

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Control de Versiones

Versión	Fecha de Elaboración	Responsable de elaboración	Fecha de Aprobación	Responsable de aprobación	Modificaciones
1	Enero 2026	Yuriko Melchor/ Director General	Enero 2026	Yuriko Melchor/ Director General	Definición de la política en su primera versión

Contenido

1.	Objetivo	3
2.	Alcance	3
3.	Glosario	3
4.	Política	6
4.1.	Los principios de protección de los datos personales	7
4.2.	Tratamiento de los datos personales	8
4.2.1.	Obtención	8
4.2.2.	Resguardo	8
4.2.3.	Bloqueo	9
4.2.4.	Supresión	9
4.2.5.	Transferencia y remisión	9
4.2.6.	Vulneración	9
4.3.	Ejercicio de los derechos ARCO	11
4.4.	Del aviso de privacidad	12

1. Objetivo

Establecer las pautas de comportamiento para el correcto tratamiento y protección de los datos personales y el mantenimiento de la seguridad de la información, asegurando el cumplimiento de los principios reguladores y el respeto a los derechos de los titulares de dichos datos.

2. Alcance

Esta Política es aplicable a todo el personal de Sustentandem, así como a proveedores, prestadores de servicios, contratistas, terceros que actúen en nombre de Sustentandem y cualquier tercero con el que éste tenga alguna relación de negocios en la medida en que les sea aplicable.

3. Glosario

Aviso de privacidad: Documento físico, electrónico o en cualquier medio que es proporcionado por el responsable del tratamiento de los datos personales, por medio del cual se informan los datos a tratar, las finalidades del tratamiento y los medios para el ejercicio de sus derechos.

Bloqueo: Identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Consentimiento: Manifestación de la voluntad del titular de los datos personales mediante la cual se efectúa el tratamiento de los mismos.

Consentimiento expreso: El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Consentimiento tácito: Habrá consentimiento tácito cuando se ponga a disposición del titular el aviso de privacidad correspondiente y éste no manifieste su oposición.

Copia no autorizada: Cuando el titular o personal de custodia no otorgó consentimiento para la generación de una copia de la información que contiene los datos personales, ya sea que se encuentre en la base de datos o en cualquier otro soporte documental.

Daño, alteración o modificación no autorizada: Cuando los datos personales sufren una transformación de manera intencional o no intencional, que compromete la pérdida de calidad e integridad derivada de acciones realizadas por una persona, sin la autorización del titular.

Datos personales: Cualquier información que identifique o haga identificable a una determinada persona física.

Datos personales sensibles: Aquellos datos personales que se refieran a la esfera más íntima del titular y que puedan dar origen a una discriminación.

Derechos ARCO: Son los derechos de acceso, rectificación, cancelación y oposición que tiene el titular respecto de sus datos personales.

Derecho de acceso: Derecho a conocer los datos personales que se recaban, así como las finalidades y condiciones de uso.

Derecho de rectificación: Derecho a solicitar la corrección de la información inexacta o incompleta o la actualización de la información que se posee.

Derecho de cancelación: Derecho a solicitar la eliminación de la información de los registros o bases de datos cuando se considere que no se han cumplido los principios, deberes y obligaciones adquiridas.

Derecho de oposición: Derecho de inconformarse con el uso de sus datos para fines específicos.

Destrucción: Cuando los datos ya no existen, o existen en una forma que ya no es posible utilizarlos, sin que haya mediado autorización de por medio.

Divulgación o revelación no autorizada: Cuando la información que contiene datos personales es divulgada o revelada por personas internas o externas a la organización, sin previa autorización o fuera de los tiempos establecidos en el procedimiento.

Documento de seguridad: Documento que describe las medidas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Encargado: Persona designada por el responsable para el tratamiento de los datos personales.

Extravío: Cuando el encargado, por un descuido, desconoce u olvida donde se encuentra el activo que contiene la información provocando la pérdida de los datos personales.

