

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	1 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

FONDO DE EMPLEADOS GREENLAND – FEGREEN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Definir los lineamientos y directrices dirigidas a otorgar seguridad a la información y a la información de carácter personal del Fondo de empleados GreenLand, Fegreen.

2. ALCANCE

Las políticas y formatos definidos aplicarán para todos los asociados, empleados, proveedores de convenios y de servicios y en general, que actúen en calidad de encargados o que requieran acceder o usar los datos personales o a la información de FEGREEN. Esta política será de obligatorio cumplimiento para todas las personas destinatarias de esta.

3. DEFINICIONES

- **Aviso de privacidad.** Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y la finalidad del tratamiento que se pretende dar a los datos personales.
- **Autoridad protección de datos.** La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Ley.
- **Autorización.** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	2 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Bases de datos.** Conjunto organizado de datos personales que sea objeto de tratamiento, pueden ser físicas o automatizados.
- **Confidencialidad.** Hace referencia a la protección de información cuya divulgación no está autorizada.
- **Dato personal.** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato personal público.** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato personal semiprivado.** Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere la ley 1266 de 2008.
- **Dato personal sensible.** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **Disponibilidad.** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Cargo				Elaboró	Aprobó
Jefe	CAD	del	Grupo	Oficial de Protección de Datos Personales	Gerencia Administrativa
Empresarial GreenLand.					

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	3 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Encargado de tratamiento.** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Fraude.** Cualquier acto deshonesto caracterizado por engaño, ocultación o abuso de confianza, cometido por una o más personas, con el fin de obtener provecho o ventajas personales o para un tercero en perjuicio de otra persona o empresa.
- **Fraude informático.** Se contemplan los accesos no autorizados, uso indebido de los recursos tecnológicos en contra de lo estipulado en la política y la alteración o robo de información a través de los medios tecnológicos.
- **Incidente.** Violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado, que deberán reportarse al registro nacional de bases de datos en adelante el RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.
- **Integridad.** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
- **Oficial de protección de datos.** Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización. Jefe Centro Administración Documental del Grupo Empresarial GreenLand.
- **Registro nacional de bases de datos.** Es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el registro será administrado por la Superintendencia de Industria y Comercio.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	4 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Responsable del tratamiento.** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- **Titular.** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Transferencia de datos.** Tiene lugar cuando el responsable y/o Encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
- **Transmisión.** Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.
- **Tratamiento.** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Usuarios.** Aplica para los empleados, asociados, proveedores y aliados estratégicos.

4. RESPONSABLES

Entre las responsabilidades a este proceso están:

- **Junta Directiva Fegreen**

Se encargará de establecer la estructura y los procesos de supervisión orientados al cumplimiento de los objetivos planteados en el direccionamiento estratégico de FEGREEN, además de identificar oportunidades de mejoramiento continuo y solicitar a la Gerencia información sobre la implementación de éstas. La Junta Directiva tiene la responsabilidad de revisar el cumplimiento de los requisitos legales, normativos, de procesos administrativos y la gestión de riesgos aplicables a FEGREEN.

Cargo				Elaboró	Aprobó
Jefe	CAD	del	Grupo	Oficial de Protección de Datos Personales	Gerencia Administrativa
Empresarial GreenLand.					

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	5 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Gerencia Fegreen**

Será la responsable de dirigir la implementación, mantenimiento y funcionamiento de los procedimientos administrativos, de gestión de riesgos; además, deberá garantizar el cumplimiento de la protección de datos personales y seguridad de la información en FEGREEN, a través de la asignación de los recursos necesarios para tal fin, y de la aprobación de políticas generales que faciliten la implementación de sistemas de gestión de la seguridad de la información, de programas integrales de gestión de datos personales que permitan minimizar el riesgo. Así como fomentar y fortalecer la cultura de seguridad de la información, la protección de datos a través de la capacitación de los empleados; en cuanto a normas, políticas, mecanismos de control y seguridad necesarios.

La Gerencia deberá propiciar una cultura organizacional de respeto a la protección de datos personales y seguridad de la información, conforme al marco de estricto cumplimiento de la Ley. También deberá garantizar la implementación y desarrollo de las políticas, directrices y lineamientos en materia de seguridad y protección de datos personales, designará los roles y responsabilidades relacionadas con seguridad de la información y la protección de los datos personales

- **Auditoría del Holding GreenLand**

El área de Auditoría interna del Holding GreenLand podrá realizar su funcionamiento a todos los niveles, funciones, procedimientos, proyectos y estructura de FEGREEN y para ello, diseñará con apoyo del Oficial de protección de datos, los mecanismos de control, indicadores de gestión y de prevención de riesgos a aplicar; esto con el fin de garantizar la correcta evaluación y seguimiento de las reglas y políticas de protección de datos personales al interior de FEGREEN.

