Nombre del documento: Procedimiento para Auditorías Internas

Número de documento: 07-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

Esta política delinea el enfoque para realizar auditorías internas para garantizar la conformidad, la efectividad y la mejora continua del SGSI de la organización tanto con los requisitos de la organización como con los estándares ISO/IEC 27001. El propósito de este procedimiento es establecer un marco para planificar, realizar e informar sobre una auditoría interna del del Sistema

de Gestión de Seguridad de la Información ("SGSI") de D3M3NT SA DE CV. Se utiliza una auditoría interna para ayudar a determinar si el SGSI controla los objetivos, los controles y las políticas y procedimientos:

- Cumplir con los requisitos aplicables de la norma ISO/IEC 27001 ("ISO 27001")
- Cumplir con los requisitos de seguridad de la información identificados
- Se implementan, mantienen o tienen oportunidades de mejora de manera efectiva

Alcance

Las auditorías abarcarán todos los elementos del SGSI para todos los recursos de información incluidos en el ámbito de aplicación y los controles aplicables identificados en la Declaración de aplicabilidad.

Declaraciones de política de auditoría interna

Frecuencia y programación de la auditoría:

Las auditorías internas del SGSI se llevarán a cabo en intervalos planificados. Los intervalos exactos y las áreas a auditar se determinarán en función del riesgo, la complejidad y el tamaño de la organización, y se comunicarán anualmente.

Principios de auditoría:

Todas las auditorías internas del SGSI se adherirán a los principios de integridad, presentación justa, debido cuidado profesional, confidencialidad, independencia y un enfoque basado en pruebas.

Gestión del programa de auditoría:

Las auditorías internas se realizarán anualmente e incluirán el alcance completo del SGSI, a menos que se especifique lo contrario.Este programa garantizará una revisión integral de todos los procesos y controles del SGSI dentro de un marco temporal definido.En función de los resultados de las auditorías y de la evolución del panorama de riesgos, se podrán realizar ajustes en el programa.

Competencia del auditor y selección del equipo:

Los auditores, ya sean internos o externos, se seleccionarán en función de su competencia demostrada, sus conocimientos específicos del sector y su comprensión de la seguridad de la información. La organización se compromete a monitorear y evaluar continuamente el desempeño de los auditores para mantener los más altos estándares de auditoría. En situaciones en las que los recursos internos sean inadecuados, podrán nombrarse auditores externos. Estos auditores externos deben estar equipados con suficientes conocimientos sobre el contexto de la organización.

Ejecución de la auditoría y elaboración de informes:

El auditor interno preparará planes de auditoría teniendo en cuenta los resultados de auditorías anteriores y los riesgos identificados. Estos planes guiarán el proceso de auditoría, especificando los criterios, el alcance y los métodos de la misma. Una vez finalizada la auditoría, se elaborará un informe detallado que se presentará a la alta gerencia, en el que se describirán los hallazgos, las no conformidades identificadas y las acciones recomendadas.

Cómo abordar las no conformidades:

Cualquier no conformidad identificada durante el proceso de auditoría se abordará con un plan de acción detallado. Este plan describirá la no conformidad, su(s) causa(s), las acciones correctivas

propuestas y asignará la responsabilidad de implementar estas acciones.

Selección de auditores

El Equipo de Seguridad de la Información puede contratar a un proveedor externo con conocimientos para realizar auditorías internas ISO 27001. La selección de los auditores será revisada y aprobada por la gerencia sénior. El auditor o auditores se evaluarán y seleccionarán en función de su objetividad e imparcialidad en el proceso de auditoría. El auditor o auditores también deben estar capacitados o calificados de otra manera para realizar la auditoría interna de un SGSI. También se debe confirmar que existe una separación adecuada de las tareas al elegir un auditor (es decir, el auditor no ha implementado o no opera ni revisa ninguno de los controles bajo auditoría).

Los auditores se evaluarán en función de su educación y experiencia para validar su competencia.

Recursos

El auditor externo o interno llevará a cabo el proceso de auditoría interna con aportes del Líder de Gestión de Seguridad de la Información y del Equipo de Seguridad de la Información.