Incidente de seguridad: Cuando se identifica o reporta una alerta de seguridad que involucra información comprometida o daño a los activos. Por ejemplo: desastres

naturales, inestabilidad social, daño físico, falla de la infraestructura, falla técnica, software malicioso, ataques técnicos, información dañada, interceptación de información y divulgación de contenido perjudicial.

Medidas de seguridad administrativas: Aquellas consistentes en la adopción e implementación de procedimientos que permitan la gestión y tratamiento de datos personales de la mejor manera posible, considerando las medidas de seguridad para su preservación, clasificación, borrado, etc.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados.

Obtención de información de forma personal: Los datos se obtienen de manera personal cuando el titular los proporciona al responsable o un encargado de este mediante la presencia física de ambos.

Obtención de información de forma directa: Cuando el titular los proporciona por algún medio que permite su entrega sin intermediarios, pese a que esta no sea presencial, se puede realizar por medios electrónicos, ópticos, sonoros, visuales o cualquier otro.

Obtención de información indirecta: Cuando el responsable los obtiene sin que el titular los proporcione de forma personal o directa, como puede ser por medio de una fuente pública o una transferencia de información.

Titular: Propietario de los datos personales.

Pérdida: Cuando los datos existen, pero el encargado de custodia pierde el control o el acceso a ellos.

Remisión ó cesión: Supone la comunicación de datos personales entre el responsable y el encargado del tratamiento.

Resguardo: Custodia o preservación de los datos personales.

Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Robo: Cuando una persona se apodera de los datos personales, sin derecho y sin consentimiento del titular.

Supresión: Actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas.

Transferencia: Implica la comunicación de datos personales dentro o fuera de territorio nacional, que realiza el responsable del tratamiento a un tercero distinto del titular, del mismo responsable o del encargado.

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio. El uso contempla cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Uso, acceso o tratamiento no autorizado: Cuando son utilizados para finalidades distintas a las que fueron recabados.

Vulneración: Incidente relacionado con los datos personales que puede implicar cualquiera de las siguientes circunstancias: (i) pérdida o destrucción no autorizada; (ii) robo, extravío o copia no autorizada; (iii) uso, acceso o tratamiento no autorizado; o (iv) daño, alteración o modificación no autorizada.

4. Política

- En todo tratamiento de datos personales deberán observarse los principios fundamentales de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, a fin de dar cumplimiento a las disposiciones legales aplicables. De igual forma, los datos personales deberán tratarse de manera confidencial y respetando la expectativa razonable de privacidad.
- Se deberá poner a disposición del titular el aviso de privacidad conforme a los lineamientos contenidos en la ley y de conformidad con el apartado 4.4. del presente documento.
- Sustentandem contará con medios que garanticen la seguridad de los datos recolectados, así mismo que se garantice la voluntad del titular respecto al tratamiento de sus datos.
- Los parámetros de comportamiento establecidos en la presente política abarcan no solamente a Sustentandem, sino que además es vinculante para clientes, socios comerciales, apoderados, contratistas, consultores, agentes y en general a cualquier persona que actúa en nombre, representación, beneficio, a cuenta o por los medios que Sustentandem proporcione.
- Es obligación para Sustentandem exigir que todas las empresas con las que colabora, quienes le presten cualquier clase de servicios, con las que se

comercialicen cualquier clase de servicio y, en general, cualquier socio comercial o de negocios con el que existe una transmisión de información, cumpla con los estándares mínimos establecidos en la presente política.

