en Gestión de Seguridad de la Información

El rol de Líder en Gestión de Seguridad de la Información tiene la autoridad para impulsar la seguridad de la información en D3M3NT SA DE CV a nivel funcional y operativo y es responsable de la coordinación de las actividades del SGSI en toda la organización. Además, el Líder en Gestión de Seguridad de la Información debe cubrir la Coordinación del SGSI: encargado de supervisar el establecimiento, el mantenimiento regular, el análisis del rendimiento y la mejora del SGSI.

El CIO es el líder designado en gestión de seguridad de la información.

Equipo de Seguridad de la Información

El Equipo de Seguridad de la Información se compone de personas que administran las actividades diarias de cumplimiento y monitoreo necesarias para lograr, mantener y mejorar el SGSI a fin de

cumplir con los Objetivos de Seguridad de la Información.

Los miembros del equipo de Seguridad de la Información se componen de los siguientes roles:

- Líder Sistemas de información
- Administradores de sistemas y red
- Ingeniero(s) sénior
- Representante de Recursos Humanos
- Junta Directiva.

Responsable de Protección de Datos

La función de Responsable de Protección de Datos tiene la autoridad para impulsar la privacidad de los datos en D3M3NT SA DE CV a nivel funcional y operativo y es responsable de la coordinación de las actividades de privacidad de datos en toda la organización.

El Líder Sistemas de información es el Responsable de Protección de Datos designado.

Responsables del riesgo

Un responsable del riesgo es una persona o entidad que tiene la autoridad para administrar un riesgo en particular y es responsable de hacerlo.

Empleados, terceros, proveedores, contratistas y consultores

Esta función incluye a todos los empleados, terceros, proveedores, contratistas y consultores que están en el alcance de los departamentos que brindan soporte al SGSI.

Responsabilidades del SGSI

En esta sección, se detallan las responsabilidades de cada función que son esenciales para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGSI.

Consejo de Gobernanza del SGSI

Responsabilidad	**Frecuencia***
Supervisar iniciativas importantes para mejorar la seguridad de la información	Anualmente o según sea necesario
Confirmar que los objetivos de seguridad de la información están establecidos, son compatibles y están actualizados en función de la dirección estratégica de la organización	Anualmente
Revisar las acciones correctivas y las mejoras en el SGSI para lograr sus objetivos previstos	Anualmente
Identificación de los requisitos de seguridad del cliente (excepciones a los controles estándar)	Según sea necesario
Supervisar el progreso de los planes de comunicación, implementación, acción correctiva y mejora	Anualmente
Revisar incidentes de seguridad de la información y apoyar la resolución dentro de su función	Según sea necesario
Proporcionar los recursos adecuados (es decir, presupuesto, personas, equipo, *software*) para establecer, operar y mejorar el SGSI	Anualmente
Aprobar las políticas de seguridad de la información	Anualmente
Aprobar los resultados de la Evaluación de Riesgos y el Plan de Tratamiento de Riesgos	Anualmente

Comunicar la importancia del SGSI y la importancia de la mejora continua	Anualmente
Realizar la revisión de gestión del SGSI	Anualmente
Revisar los resultados de pruebas técnicas y auditorías internas y externas del SGSI	Anualmente
Identificar, administrar y apoyar al personal que opera el SGSI, responsabilidad de su función respectiva	Continuamente

Líder en Gestión de Seguridad de la Información

Responsabilidad	**Frecuencia***
Garantizar que el SGSI cumple con los requisitos del estándar ISO 27001	Continuamente
Informar sobre el rendimiento del Sistema de Gestión de la Seguridad de la Información a la alta gerencia	Anualmente o según sea necesario
Supervisar todas las iniciativas del SGSI de la organización	Continuamente
Supervisar la ejecución del Plan de comunicación o implementación, auditorías internas, revisión de la gerencia y acciones correctivas o mejoras	Continuamente
Mantener y actualizar el modelo de gobernanza y supervisión del SGSI	Continuamente
Preparar, agregar y presentar el material de confirmación necesario para que el Consejo de Gobernanza del SGSI cumpla con sus responsabilidades	Anualmente
Confirmar que las actas de reunión se conservan durante las reuniones del Consejo de Gobernanza del SGSI y se ejecutan todas las medidas	Trimestral
Confirmar que el Consejo de Gobierno del SGSI está informado de los cambios esenciales en el perfil de riesgo de la organización o en los controles clave	Según sea necesario
Revisar, actualizar y confirmar que las políticas del SGSI están al día y cumplen con los objetivos	Anualmente
Supervisar la ejecución de la auditoría interna del SGSI y otras auditorías y pruebas técnicas	Anualmente
Solicitar recursos (es decir, presupuesto, personas, equipos, *software*) necesarios para establecer, operar y mejorar el SGSI	Anualmente
Comunicar la importancia del SGSI y la esencialidad de la mejora continua dentro de su función	Anualmente
Implementar y coordinar la formación y la concientización en materia de seguridad	Anualmente
Garantizar que los nuevos tratamientos de riesgo estén integrados en el SGSI	Anualmente
Administrar los documentos y registros del SGSI	Continuamente

