D1 S.A.S

Política de Seguridad de la Información para Proveedores

Versión 1.1

31/DICIEMBRE/2024

Tabla de Contenido

1. OBJETIVO

Conforme al marco de Seguridad de la Información definido para D1 S.A.S por medio de la presente política se busca asegurar que toda la información de la compañía, en poder de proveedores o contratistas, independiente de su formato o presentación debe ser protegida de acceso no autorizado, contar con procedimientos para la transmisión, procesamiento, devolución y destrucción segura de la información, una vez concluya su vida útil o la finalización del contrato.

2. ALCANCE

Para reducir los riesgos de pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información, todo contrato firmado con empresas o personas externas que involucre el manejo de información de D1 SAS, debe cumplir plenamente con la presente política y la Política de Seguridad de la Información como base para cualquier negociación con terceros.

3. LINEAMIENTOS, REQUISITOS Y CONDICIONES DE LA POLÍTICA

D1 SAS desarrolla esta política con los siguientes lineamientos:

3.1. Obligaciones del Contratista:

3.1.1. El CONTRATISTA protegerá y garantizará la Confidencialidad, Integridad y Disponibilidad de la Información, sin importar el medio, formato o presentación en que sea creada, procesada, almacenada o utilizada manteniendo un inventario actualizado y vigente del mismo.

3.1.2. EL CONTRATISTA debe establecer formalmente los responsables de los activos de información que D1 SAS le suministró para el cumplimiento de las labores contratadas.

3.1.3. En todo momento EL CONTRATISTA debe garantizar que las contraseñas y mecanismos de autenticación estén debidamente custodiados. Así mismo, los usuarios de los recursos informáticos no deben compartir su cuenta de usuario, contraseña o cualquier mecanismo otorgado para su identificación y autenticación.

3.1.4. En todo momento EL CONTRATISTA debe garantizar el cumplimiento de la complejidad de las contraseñas, de acuerdo con lo definido por D1 SAS:

- La contraseña está compuesta por mínimo 10 caracteres con un grado de complejidad de al menos 4 de estos grupos:
  - Letras mayúsculas (de la A - Z)
  - Letras minúsculas (de la a - z)
  - Números (del 0 al 9)
  - Símbolos (caracteres no alfanuméricos) ! @ # $ % & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
- Vigencia de 42 días.
- La contraseña se bloqueará después de 3 intentos y reactivándose después de 15 minutos.

3.1.5. EL CONTRATISTA será responsable por el uso que se dé a los usuarios y permisos asignados. En todo caso, EL CONTRATISTA se abstendrá de obtener, modificar, acceder y en general ejercer cualquier acto sobre la información, sin la previa autorización expresa y escrita por D1 SAS.

3.1.6. Los permisos de acceso a la infraestructura de D1 SAS y los recursos informáticos aprobados y asignados a EL CONTRATISTA deben ser utilizados únicamente para el cumplimiento de las actividades previamente definidas en el contrato.

3.1.7. A menos que en el contrato se apruebe expresamente, EL CONTRATISTA no está autorizado para participar en las redes sociales en nombre de D1 SAS, así mismo, la publicación de información en medios masivos deberá ser autorizada por el responsable de la estrategia de mercadeo de D1 SAS cumpliendo con los requerimientos legales que faculten su utilización.

3.1.8. EL CONTRATISTA se abstendrá de instalar software en los equipos de D1 SAS, sin la previa autorización por parte de éste. EL CONTRATISTA garantizará a D1 SAS que ha obtenido las licencias y autorizaciones respectivas de los propietarios del software que pretenda instalar e instale con la autorización del D1 SAS en sus equipos.

3.1.9. EL CONTRATISTA se abstendrá de enviar y revelar Información de D1 SAS a terceros, sin la previa autorización expresa y escrita por parte del D1 SAS.

3.1.10. Toda conexión externa a otras redes públicas o privadas que EL CONTRATISTA pretenda realizar desde y hacia las instalaciones de D1 SAS, deberá ser aprobada de manera previa, expresa y por escrito por parte del D1 SAS.

3.1.11. EL CONTRATISTA deberá garantizar la transmisión y transporte seguro de la Información a través de redes y dispositivos mediante el uso de mecanismos, que garanticen la confidencialidad, integridad, disponibilidad y privacidad de la Información.

3.1.12. EL CONTRATISTA mantendrá las áreas en donde se encuentre la Información y recursos informáticos, con las protecciones necesarias, controles de seguridad ambientales y acceso físico adecuados, de modo tal que se garantice la protección y conservación de la misma.