4.1. Los principios de protección de los datos personales

- El tratamiento de todos los datos personales recolectados por Sustentandem debe respetar, al menos, los siguientes principios:
 - Licitud. Se considera tratamiento lícito aquel que cumple con los estándares legales en cada legislación, nunca obteniendo la información por medios engañosos y fraudulentos y cumpliendo con las expectativas de privacidad.
 - Consentimiento. El tratamiento de datos personales, salvo excepciones reguladas por ley, estará sujeto al consentimiento de los titulares. Dicho consentimiento podrá ser expreso o tácito en aquellas situaciones en los que las leyes lo permitan, sin embargo, tratándose de datos financieros, patrimoniales o sensibles, el consentimiento deberá ser expreso, salvo excepciones por ley. El consentimiento se podrá manifestar por cualquier medio que permita recabarlo de manera inequívoca.
 - Información. El titular de los datos personales deberá siempre ser informado de los datos personales a tratar, así como de las finalidades del tratamiento y los medios para ejercitar sus derechos; así mismo, deberá informarse de los cambios realizados en los medios, fines o tratamiento de los datos personales.
 - Calidad y proporcionalidad. Los datos obtenidos deberán ser exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados. De igual forma, sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.
 - Finalidad. El tratamiento de los datos personales deberá limitarse a las finalidades establecidas en el aviso de privacidad, para las cuales el titular otorgó su consentimiento.
 - Confidencialidad. Bajo ningún motivo, los datos personales podrán ser divulgados o publicados a terceros sin que medie consentimiento del titular de estos, aplicando siempre medidas que garanticen su seguridad.
 - Lealtad. Los datos personales deberán tratarse privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

- Responsabilidad. El responsable está obligado a velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión.
- Los presentes principios serán los mínimos que deben observarse y ser incluidos en todas las actuaciones al respecto del tratamiento de datos personales que realiza el responsable o el encargado.

4.2. Tratamiento de los datos personales

4.2.1. Obtención

- Sustentandem establecerá y documentará los procedimientos relativos a la obtención, uso y/o tratamiento de los datos personales de los socios, empleados, proveedores, clientes y/o cualquier otro que tenga relación con la empresa.
- Los datos personales podrán recabarse ya sea de manera presencial o por medio de correo electrónico, sitio de internet, vía telefónica, fuente de acceso público, entre otros.
- Por otro lado, Sustentandem, podrá obtener indirectamente datos personales mediante la transferencia de datos, previa verificación de que, quién los transfiere, tiene la autorización para ello.
- Cuando se trate de la obtención de datos personales de menores de edad, personas en estado de interdicción o incapacidad declarada, se deberá de solicitar la autorización de los padres, tutores o representantes legales para otorgar el consentimiento mediante el aviso de privacidad.

4.2.2. Resguardo

El resguardo de los datos personales se gestionará mediante una base de datos física o electrónica, adoptando todas las medidas de seguridad idóneas y razonables, a la que únicamente el encargado del tratamiento de datos personales podrá acceder. Además, el encargado del tratamiento deberá elaborar un inventario de datos personales y los sistemas de tratamiento que usará, como la utilización de aplicaciones e infraestructura en el denominado cómputo en la nube.

4.2.3. Bloqueo

Una vez cumplida la finalidad para la cual se obtuvo la información, el encargado del tratamiento deberá bloquear los datos personales recabados y resguardarlos hasta el que finalice el plazo de prescripción legal o contractual. Durante ese tiempo, los datos personales no podrán ser objeto de tratamiento.

4.2.4. Supresión

Transcurrido el plazo estipulado o cumplida la finalidad, el titular de los datos personales podrá solicitar la cancelación y, en consecuencia, la supresión de los datos personales de la base de datos, lo cual consiste en la baja archivística de los datos personales, sea por eliminación, borrado o destrucción de los mismos, previas medidas de seguridad establecidas por el responsable.

El encargado deberá establecer métodos y/o técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima, asegurando el borrado seguro de datos.

4.2.5. Transferencia y remisión

Sustentandem podrá transferir datos personales a terceros, siempre y cuando se cuente con la autorización del titular de los datos personales y esto sea legalmente exigido. Previo a la transferencia, se verificará el nivel de protección de datos ofrecido por un tercero, el cual deberá de ser igual o mayor que la protección de la presente Política, y además deberá de respetar los marcos normativos de protección de datos.

