POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PERSONAL EN PROTECCION DE DATOS PERSONALES

En ALIANSAP CONSULTING S.A.S., la información es un activo fundamental para el desarrollo de su objeto social y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso con la seguridad en la protección de los datos personales, como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad de la información.

Consciente de las necesidades actuales, ALIANSAP CONSULTING S.A.S., implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y mitigar los riesgos a los cuales se expone la información, ayuda a la reducción de riesgos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales y comerciales vigentes.

Los terceros, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de ALIANSAP CONSULTING S.A.S., deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política General de Seguridad de la Información de ALIANSAP CONSULTING S.A.S., se encuentra soportada por políticas y procedimientos específicos los cuales guiarán el manejo adecuado de la información. Adicionalmente, se establecerán políticas específicas de seguridad de la información.

ALIANSAP CONSULTING S.A.S., tendrá la capacidad de modificar la Política General o las Políticas específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de estas.

ALIANSAP CONSULTING S.A.S., con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, ALIANSAP CONSULTING S.A.S., mediante la suscripción de los correspondientes contratos de transmisión, de aplicar para ALIANSAP CONSULTING S.A.S., ha requerido a los encargados del tratamiento con los que trabaja la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

CLASIFICACIÓN Y MANEJO DE INFORMACIÓN

La información es un insumo vital para el funcionamiento de ALIANSAP CONSULTING S.A.S., por esta razón expresa su compromiso ante la seguridad de esta.

En este sentido ALIANSAP CONSULTING S.A.S., dispondrá de los recursos necesarios para identificar y clasificar la información, para poder realizar una gestión pertinente en cuanto a seguridad de la información.

No toda la información tiene el mismo nivel de importancia para ALIANSAP CONSULTING S.A.S., en consecuencia, la clasificación de la información con niveles de acceso es necesaria para identificar los criterios fundamentales en la determinación de su valor y el conjunto de controles apropiados y requeridos para preservar su valor.

Se debe hacer una valoración de los activos de información, clasificándolos, ordenándolos y tomando las medidas de seguridad apropiadas para su acceso, conservación y destrucción con acciones preventivas tanto en la información física como digital, para garantizar que los archivos sean tratados de acuerdo con las políticas de seguridad de la Información de ALIANSAP CONSULTING S.A.S..

Esta información está enmarcada en los principios de ciclo de vida del dato personal y su grado de confidencialidad donde se han definido los siguientes niveles en marcando el manejo de información de acuerdo con su uso.

Información altamente confidencial	Información que puede generar alto riesgo reputacional en caso de no ser tratada de manera adecuada, tanto para FANATICADA S.A.S. como para sus clientes.

Información confidencial:	Información que por su naturaleza no debe ser divulgada y que su divulgación o alteración implica un riesgo alto para ALIANSAP CONSULTING S.A.S. y sus clientes, y solo deben tener acceso a ella los directivos
Información privada:	Información pertinente únicamente a ciertas personas de ALIANSAP CONSULTING S.A.S., y que solamente tienen acceso ciertas áreas.
Información de uso interno:	Información de ALIANSAP CONSULTING S.A.S., a la que pueden tener acceso los autorizados, pero no es de conocimiento público
Información pública:	Información relacionada con su labor u oficio, o información que se encuentre en internet y que no necesite ningún nivel de autenticación.

A continuación, se exponen las medidas de seguridad implantadas por ALIANSAP CONSULTING S.A.S., que están recogidas y desarrolladas en la presente política (Tablas II, III, IV y V.). La Tabla VI. Corresponde al Procedimiento de Clasificación y Manejo de Información

Tabla II. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas).

Gestión de documentos y soportes	Control de acceso	Incidencias	Personal	Manual Interno de Seguridad
1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Autorización del responsable para la salida de documentos o soportes por medio electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado. 5. Gestión de contraseñas. 6. Implementación de mecanismos de doble validación.	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias.	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos. 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.	1. Elaboración e implementación del Manual de obligatorio cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

Tabla III. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos.

Archivo	Almacenamiento de documentos	Custodia de documentos	Identificación y autenticación	Telecomunicaciones
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	1. Acceso a datos mediante redes seguras.

Tabla IV. Medidas de seguridad para datos privados según el tipo de bases de datos

Auditoría	Responsable de seguridad	Manual Interno de Seguridad	Gestión de documentos	Control de acceso	Identificación y autenticación	Incidencias
1. Auditoría ordinaria (interna o externa) cada dos meses. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento. 5. Conservación del Informe a disposición de la autoridad.	1. Designación de uno o varios responsables de seguridad. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.	1. Controles periódicos de cumplimiento.	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

Tabla V. Medidas de seguridad para datos sensibles según el tipo de bases de datos

Bases de datos no automatizadas				Bases de datos automatizadas		
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**	**Gestión de documentos**	**Control de acceso**	**Telecomunicaciones**
1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autorizados. 2. Destrucción que impida el acceso o recuperación de los datos.	1. Medidas que impidan el acceso o manipulación de documentos.	1. Sistema de etiquetado confidencial. 2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando salgan fuera.	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 2. Control del registro de accesos por el responsable de seguridad. Informe mensual. 3. Conservación de los datos: indefinido.	1. Transmisión de datos mediante redes electrónicas cifradas.

Tabla VI. Procedimiento de clasificación y manejo de información

Nombre de la actividad	Descripción	Documento	Responsable de la actividad
Identificación de repositorios deinformación	Mediante la revisión de cada uno de los procesos se identifican los tipos de información	Inventario de información	Oficial de protección de datos personales
Clasificación de la información	Una vez definido los tipos de información se establece la clasificación dependiente del nivel de confidencialidad y del riesgo que puede presentar en caso de afectar alguno de los pilares de seguridad de la información como son confidencialidad, disponibilidad e integridad de la información	Inventario de información	Oficial de protección de datos personales
Definición de niveles de acceso	Teniendo la información identificada se establece el responsable interno de la información y los demás cargos con acceso a la información	Inventario de información	Oficial de protección de datos personales
Determinación de tiempo de archivo	El archivo físico deberá tener unos tiempos de retención en la actualidad los archivos identificados en documentos físicos se almacenarán por lo menos el tiempo estipulado por las normas.	Inventario de información	Oficial de protección de datos personales

Firma:

Representante Legal
DALIA CAROLINA CASTILLO CERON

CONTROL DE DOCUMENTOS Y CAMBIOS

Control de Documentos			
Elaborado por	Comité de Seguridad de la Información	**Fecha:**	5/01/2025
Aprobado por	Representante Legal	**Fecha:**	5/01/2025

Control de Cambios				
Versión	**Fecha**	**Cambio**	**Revisado por**	**Aprobado por**
1.0	5/01/2025	Actualización General	Oficial de Protección de Datos	Representante Legal