Las principales responsabilidades del auditor son las siguientes:

- Planificar las auditorías internas del SGSI, según la frecuencia y el cronograma definidos
- Realizar la auditoría interna según el plan de auditoría y compartir los resultados de la auditoría con el Líder en Seguridad de la Información para su revisión y aprobación
- Garantizar la confidencialidad e integridad de los datos de auditoría y las pruebas de respaldo bajo el control del auditor
- Proporcionar todos los registros de auditoría al Líder en Seguridad de la Información según lo solicitado
- Identificar las medidas correctivas por tomar para cerrar las observaciones o incumplimientos identificados de auditoría, revisar las medidas tomadas para cerrar las deficiencias reportadas y evaluar la efectividad de dichas medidas.

Frecuencia y horario

La frecuencia de la auditoría interna está programada para realizarse anualmente como mínimo. El Consejo de Gobernanza del SGSI determinará si la frecuencia de la auditoría debe aumentar según el número de hallazgos identificados durante la auditoría, la gravedad de los hallazgos de la auditoría anterior y la eficiencia operativa de la realización de la auditoría anualmente.

Criterios de auditoría

Los criterios de auditoría tendrán en cuenta el conjunto definido de políticas y procesos del SGSI, cualquier requisito regulatorio, legal y contractual, ISO 27001 y cualquier norma autorizada adicional, según sea necesario.

Criterios de evaluación

Un incumplimiento ("NC") es una deficiencia con respecto a la norma ISO 2700 que puede tener un efecto adverso para los intereses del SGSI.

- ***NC grave:*** el efecto adverso es inmediato y afecta directamente a la capacidad del SGSI para lograr sus objetivos.
- ***NC leve:*** el efecto puede tener lugar durante un período y no tiene un impacto adverso inmediato en el SGSI.

- ***Cumplimientos:*** los controles están diseñados y funcionan de manera efectiva de acuerdo con los requisitos de ISO 27001.
- ***Oportunidad de mejora ("OFI"):*** una observación puede surgir de una oportunidad de mejora.

Etiquetado alternativo de los hallazgos

D3M3NT SA DE CV se reserva el derecho de aplicar cualquier auditoría interna apropiada de los controles de seguridad de la información a los requisitos de auditoría interna de la norma ISO 27001. Los enfoques de auditoría alternativos pueden identificar los hallazgos utilizando términos alternativos como "Sí/No/Parcial", o "En su lugar/No en su lugar". En los casos en que se aplique una norma o un enfoque alternativo a los requisitos de auditoría interna de la norma ISO 27001, los controles se "mapearán" a los controles de la norma ISO 27001 y el lenguaje de los hallazgos se mapeará a los criterios de evaluación de la norma ISO 27001. Por ejemplo, los controles etiquetados como "Sí" y "En su lugar" pueden ser mapeados a ISO 27001 como "Cumplimiento".

Documentación de auditoría

El auditor interno auditará las políticas y procesos del SGSI, implementará los controles de seguridad de la información y la efectividad del SGSI frente a los requisitos de la norma ISO 27001. El auditor puede recopilar artefactos y documentos como prueba, además de observaciones y entrevistas.

Informes de auditoría

El auditor interno documentará los resultados de la auditoría y las observaciones junto con las pruebas de respaldo. Se producirá un informe final y se compartirá con el Líder en Seguridad de la Información para su revisión y finalización iniciales. Los puntos destacados del interno se comunicarán al Consejo de Gobernanza del SGSI. El informe de auditoría interna completo se proporcionará al Consejo de Gobernanza del SGSI a petición. Un informe de auditoría interna mostrará los resultados de la auditoría, incluidos los incumplimientos y las observaciones.

Retención de registros de auditoría

La prueba recopilada y la documentación preparada como parte de la auditoría interna se protegerán y conservarán de acuerdo con los requisitos definidos en el documento *05-SGSI Proceso para el Control de la Información Documentada*.

Cobertura ISO 27001

ISO 27001 6.2; 9.2

Historial de versiones

Versión	Fecha	Descripción	Autor	Aprobado por
1.0	26/06/2023	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".