Equipo de Seguridad de la Información

Responsabilidad	**Frecuencia***
Definir, supervisar e informar las métricas de comunicación, implementación, mejora, planes de acción correctiva y medición de la eficacia	Según sea necesario
Hacer seguimiento de todos los incidentes informados a la resolución y compartir oportunidades de aprendizaje con todas las funciones aplicables	Según sea necesario
Identificar los cambios y su impacto en el contexto interno o externo de la organización, las partes interesadas, el alcance, los límites y los objetivos	Continuamente
Rastrear excepciones a las políticas y estándares del SGSI	Según sea necesario

Notificar al Líder de Gestión de Seguridad de la Información sobre cualquier asunto relativo a la competencia del personal que apoya al SGSI	Según sea necesario
Coordinar y gestionar la ejecución de las auditorías internas o externas y el tratamiento de brechas o casos de incumplimientos	Anualmente
Facilitar las evaluaciones de riesgos y las pruebas técnicas	Anualmente
Proporcionar aportes para la revisión de la gerencia	Anualmente
Apoyar al personal que se encuentra implementando y operando controles gestionados y que son responsabilidad de su respectiva función	Continuamente
Implementar medidas correctivas y mejoras para los controles gestionados que son responsabilidad de su respectiva función	Continuamente
Medir e informar sobre la efectividad de los controles del SGSI gestionados y que son responsabilidad de su respectiva función	Anualmente y según sea necesario
Evaluación del riesgo de proveedores y terceros, incluidos los proveedores de servicios en la nube	Anualmente y según sea necesario
Participar en auditorías internas, revisiones de gestión y auditorías externas	Según sea necesario

Empleados, terceros, proveedores, contratistas y consultores

Responsabilidad	**Frecuencia***
Participar activamente en iniciativas del SGSI, como capacitación y concientización del SGSI, auditorías del SGSI, revisiones, entre otros	Continuamente
Eliminar la información en su posesión de acuerdo con la política de la empresa	Según sea necesario
Mantener la estricta confidencialidad e integridad de la información de la empresa y del cliente	Continuamente
Informar sobre incidentes o infracciones de seguridad e incidentes sospechosos a través del proceso de gestión de incidentes	Según sea necesario
Comprender sus responsabilidades en materia de seguridad y seguir la política de seguridad de la información, los objetivos, los requisitos u obligaciones reglamentarias, legales y contractuales	Continuamente
Adherirse a las Políticas, el Código de Ética y los Estándares de Conducta de la empresa	Continuamente

* La frecuencia de cualquier actividad puede realizarse según sea necesario.

Competencia

Para implementar y mantener con éxito el Sistema de Gestión de Seguridad de la Información (SGSI), es crucial garantizar la competencia de las personas implicadas. Esta política pretende garantizar la claridad en la determinación, asignación y mantenimiento de la competencia. anualmente, D3M3NT SA DE CV evaluará el rendimiento y la competencia del personal aplicable frente a las competencias requeridas por el SGSI. Esto se completará definiendo el papel del personal, evaluando el desempeño del trabajo y la competencia durante las revisiones de desempeño y abordando cualquier brecha de competencia.

Definir

Las funciones de la persona se definen a través de descripciones de puestos individuales en los que un gerente de D3M3NT SA DE CV se coordina directamente con Recursos Humanos para desarrollar. Además de las descripciones de puestos, las funciones y responsabilidades pertinentes para la gestión del SGSI se documentan en las secciones 2 y 3 de este documento.

Medida

El personal se mide inicialmente para su competencia a fin de cumplir con los requisitos de la descripción del puesto durante todo el proceso de entrevista, que incluye al gerente o delegado de Recursos Humanos y D3M3NT SA DE CV. Anualmente, D3M3NT SA DE CV realiza una evaluación del desempeño del empleado, dicha evaluación la realizan Recursos Humanos y gerentes directos.

Como parte de la capacitación anual sobre Concienciación sobre la Seguridad de la Información, el equipo de Seguridad de la Información puede emitir pruebas para evaluar el conocimiento y concienciación de una persona sobre temas de seguridad y políticas de la empresa.

Deficiencias en las competencias

Las soluciones para subsanar las deficiencias en materia de competencias serán supervisadas y evaluadas en cuanto a su eficacia por el responsable directo de la persona y documentadas con Recursos Humanos a través de la evaluación del desempeño anual de los empleados. Las soluciones pueden incluir brindar capacitación o tutoría, reasignar tareas o personal, o complementar con contratistas o consultores.

Los empleados que no aprueben la(s) prueba(s) de concientización en materia de seguridad podrán estar obligados a completar la formación de nuevo y a volver a realizar la(s) prueba(s), o a realizar otras actividades de corrección, según sea necesario.

Cobertura ISO 27001

ISO 27001 5.1; 5.3; 6.2; A.6.1.1; A.6.1.2

Historial de versiones

Versión	Fecha	Descripción	Autor	Aprobado por
1.0	25/05/2023	Política inicial	Víctor Acosta	Marco Villanueva
2.0	15/04/2024	Ajustes por traducción	Víctor Acosta	Marco Villanueva

Anexo 27701 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".