Nombre del documento: Plan de objetivos de Seguridad de la Información

Número de documento: 10-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 libro de trabajo es establecer los Objetivos de Seguridad de la Información y el Plan de Objetivos de Seguridad de la Información de D3M3NT SA DE CV para lograrlos.

Planificación operativa y evaluación del rendimiento

En D3M3NT SA DE CV, comprendemos la importancia de un seguimiento y una medición regulares y precisos de nuestro SGSI. Para alinearnos con nuestro compromiso de mantener los más altos estándares de seguridad de la información, utilizamos la plataforma de gestión de confianza Vanta. Vanta se integra perfectamente con nuestra infraestructura existente, automatizando el proceso de supervisión para garantizar que nuestros controles de seguridad funcionan con eficacia.

Procedimientos de seguimiento y medición con Vanta

Definición de los criterios

Qué monitorear y medir: utilizando Vanta, todos los componentes vitales de nuestro SGSI, incluidos los controles de seguridad, las actividades de gerencia de riesgos y los procesos operativos relacionados, estarán bajo observación automatizada continua.

Metodología: Vanta ofrece metodologías confiables al integrarse con nuestra infraestructura, proporcionando un monitoreo consistente y asegurando que los resultados sean comparables y reproducibles.

Responsabilidad y oportunidad: el Equipo de Seguridad de la Información designado supervisará la plataforma Vanta, asegurando revisiones oportunas de la información generada automáticamente.

Procedimientos de análisis y evaluación

Análisis de resultados: el Equipo de Seguridad de la Información analizará e interpretará regularmente los datos proporcionados por Vanta.

Métodos de evaluación: aprovechando las herramientas analíticas de Vanta, se emplearán métodos estandarizados para evaluaciones rigurosas y válidas.

Responsabilidad y tiempo: el Líder en Gestión de Seguridad de la Información, con el apoyo del Equipo de Seguridad de la Información, analizará y evaluará los hallazgos de Vantara en intervalos predeterminados.

Aspectos de evaluación

Evaluación del desempeño de la seguridad de la información: con los conocimientos de Vanta, esto evalúa si D3M3NT SA DE CV está funcionando como se esperaba, midiendo la efectividad de los procesos de nuestro SGSI.

Evaluación de eficacia del SGSI: Vanta ayuda a determinar si D3M3NT SA DE CV está implementando las medidas de seguridad más adecuadas evaluando en qué medida se cumplen nuestros objetivos de seguridad.

Contribución del equipo a la evidencia

El Equipo de Seguridad de la Información proporcionará actualizaciones periódicas sobre las pruebas, alineándose tanto con los KPI sugeridos por Vanta como con los definidos por D3M3NT SA DE CV. Esta colaboración garantiza que el SGSI siga siendo transparente, rinda cuentas y mejore continuamente.

Objetivos de Seguridad de la Información

Descripción del objetivo	Plan de acción para alcanzar los objetivos	Medidas de eficacia	Recursos necesarios	Responsable	Fecha prevista de finalización
Implementar, mantener y mejorar la Política del Sistema de Gestión de Seguridad de la Información (SGSI) que cumple los requisitos de ISO 27001	Establecer, implementar, mantener y mejorar continuamente un SGSI y someterse a una auditoría de certificación ISO 27001	1. Obtener la certificación ISO 27001	La Junta Directiva Consejo de Gobernanza del SGSI Equipo de Seguridad de la Información	Líder en Gestión de Seguridad de la Información	Cuarto trimestre de2024