El área de Auditoría podrá realizar auditorías periódicas a FEGREEN en materia de protección de datos personales y seguridad de la información para garantizar que esta se esté ejecutando conforme a los lineamientos de la Ley.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	6 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Oficial de protección de datos del Holding GreenLand**

El Oficial de protección de datos será el encargado de la empresa vinculante y se encargará de coordinar con apoyo de las diversas áreas del Holding, entre ellas la Gerencia de FEGREEN y de las TIC's, el desarrollo e implementación de políticas, procesos y procedimientos de seguridad de la información que incorporen las medidas de seguridad (técnicas, humanas y administrativas) que protejan los datos personales y la información. A su vez, impulsará una cultura de seguridad de la información y protección de datos en todas las áreas de la empresa vinculante.

El Oficial mantendrá un inventario de las bases de datos personales en poder del Holding, las clasificará según su tipo y las relacionará en el Registro Nacional de Bases de Datos para actualizar el reporte, atendiendo las instrucciones que sobre el particular emita la SIC.

Con el fin de hacer seguimiento a las medidas, políticas y procedimientos de protección a los datos personales, el Oficial articulará un programa de entrenamiento en protección de datos personales específico para las diferentes áreas, con mayor incidencia en cuanto al tratamiento de datos y un entrenamiento general en protección de datos personales para todos los empleados de FEGREEN.

También diseñará con el apoyo del área de Auditoría del Holding, los mecanismos de control, indicadores de gestión y de prevención de riesgos que aplicará a FEGREEN, con el fin de garantizar la correcta evaluación y seguimiento de las reglas y políticas de protección de datos; por lo que, deberá verificar que en todos los procesos de seguridad física actuales y futuras en los que se soliciten datos personales (minutas de registro de equipos, captura de fotos y datos para control de acceso, entre otros) se obtenga la debida autorización de acuerdo con los requerimientos legales.

Con el apoyo del área jurídica de la empresa vinculante, deberá establecer los controles oportunos que permitan verificar que los encargados de tratamiento contratados cumplen con los requisitos establecidos para el tratamiento de datos personales y deberá gestionar, para este caso con FEGREEN, los incidentes en materia de protección

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	7 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

de datos conforme los lineamientos establecidos por la Superintendencia de Industria y Comercio.

- **Gerencia de TIC's Grupo del Holding GreenLand**

Será responsable de definir y mantener las políticas de uso de recursos informáticos en coordinación con las áreas del Holding, proponiendo los cambios necesarios para garantizar la incorporación de la tecnología de punta en la compañía, la cual acobija directamente a FEGREEN.

También se encargará de la administración, mantenimiento, operación, expansión de la infraestructura tecnológica, la definición de lineamientos, reglas y procedimientos que garanticen la disponibilidad, seguridad y confiabilidad del entorno tecnológico a FEGREEN y las áreas en general.

El área de TIC's será responsable de la seguridad de la información almacenada por los empleados en los servidores, para lo cual los empleados de FEGREEN tendrán asignada una unidad personal "G" y el OneDrive para el almacenamiento de sus archivos particulares.

Regulará el uso de recursos corporativos como el internet y el correo electrónico por medio de lineamientos, reglas y procedimientos que garanticen el uso adecuado de los mismos, fortaleciendo los canales de comunicación entre FEGREEN y la empresa vinculante, para ello analizará, evaluará y establecerá el montaje e implementación de su infraestructura tecnológica (Hardware y Software).

La Gerencia de TIC's tramitará la negociación de cualquier componente de tecnología HW (equipos) y SW (comercial y/o de industria) que requiera FEGREEN, solicitando al personal del área comercial de la empresa vinculante, donde se detalle explícitamente las características de fabricante, marca, modelo y especificaciones técnicas de la solución a adquirir, para que ellos procedan a la negociación previo cumplimiento de las políticas de adquisición de bienes y servicios, conflicto de intereses y la política de contratación.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	8 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

Entre sus responsabilidades, deberá apoyar al Oficial de protección de datos en la gestión de incidentes ante la SIC en el caso de las bases de datos automatizadas, implementar las medidas de seguridad en entornos tecnológicos que protejan los datos personales y la información de FEGREEN e implementar las medidas de seguridad físicas requeridas para el cumplimiento de las políticas asociadas con los recursos físicos “Hardware” y los controles de acceso a los sitios restringidos.

- **Jefe Fegreen**

Será responsable de solicitar la cuenta de usuario, la asignación de perfiles de acceso al ingreso del empleado e informar sobre la ausencia y retiro de este ante el área de TIC's y garantizar que se realicen los acuerdos de confidencialidad contemplados por el Holding.