4.2.6. Vulneración

Habrà vulneración a los datos personales cuando exista pérdida, destrucción, robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado; daño, alteración o modificación no autorizada; divulgación o revelación no autorizada; ya sea por debilidad, fallo o error en el sistema de información, procedimientos o en la seguridad del sistema.

Además de los supuestos anteriores, habrá vulneración cuando exista algún incidente de seguridad relacionado con el tratamiento de datos personales.

De manera preventiva, el encargado y/o el responsable deberán de desarrollar controles de seguridad y otros mecanismos que permitan actuar ante los incidentes seguridad, en los que se deberá de contemplar lo siguiente:

- El funcionamiento y podrá llevar a cabo una simulación del incidente para corroborar que los controles implementados sean eficaces.
- Mejora continua: consiste en complementar la documentación de lo que se hizo respecto al incidente y comunicar a las partes interesadas el estado de la seguridad de los activos después del incidente. Sustentandem deberá de generar un archivo o bitácora que permita a los encargados contar con una base de conocimiento que pueda ser utilizada para entrenar a nuevos integrantes del equipo de respuesta a incidentes.
- Preparación: consiste en elaborar un plan de respuesta a incidentes, mediante la implementación de medidas de seguridad, en tanto no se presente una vulneración Sustentandem deberá implementar un sistema de gestión de seguridad de datos personales y crear constantemente respaldos o copias de seguridad de los datos personales en su posesión.
- Identificación: consiste en detectar las alertas de seguridad y se determina si éstas pueden ser catalogadas como incidentes. Sustentandem deberá documentar las alertas de seguridad que se consideren relevantes o que se relacionen con un incidente.
- Contención: consiste en limitar el alcance o impacto del incidente identificado. Sustentandem deberá ordenar que se aíslen los activos afectados y la creación de respaldos de seguridad.
- Mitigación: consiste en realizar el tratamiento profundo del incidente de seguridad para minimizar la posibilidad de que éste se vuelva a repetir. Sustentandem deberá de recolectar evidencia para el análisis forense y reforzar la seguridad de los datos.
- Recuperación: consiste en dar seguimiento a las medidas implementadas en la mitigación, y los activos que fueron afectados, Sustentandem deberá monitorear los sistemas de tratamiento y las nuevas medidas adoptadas para garantizar que no exista algún mal deberá de emitir un reporte final sobre un incidente que se haya erradicado.

El responsable deberá informar al titular sobre cualquier vulneración de seguridad de sus datos personales ocurrida en cualquier fase del tratamiento, y deberán, al mismo tiempo, realizar un informe detallado que contenga por lo menos:

- La hora y fecha de la identificación de la vulneración.
- La hora y fecha del inicio de la investigación sobre la vulneración.
- La naturaleza del incidente.
- Los datos personales comprometidos.
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
- Los sistemas de tratamiento comprometidos.

- Las acciones correctivas realizadas de forma inmediata.
- La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.
- Las recomendaciones a adoptar.
- La documentación que se considere conveniente acompañar al reporte.
- Los medios donde puede obtener mayor información al respecto.

Dicho informe deberá ser enviado, también a las autoridades correspondientes, en caso de encontrarse ante hechos de apariencia delictiva.

Sustentandem tendrá la obligación de notificar a los titulares de cualquier vulneración relacionada con el tratamiento de sus datos personales en cualquiera de los siguientes 3 momentos:

- En el menor tiempo posible.
- Cuando ya se tenga información concreta del incidente.
- Cuando ya no exista exposición de los activos involucrados en la vulneración.

4.3. Ejercicio de los derechos ARCO

El encargado de datos personales deberá desarrollar el procedimiento para el acceso, rectificación, cancelación y oposición al tratamiento de datos personales y deberá mencionarlo en el aviso de privacidad.

