Política de gestión de terceros

Propietario de la política: Jonathan Spano

Fecha de entrada en vigencia: 09/04/2024

Objetivo

Para garantizar la protección de los datos y recursos de la organización que se comparten, son accesibles o están gestionados por proveedores, incluidos proveedores externos u organizaciones de terceros, como proveedores de servicios, proveedores y clientes, y para mantener un nivel acordado de seguridad de la información y prestación de servicios de conformidad con los acuerdos con los proveedores.

En este documento, se describe una línea base de controles de seguridad que D3M3NT SA DE CV espera que los socios y otras empresas externas cumplan al interactuar con los datos confidenciales de D3M3NT SA DE CV.

Alcance

Todos los datos y sistemas de información propiedad o utilizados por D3M3NT SA DE CV que son críticos para el negocio o procesan, almacenan o transmiten datos confidenciales. Esta política se aplica a todos los empleados de D3M3NT SA DE CV y a todas las partes externas, incluidos, entre otros, consultores, contratistas, socios comerciales, vendedores, proveedores, socios, proveedores de servicios subcontratados de D3M3NT SA DE CV y otras entidades de terceros con acceso a datos, sistemas, redes, o recursos del sistema de D3M3NT SA DE CV.

Política

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los recursos de la organización se acordarán con el proveedor y se documentarán.

Para todos los proveedores de servicios que puedan acceder a los datos, sistemas o redes confidenciales de D3M3NT SA DE CV, se deberá llevar a cabo la correspondiente diligencia debida antes de proveer acceso o participar en actividades de procesamiento. Se conservará la información relacionada con los requisitos normativos o de certificación que gestiona o afecta cada proveedor de servicios, y que administra D3M3NT SA DE CV según sea necesario. Los requisitos normativos o de certificación aplicables pueden incluir lSO 27001, SOC 2, PCI DSS, CCPA, RGPD u otros marcos, normas de cumplimiento o reglamentos.

Seguridad de la lnformación en relaciones con terceros

Abordar la seguridad en los acuerdos

Los requisitos relevantes de seguridad de la información se establecerán y acordarán con cada proveedor que pueda acceder, procesar, almacenar, transmitir o afectar la seguridad de los datos y sistemas confidenciales, o proporcionar componentes de infraestructura de TI físicos o virtuales para D3M3NT SA DE CV.

Con todos los proveedores de servicios que puedan acceder a los sistemas de producción de D3M3NT SA DE CV, o que puedan afectar a la seguridad del entorno de producción de D3M3NT SA DE CV, se mantendrán acuerdos por escrito que incluyan la aceptación por parte del proveedor de servicios de sus responsabilidades en cuanto a la confidencialidad de los datos de la empresa y del cliente, y cualquier compromiso relativo a los controles de integridad, disponibilidad o privacidad que manejan para cumplir con las normas y requisitos que D3M3NT SA DE CV ha establecido de conformidad con el programa de seguridad de la información o cualquier marco pertinente de D3M3NT SA DE CV.

Cadena de suministro de tecnología

D3M3NT SA DE CV considerará y evaluará el riesgo asociado con los proveedores y la cadena de suministro de tecnología. Si está garantizado, los acuerdos con los proveedores incluirán requisitos para abordar los riesgos de seguridad de la información relevantes asociados con los servicios de tecnología de la información, las comunicaciones y la cadena de suministro de productos.

Gestión de prestación de servicios de terceros

Monitoreo y revisión de servicios de terceros

D3M3NT SA DE CV deberá monitorear, revisar y auditar regularmente la prestación de servicios del proveedor. La seguridad del proveedor y el desempeño de la prestación de servicios se revisarán, al menos, una vez al año.

Gestión de cambios en los servicios de terceros

Los cambios en la prestación de servicios por parte de los proveedores, incluidos los cambios en los acuerdos, servicios, tecnología, políticas, procedimientos o controles, se gestionarán, teniendo en cuenta la importancia de la información comercial, los sistemas y los procesos involucrados. D3M3NT SA DE CV evaluará el riesgo de cualquier cambio material realizado por los proveedores y hará las modificaciones correctas a los acuerdos y servicios según corresponda.

Gestión de riesgos de terceros

D3M3NT SA DE CV garantizará que los riesgos potenciales planteados al compartir datos confidenciales o al proporcionar acceso a los sistemas de la empresa se identifiquen, documenten y aborden conforme esta política. La gestión de riesgos juega un papel integral en la gobernanza y gestión de la organización a nivel estratégico y operativo. El objetivo de una política de seguridad de socios y terceros es garantizar que las asociaciones y los servicios alcancen los objetivos de su plan de negocio, y que sean consistentes con los requisitos de D3M3NT SA DE CV para la seguridad de la información.

D3M3NT SA DE CV no compartirá ni transmitirá datos confidenciales a terceros sin realizar primero una evaluación de riesgos de terceros y otorgar plenamente un contrato escrito, una declaración de servicios o trabajo, o un acuerdo de servicio que describa los niveles de servicio esperados y cualquier requisito específico de seguridad de la información.

Seguridad de la información para el uso de servicios en la nube

Esta sección describe los parámetros fundamentales para la gestión y mitigación de los riesgos relacionados con el uso de los servicios en la nube.