3.1.13. Una vez terminado el contrato o por solicitud de D1 SAS, EL CONTRATISTA identificará la información de D1 SAS que, con ocasión de la relación precontractual y contractual, ha sido copiada, procesada, almacenada o transmitida, la cual deberá ser objeto de eliminación o destrucción.

3.1.14. EL CONTRATISTA deberá reportar ante el líder de área responsable del contratista y la mesa de servicio (mat@d1.com.co) los incidentes de Seguridad de la Información y Ciberseguridad que comprometan o tengan una afectación en la información y operación de D1 SAS.

3.1.15. En caso de que EL CONTRATISTA requiera subcontratar con un tercero para realizar parcial o completamente actividades propias del contrato, EL CONTRATISTA deberá garantizar que las medidas de seguridad y ciberseguridad definidas por D1 SAS se mantengan durante la transmisión, procesamiento y borrado seguro de la información y datos personales, así mismo, EL CONTRATISTA deberá notificar la presente situación ante el área responsable del CONTRATISTA en D1 SAS.

Los subcontratistas quedarán obligados sólo ante EL CONTRATISTA principal, quien asumirá la responsabilidad de la ejecución del contrato, protección de los activos de información y aplicación de las políticas frente a D1 SAS.

3.1.16. En el evento en que EL CONTRATISTA almacene Información dentro de sus recursos informáticos, en la nube o de terceros, se obliga a destruir de manera segura la Información suministrada por D1 SAS, cuando el recurso vaya a ser cambiado, desechado o enviado a mantenimiento. Igualmente, EL CONTRATISTA se obliga a destruir la Información independiente del tipo del formato y el repositorio en el que se encuentre almacenada, a la finalización del contrato al que se anexa el presente documento, salvo que dentro del contrato se haya pactado un término diferente o que por disposición legal EL CONTRATISTA esté obligado a conservarla por un término mayor.

3.1.17. Los CONTRATISTAS que asignen personal para desempeñar funciones en D1 S.A.S. tienen la responsabilidad de informar oportunamente al mat@d1.com.co y al área responsable del contratista el retiro o cambio del recurso con el fin de retirar los accesos a los servicios de tecnología. Cualquier evento que durante el retiro de la persona y el retiro del acceso a la plataforma será responsabilidad del CONTRATISTA.

3.1.18. El transporte y almacenamiento de información se debe realizar por canales y protocolos de seguridad definidos por D1 S.A.S.

3.1.19. Todo CONTRATISTA que administre (Genere, almacene, transmita) información de D1 SAS, debe contar con planes de contingencia y recuperación de información claros y que aseguren una continuidad de los servicios según los ANS definidos.

3.1.20. Los CONTRATISTAS deben tener definidos formalmente políticas y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información de D1 SAS, protegiéndola de la divulgación, el uso, la alteración o la destrucción accidentales, no autorizados o indebidos.

3.2. Obligaciones de Contratistas Tecnológicos

Para aquellos contratistas que presten servicios tecnológicos donde manipulen información o activos tecnológicos que contengan datos, adicional a las obligaciones expuestas en la sección 3.1, deben cumplir con los siguientes lineamientos:

3.2.1. Los CONTRATISTAS deben contar con un programa de seguridad que esté alienado con las prácticas dispuestas por marcos de referencia (p.a. ISO27001, NIST, entre otros).

3.2.2. EL CONTRATISTA debe elaborar un programa de capacitación, concientización y creación de cultura organizacional en Seguridad de la Información y Ciberseguridad, dirigido a sus empleados y proveedores para conocimiento de sus deberes, responsabilidades y de las consecuencias administrativas, legales y penales relacionados con el incumplimiento de los lineamientos entregados por D1 SAS, las disposiciones legales y regulatorias.

3.2.3. EL CONTRATISTA debe contar con planes detallados de continuidad para responderle a D1 SAS de manera oportuna y eficiente frente a fallas e interrupciones o eventos imprevistos relacionados entre otros, con fluido eléctrico, software, hardware, ataques cibernéticos, telecomunicaciones, entre otros, que afecten tanto la ejecución óptima de los servicios contratados por D1 SAS como el normal desarrollo del objeto social del CONTRATISTA.

Como consecuencia de lo anterior, EL CONTRATISTA debe tener definido, documentado, implementado, probado y mantendrá durante la vigencia del contrato, procesos para administrar la continuidad del negocio, procesos de seguridad de la información y Ciberseguridad.