El titular podrá solicitar ante el responsable que posee los datos personales, una solicitud mediante la cual pueda acceder, rectificar, cancelar u oponerse al tratamiento de los mismos.

La solicitud de ejercicio de derechos ARCO deberá de contener como mínimo lo siguiente:

- Nombre del titular o de su representante.
- Documentos que acrediten la identidad del titular o de su representante.
- Domicilio o cualquier medio para recibir notificaciones.
- Descripción clara y precisa de los datos personales.
- Descripción del derecho que se pretende ejercer.
- Además de lo anterior, el titular, dependiendo del derecho que desea ejercer, deberá aportar la siguiente información específica:
- Derecho de acceso: la modalidad en la que refiere que se reproduzcan los datos personales solicitados.

- Derecho de rectificación: las modificaciones que solicita que se realicen a los datos personales, así como aportar la documentación en la que sustenten su solicitud.
- Derecho de cancelación: las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
- Derecho de oposición: las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe.

El titular podrá ejercer sus derechos ARCO en todo momento, siempre y cuando sea dentro de la vigencia del tratamiento. Una vez presentada la solicitud, el responsable deberá de emitir un acuerdo de admisión o prevención en un término no mayor a 10 días hábiles contados a partir del día siguiente de la presentación de la solicitud.

Sustentandem estará facultado de prevenir al titular respecto de su solicitud, cuando no proporcione la información general y específica antes descrita. Para tal efecto, el titular o su representante deberán de desahogar la prevención formulada por el responsable en el término de 3 días hábiles, contados a partir del día siguiente en que se realizó la notificación.

Desahogada la prevención, el responsable deberá, en un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud o del desahogo de la prevención, informar si procede o no el ejercicio del derecho solicitado.

En caso de que haya procedido el ejercicio del derecho, el responsable deberá de llevar a cabo las acciones necesarias para hacer efectivo el ejercicio del derecho, en un plazo de 15 días hábiles, contados a partir del día siguiente en que se haya notificado la respuesta de procedencia.

Sustentandem estará obligado a responder la solicitud, aun cuando no proceda el ejercicio del derecho solicitado, explicando las causas de la improcedencia respectiva en un plazo de 20 días hábiles contados a partir del día siguiente a la recepción de la solicitud o del desahogo de la prevención.

4.4. Del aviso de privacidad

Es obligación del responsable contar con un documento en el que informe al titular, por lo menos:

- La identidad y el domicilio del responsable.
- Las finalidades del tratamiento de los datos.

- Los medios para manifestar la negativa respecto al tratamiento de sus datos para finalidades secundarias o accesorias, en caso de existir.
- Los datos personales tratados.
- La obtención expresa de consentimiento del titular respecto a los datos sensibles recabados.
- Las transferencias de datos que podrían realizarse y, en su caso, la expresión del consentimiento del titular para dichas transferencias.
- Los medios para ejercitar los derechos ARCO.
- Los medios para revocar el consentimiento para el tratamiento de los datos personales.
- Los medios para limitar el uso o divulgación de datos personales.
- En su caso, informar el uso de cookies, web beacons o cualquier tecnología similar o análoga.
- Los medios por los que se informarán los cambios en el aviso de privacidad.

El aviso de privacidad se debe poner a disposición del titular en los siguientes momentos:

- Previa obtención de los datos personales: cuando la información se obtenga de manera directa o personal del titular de manera física.
- Al primer contacto con el titular: cuando los datos se obtienen de forma indirecta y el tratamiento de la información requiere contacto directo con el titular.
- Previo al aprovechamiento de los datos: cuando los datos se obtienen de manera indirecta pero el tratamiento no requiere contacto personal o directo.

Se deberá contar con tantos avisos de privacidad como sean necesarios dependiendo de su contenido o destino, por ejemplo, contar con un aviso de privacidad para clientes, proveedores y empleados.