Nombre del documento: Proceso de Evaluación y Tratamiento de Riesgos

Número de documento: 04-ISMS

Nombre de la empresa:	D3M3NT SA DE CV
Propietario(s) de la política:	Víctor Acosta
Fecha de entrada en vigencia:	25/05/2023

Objetivo

El objetivo del proceso de evaluación de riesgos y tratamiento de riesgos es evaluar los riesgos para el logro de los objetivos comerciales y de seguridad de la información de D3M3NT SA DE CV.

Política

Los riesgos de seguridad de la información y los tratamientos de los riesgos se gestionarán de acuerdo con la siguiente política de D3M3NT SA DE CV: *Política de Gestión de Riesgos*.

Declaración de aplicabilidad (SoA)

En la Declaración de Aplicabilidad, se documentarán los controles seleccionados del Anexo A de la norma de Seguridad de la Información ISO/IEC 27001 ("ISO 27001") **y los motivos de su selección o exclusión.**

Aprobación de gestión

El Consejo de Gobernanza del SGSI se presentará con la Declaración de Aplicabilidad ("SoA") y se destacará de la evaluación de riesgos según lo determine el Líder en Gestión de Seguridad de la Información. El informe completo de SoA y evaluación de riesgos estará disponible para los miembros del Consejo de Gobernanza del SGSI previa solicitud.

El Consejo de Gobernanza del SGSI puede proporcionar comentarios sobre el proceso de gestión de riesgos a la gerencia durante la revisión anual de la gerencia, o según sea necesario, a exclusivo criterio del Consejo de Gobernanza del SGSI.

A menos que se reciba información explícita del Consejo de Gobernanza del SGSI con respecto a la SoA o evaluación de riesgos, la SoA y todos los planes de tratamiento de riesgos se considerarán aceptables y aprobados por el Consejo de Gobernanza del SGSI después de la revisión de la gerencia.

Mantenimiento y criterios para realizar evaluaciones de riesgos

Se realizará una evaluación de riesgos al menos anualmente, o puede llevarse a cabo en las siguientes circunstancias con diferentes ámbitos, según lo determine el Líder de Gestión de Seguridad de la Información. Además, los riesgos pueden evaluarse en varios niveles de la organización en caso de circunstancias que incluyen:

- Riesgos para el logro de los objetivos del SGSI
- Posibilidad de pérdida de confidencialidad, integridad o disponibilidad de los datos del cliente o de la empresa
- Como parte de proyectos que implican un cambio significativo en la organización, el SGSI o los recursos de la organización
- Desarrollo de *software*, tecnología y cambios organizativos
- Cuando se contratan o cambian periódicamente proveedores externos durante la relación
- En respuesta a cambios externos significativos que afectan a la organización y que pueden invalidar las conclusiones de evaluaciones de riesgo anteriores, por ejemplo, cambios en la legislación pertinente.

Las evaluaciones de riesgos se pueden realizar como resultado de otras circunstancias a exclusivo criterio del Líder en Gestión de Seguridad de la Información o del Consejo de Gobernanza del SGSI.

Cobertura ISO 27001

ISO 27001 6.1.1; 6.1.2; 6.1.3; 8.1

Historial de versiones

Versión	Fecha	Descripción	Autor	Aprobado por
1.0	25/05/2023	Política inicial	Victor 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".