3.2.4. EL CONTRATISTA debe permitir y brindar el acompañamiento necesario para la ejecución de auditorías durante la ejecución del contrato, con el fin de verificar el cumplimiento de los procesos que EL CONTRATISTA ejecute para prevenir, detectar, responder, recuperar la información. Así mismo debe permitir la ejecución de pruebas de vulnerabilidades en las plataformas donde se encuentra alojada o soportando la información de D1 SAS.

3.2.5. En el evento en que el servicio prestado por EL CONTRATISTA se refiera a la venta, desarrollo o licenciamiento de software, deberá asegurar a D1 SAS que al software objeto de venta, desarrollo o licenciamiento, fueron aplicados principios y buenas prácticas de seguridad, durante las etapas del ciclo de vida del desarrollo seguro de software, así como mecanismos de identificación y autenticación de usuarios. Cuando el software sea desarrollado para cumplir con requerimientos específicos del D1 SAS se deberán asignar los derechos de propiedad intelectual a D1 SAS.

3.2.6. Los contratistas que presten soluciones de inteligencia artificial deben asegurar que estas soluciones cumplan con todas las leyes y regulaciones relevantes en materia de seguridad de la información y protección de datos personales y que estás no permitan ningún tipo de fijación de precios o prácticas anticompetitivas con los demás clientes que tenga el proveedor o contratista

3.2.7. Los proveedores que presten soluciones de Inteligencia Artificial deben garantizar la confidencialidad de toda la información y datos a los que tengan acceso, implementando medidas de seguridad adecuadas.

3.2.8. Los proveedores que presten servicios de inteligencia artificial deben obtener y mantener certificaciones ISO 27001, informes SOC 2 y/o SOC 3, que validen la eficacia de sus controles internos en relación con la confidencialidad, disponibilidad e integridad de la información.

3.3. Responsabilidades de los colaboradores con función de contratar.

Los colaboradores encargados de seleccionar los Contratistas deben asegurar el cumplimiento de los siguientes lineamientos:

3.3.1. Informarse, entender los cambios que se hagan a la presente política, así como comunicárselos a los respectivos CONTRATISTAS.

3.3.2. Para todas las contrataciones donde existe relación de componentes tecnológicos y de transferencia de información de D1 en cualquiera de sus formas (digital o física), se debe contemplar la presente política y el involucramiento de la Dirección de Tecnología y al CISO o quien este delegue.

3.3.3. Cualquier incumplimiento a la presente política por parte del CONTRATISTA será el área responsable del CONTRATISTA quien abrirá un evento o incidente de seguridad según sea el caso y comunicando a la mesa de servicio (mat@d1.com.co) y al CISO la situación, para generar las acciones correspondientes y mitigar el riesgo presentado.

3.3.4. Se deben incluir cláusulas de seguridad de la información y Ciberseguridad en los contratos firmados con CONRTATISTAS que tengan o puedan llegar a tener riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información en D1. Estas cláusulas deben estar relacionadas con:

- Confidencialidad de la información.
- Transmisión de Datos (Si aplica).
- Contar con un Plan de Continuidad del Negocio, el cual debe ser probado periódicamente.
- Cumplimiento a propiedad intelectual.
- Conocimiento y cumplimiento a todas las regulaciones nacionales que impacten a D1 SAS.
- Cumplimiento a la presente política de información para proveedores.

4. ROLES

4.1. Área Responsable del CONTRATISTA

Todos los Responsables del Proyecto D1 SAS, son los encargados de compartirles los cambios de la presente Política, así como reportar los incidentes de seguridad que se presente.

La presente política, la Política de Seguridad de la Información y el Manual de Seguridad de la Información son de obligatorio cumplimiento.

4.2. Contratistas:

Persona natural o jurídica que abastece a D1 SAS de cualquier producto o servicio que son necesarios para cumplir con los objetivos del negocio. deben cumplir estrictamente la presente política, la Política de Seguridad de la Información y el Manual de Seguridad de la Información.

4.3. Gerente de Riesgos de Ciberseguridad (CISO)

Será el encargado de mantener, actualizar, divulgar y capacitar a todos los interesados frente a la presente política y el Manual de Seguridad de la Información.

4.4. Área Legal:

Será el encargado de incluir clausulas dentro de los contratos que asegure el conocimiento y el cumplimiento de la presente política.

5. ENTRADA EN VIGOR

La presente política entrará en vigor a partir de la fecha de aprobación y divulgación vía correo electrónico.