Cumplir con las leyes / regulaciones aplicables y las obligaciones contractuales del cliente	Identificar las leyes/regulaciones aplicables y las obligaciones contractuales del cliente. Proporcionar formación y concientización en materia de seguridad. Realizar evaluaciones anuales de riesgos	1. Finalización de la revisión de la gestión 2. Menos de un (1) evento de violación de seguridad notificable 3. Planes de remediación para los riesgos regulatorios y contractuales identificados	Consejo de Gobernanza del SGSI Equipo de Seguridad de la Información	Líder en Gestión de Seguridad de la Información	N/D: en curso
Proteger la confidencialidad de los datos de los clientes	1. Cumplir con los requisitos de control de acceso 2. Identificar y corregir las vulnerabilidades de alto riesgo 3. Realizar una evaluación de riesgos 4. Realizar pruebas de penetración en la red de producción y en la aplicación 5. Realizar análisis de vulnerabilidad en los sistemas de producción al menos una vez cada 3 meses siempre y cuando se tenga alguna aplicación en producción. 6. Crear planes para remediar las vulnerabilidades de alto riesgo en un plazo de 60 días	1. Menos de un (1) hallazgo en revisiones trimestrales de acceso a los sistemas de producción 2. Planes de remediación para vulnerabilidades de alto riesgo 3. Finalización oportuna de los planes de remediación	Consejo de Gobernanza del SGSI Equipo de Seguridad de la Información	Líder en Gestión de Seguridad de la Información	N/D: en curso
Reducción de datos	1. Solo recopile la PII necesaria para un propósito comercial. 2. Garantice que la recopilación y el procesamiento de la PII se limitan a lo que se informa en los Principios de la PII, a lo que se acepta o a lo que se ajusta a un propósito comercial legítimo.	1. El 100 % de las SAR se responden y cierran dentro de los plazos correspondientes. 2. 0 quejas ante las autoridades de datos 3. 0 violaciones de datos de la PII	Consejo de Gestión de S&PMS Equipo de seguridad de la Información	Líder en Gestión de Seguridad de la Información	N/D: en curso

	3. Elimine la PII de forma segura cuando ya no sea necesario. 4. Utilice los siguientes procesos de desidentificación: seudonimización.				

Métricas y criterios de medición

Política/Procedimiento/Control	**Control del SGSI (2013)**	**Detalle de la medición**	**Quién reúne métricas**	**Quién recibe métricas y frecuencia**	**Criterios**
Gestión técnica de vulnerabilidades	A.12.6.1	Vulnerabilidades detectadas y reparadas	Equipo de operaciones/Proveedor de servicios	Consejo de Gobernanza del SGSI - mensualmente	Las vulnerabilidades críticas y altas se solucionan dentro de los plazos del SLA
Respuesta del usuario a los intentos de phishing	A.7.2.2	Respuestas de los usuarios a las pruebas de phishing	Equipos de operaciones	Consejo de Gobernanza de CISO y SGSI - trimestral	1. Número de usuarios que pasan las pruebas de phishing 2. Los usuarios que no pasan las pruebas reciben capacitación de concientización
Se reportan y administran equipos perdidos y robados	A.16.1.2 A.16.1.5	1. Los usuarios informan adecuadamente los incidentes 2. La respuesta a los incidentes es adecuada y de acuerdo con las políticas y los procesos	Administradores de sistemas	Consejo de Gobernanza de CISO y SGSI - trimestral	El reporte y la respuesta son oportunos y se ajustan a la política y el proceso
Aplicación de parches del sistema	A.12.6.1	Número de sistemas parchados/sin parchar Tiempo de parche (TTP)	Administradores de sistemas	Consejo de Gobernanza de CISO y SGSI - trimestral	Los sistemas con vulnerabilidades críticas o altas se reparan de acuerdo con los plazos de SLA.
Política/Procedimiento/Control	**Control SGSI (2022)**	**Detalle de la medición**	**Quién reúne métricas**	**Quién recibe métricas y frecuencia**	**Criterios**
Gestión técnica de vulnerabilidades	A.8.8	Vulnerabilidades detectadas y reparadas	Equipo de operaciones/Proveedor de servicios	Consejo de Gobernanza del SGSI - mensualmente	Las vulnerabilidades críticas y altas se solucionan

					dentro de los plazos del SLA
Respuesta del usuario a los intentos de phishing	A.6.3	Respuestas de los usuarios a las pruebas de phishing	Equipos de operaciones	Consejo de Gobernanza de CISO y SGSI, trimestral	1. Número de usuarios que pasan las pruebas de phishing 2. Los usuarios que no pasan las pruebas reciben capacitación de concientización
Se reportan y administran equipos perdidos y robados	A.6.8 A.5.26	1. Los usuarios informan adecuadamente los incidentes 2. La respuesta a los incidentes es adecuada y de acuerdo con las políticas y los procesos	Administradores de sistemas	Consejo de Gobernanza de CISO y SGSI, trimestral	El reporte y la respuesta son oportunos y se ajustan a la política y el proceso
Aplicación de parches del sistema	A.8.8	Número de sistemas parchados/sin parchar Tiempo de parche (TTP)	Administradores de sistemas	Consejo de Gobernanza de CISO y SGSI, trimestral	Los sistemas con vulnerabilidades críticas o altas se reparan de acuerdo con los plazos de SLA.

Cobertura ISO 27001

ISO 27001 10.2

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".