Responsabilidades y gestión de riesgos:

- Las funciones y responsabilidades relacionadas con el uso y la gestión de los servicios en la nube pueden consultarse en la *Política de funciones y responsabilidades*.
- Los riesgos para la seguridad de la información asociados al uso de servicios en la nube se gestionarán de acuerdo con esta política y con la *Política de gestión de riesgos*.

Requisitos y control de la seguridad:

- La empresa será responsable de todos los controles del cliente definidos en las matrices de responsabilidad de los proveedores de servicios en la nube.

Selección del servicio y alcance de uso:

- Las revisiones de los acuerdos de servicios en la nube para los proveedores de alto riesgo inherente se realizarán anualmente para garantizar que se ajustan a los requisitos de la empresa.

Gestión de incidentes:

- Los incidentes de seguridad de la información relacionados con los servicios en la nube se gestionarán de acuerdo con el Plan de respuesta a incidentes.

Revisión del servicio y estrategia de salida:

- Los riesgos relacionados con la salida y el bloqueo del proveedor deben evaluarse antes de la adquisición como parte de la evaluación de la seguridad del proveedor.

Acuerdo entre proveedor y cliente:

- Los acuerdos con los proveedores de servicios en la nube especificarán protecciones para los datos de D3M3NT SA DE CVy la disponibilidad del servicio, aunque puedan estar predefinidos y no ser negociables.
- Siempre que sea posible, D3M3NT SA DE CV buscará notificaciones anticipadas de proveedores sobre cambios sustanciales en la prestación de servicios, incluidos cambios en la infraestructura técnica, la ubicación del almacenamiento de datos o el uso de subcontratistas.

Gestión y garantía continuas:

- La información relativa a cómo obtener y utilizar las capacidades de seguridad de la información proporcionadas por el proveedor de servicios en la nube debe evaluarse como parte de la revisión del proveedor en el momento de la adquisición.

Estándares de seguridad de terceros

Todos los terceros deben mantener controles organizacionales y técnicos razonables según lo evaluado por D3M3NT SA DE CV.

Para la evaluación de terceros que reciben, procesan o almacenan datos confidenciales o acceden a los recursos de D3M3NT SA DE CVse considerarán los siguientes controles según corresponda en función del servicio prestado y la confidencialidad de los datos almacenados, procesados o intercambiados.

Política de seguridad de la información

Los terceros mantienen políticas de seguridad de la información respaldadas por su gerencia ejecutiva, que se revisan regularmente.

Evaluación y tratamiento de riesgos

Los terceros mantienen programas que evalúan y gestionan los riesgos de la información y la tecnología.

Seguridad de las operaciones

Los terceros implementan prácticas y procedimientos por razones comerciales diseñados, según corresponda, para mantener la seguridad de las operaciones. Las protecciones pueden incluir lo siguiente:

- Pruebas técnicas
- Protección contra *software* malicioso
- Protección y gestión de la red
- Gestión técnica de vulnerabilidades
- Registro y monitoreo
- Respuesta ante incidentes
- Planificación de la continuidad del negocio

Control de acceso

Los terceros mantienen un programa técnico de control de acceso.

Desarrollo seguro de sistemas

Los terceros mantienen un programa de desarrollo seguro de acuerdo con las mejores prácticas de desarrollo de *software* y los sistemas de la industria, que incluyen la evaluación de riesgos, la gestión de cambios formales, los estándares de código, la revisión de código y las pruebas.

Seguridad física y ambiental

Si los terceros almacenan o procesan datos confidenciales, sus controles de seguridad física y ambiental deben cumplir con los requisitos de la Política de Seguridad Física de D3M3NT SA DE CV.

Recursos Humanos

Los terceros mantienen políticas y procesos de recursos humanos que incluyen verificaciones de antecedentes penales para cualquier empleado o contratista que acceda a la información confidencial de D3M3NT SA DE CV.

Cumplimiento y ordenamiento jurídico

D3M3NT SA DE CV tendrá en cuenta todas las regulaciones y leyes aplicables al evaluar a los proveedores y terceros que accederán, almacenarán, procesarán o transmitirán datos confidenciales de D3M3NT SA DE CV. Las evaluaciones de terceros deben tener en cuenta los siguientes criterios:

- Protección de datos de clientes, registros organizativos y retención y disposición de registros
- Privacidad de la información de identificación personal (PII)

Excepciones

Las solicitudes de excepción a esta Política deben enviarse al director de operaciones financieras para su aprobación.

Infracciones y cumplimiento

Cualquier infracción conocida de esta política debe ser reportada al director de operaciones financieras. Las infracciones de esta política pueden dar lugar a la cancelación o suspensión inmediata de los privilegios del sistema y la red o a medidas disciplinarias de acuerdo con los procesos de la empresa, incluido el despido.

Versión	Fecha	Descripción	Autor	Aprobado por
1.0	25/03/2023	PRIMERA REVISION	VICTOR ACOSTA	MARCO VILLANUEVA
1.1	09/04/2024	AJUSTE POR TRADUCCIÓN	VICTOR ACOSTA	MARCO VILLANUEVA