6. CONTROL DE VERSIONES DEL DOCUMENTO Y RESPONSABLES

Versión	Descripción de la Modificación	Fecha
1.0	*Elaboración inicial del Documento*	*25/09/2023*
1.1	*Inclusión numerales 3.2.6, 3.2.7 y 3.2.8, los cuales hacen referencia al cumplimiento de seguridad en los servicios que involucren servicios de IA*	*31/12/2024*

Versión	Elaboró	Revisó	Aprobó
1.0	Gerente de Riesgos de Ciberseguridad	• Director de Control y Cumplimiento • Alta Gerencia	• Comité de Seguridad y Ciberseguridad • Alta Gerencia
1.1	Gerente de Riesgos de Ciberseguridad	• Director de Control y Cumplimiento • Director de tecnología nacional	• Director de Control y Cumplimiento • Director de tecnología nacional • Comité de Seguridad y Ciberseguridad

7. GLOSARIO Y TÉRMINOS

Política: Es la línea de acción de una organización para la mejora de sus procesos internos.

Activo de Información: es un bien o un servicio con capacidades funcionales y operativas que tiene valor significativo para la compañía y que se debe proteger.

Amenaza: Son situaciones que desencadenan un evento o incidente en la compañía, realizando un daño material o pérdidas inmateriales de sus activos de información.

Área responsable del CONTRATISTA: Encargados de compartirles los cambios de la presente Política a los Contratistas, así como reportar los incidentes de seguridad que se presenten con el Contratista.

Aplicaciones: Es todo el software que se utiliza para la gestión de la información.

Brecha de seguridad: Es un evento que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos que pueden causar un impacto en la operación de la compañía.

CISO: "*Chief Information Security Officer*" es la autoridad que lidera la seguridad de la información, siendo su principal función la de garantizar la protección de los activos de información de la compañía.

Ciberseguridad: Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos proveniente de internet.

Colaborador: Es aquella persona que cuenta con acceso a los diferentes sistemas tecnológicos y a la información almacenada en ellos. Se considera como colaborador a todos los empleados, contratistas, estudiantes en práctica que hagan uso de la información y recursos tecnológicos propiedad de D1 S.A.S.

Contratista: Persona natural o jurídica que abastece a D1 SAS de cualquier producto o servicio que son necesarios para cumplir con los objetivos del negocio.

Confidencialidad: Característica y/o propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Confidencial: Fuente de información que maneja los empleados de la compañía que no puede ser revelada a ninguna persona sin respectiva autorización.

Credencial: Es la adecuada combinación de datos que permiten el acceso a la información según los niveles de permisos definidos por el responsable de la información. Las credenciales se dan mediante un usuario, contraseña o la implementación de dispositivos biométricos o aplicaciones diseñadas para tal fin.

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen.

Disponibilidad: Es la propiedad mediante la que se garantiza el acceso autorizado a la información en el momento en que se requiera.

Evento: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha o incumplimiento de la Política de Seguridad de la Información y Ciberseguridad o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Incidente: Evento único o serie de eventos inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Es un conjunto de datos acerca de un hecho, fenómeno o situación que se encuentran organizados y analizados, que en un contexto determinado tienen significado y valor al incrementar o facilitar el conocimiento.

Integridad: Es la propiedad que mantiene con exactitud la información una vez que ella fue organizada, evitando su alteración, o manipulación.

Infraestructura: Conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo y operación de D1 S.A.S.

Marcos de Referencia: Fuente escrita de principios, puntos de referencia o perspectivas que se utilizan como base para medir, comparar o analizar algo.

Plataforma Tecnológica: Conjunto de sistemas, aplicaciones, arquitectura de hardware que interactúan en procesamiento y que soportan las operaciones de la compañía.

Privacidad: Principio encaminado a que la información del negocio y la información personal de los COLABORADORES de D1 SAS sea utilizada dentro de los propósitos para los cuales fue obtenida y no sea divulgada sin autorización.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Responsable: Valor o cualidad de todo ser humano, que cumple con sus obligaciones al hacer, decir u ofrecer algo con plena conciencia de sus actos.

Tecnología: Conjunto de técnicas, conocimientos y procesos, que sirven para el diseño y construcción de objetos para satisfacer un requerimiento de la compañía.

Usuario: Credencial intransferible otorgada a algún colaborador para acceder a los diferentes sistemas tecnológicos y a la información almacenada en los recursos tecnológicos propiedad de **D1 S.A.S.**

Usuario Privilegiado: Acceso de confianza sobre la plataforma tecnológica con capacidad de crear, modificar y eliminar objetos en los sistemas de información de la compañía.