El Jefe de FEGREEN garantizará que esta política se implemente adecuadamente y perdure su debida ejecución en el tiempo; para ello, deberá establecer planes de acción frente a los resultados de auditoria que realice el Holding y realizar revisiones periódicas del estado de implementación de la política y medidas de seguridad (por lo menos una vez año).

- **Usuarios**

Serán responsables de cumplir estrictamente la política definida, velar por la integridad, confidencialidad, disponibilidad y seguridad de la información que generan, administran, gestionan y/o custodian y de guardar especial reserva respecto a la información personal de carácter sensible, privada y de menores de edad.

En el caso de los empleados que son los responsables de establecer convenio con los proveedores, deberán garantizar que estos se acojan a los acuerdos de confidencialidad estipulados por FEGREEN.

También deberán reportar incidentes de seguridad con la base de datos físicas o automatizadas, nuevas bases de datos y/o novedades de conformidad al procedimiento señalado al Jefe Fegreen y Oficial de protección de datos del Holding y

Cargo				Elaboró	Aprobó
Jefe	CAD	del	Grupo	Oficial de Protección de Datos Personales	Gerencia Administrativa
Empresarial GreenLand.					

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	9 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

deberán participar en las capacitaciones y sensibilizaciones en materia de seguridad de la información y protección de datos que imparta la empresa vinculante.

5. NORMAS Y POLITICAS RELACIONADAS

Esta política complementará la normatividad, además de otras definidas por FEGREEN, las cuales contienen información adicional para aplicar:

- Manual General del Sistema de Administración del Riesgo de Lavado de Activos y la Financiación del Terrorismo, SARLAFT.
- Política de privacidad para el tratamiento de datos personales.
- Política de proveedores.

6. DESARROLLO

6.1 GENERALIDADES

La Constitución Política de Colombia en el artículo 15 establece el derecho de protección de datos personales, definido como el derecho fundamental de toda persona para conocer, actualizar, incluir, rectificar y/o cancelar o suprimir la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas, así como la de revocar la autorización. Este derecho fundamental fue objeto de regulación por el legislador a través de la Ley Estatutaria 1581 de 2012, Decreto único 1074 de 2015 y normas expedidas por parte de la Superintendencia de Industria y Comercio. Dentro de este marco regulatorio, el principio de seguridad establece el requerimiento por parte de los responsables y encargados de manejar la información personal con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Igualmente, y ante un evento de incidente, se deberá informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

Con base en lo anterior, FEGREEN reconocerá la necesidad de proteger la información corporativa y adoptará la presente política con la finalidad de establecer las directrices y

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	10 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

lineamientos para la seguridad de la información y en especial la información de carácter personal.

6.2 PRINCIPIOS

- **Principio de legalidad en materia de tratamiento de datos.** El tratamiento a que se refiere este principio es a una actividad regulada que deberá sujetarse a lo establecido en la Ley y en las demás disposiciones que la desarrollen.
- **Principio de finalidad.** El tratamiento deberá obedecer a una finalidad legítima de acuerdo con la constitución y la Ley, la cual debe ser informada al titular.
- **Principio de libertad.** El tratamiento sólo se podrá ejercer con el consentimiento previo, expreso e informado del titular; por lo tanto, los datos personales no podrán ser obtenidos o divulgados sin previa autorización o en ausencia de mandato legal o judicial que releve el consentimiento.
- **Principio de veracidad o calidad.** La información sujeta a tratamiento deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible; por lo que, se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de transparencia.** En el tratamiento se deberá garantizar el derecho del titular a obtener del responsable de este proceso, en cualquier momento y sin restricciones, la información acerca de la existencia de datos que le conciernen.
- **Principio de acceso y circulación restringida.** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley y la constitución. En este sentido, el tratamiento sólo se podrá hacer por personas autorizadas por el titular y/o por las personas contempladas por la Ley.
- **Principio de seguridad.** La información sujeta a tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Cargo				Elaboró	Aprobó
Jefe	CAD	del	Grupo	Oficial de Protección de Datos Personales	Gerencia Administrativa
Empresarial GreenLand.					

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	11 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

En este principio FEGREEN tendrá en consideración las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes.
 - Cumplir con los principios de seguridad de la información.
 - Mantener la confianza de sus empleados, asociados, proveedores y aliados estratégicos.
 - Apoyar la innovación tecnológica.
 - Proteger los activos tecnológicos.
 - Establecer los manuales, políticas, procedimientos e instructivos en materia de seguridad de la información y protección de datos personales.
 - Fortalecer la cultura de seguridad de la información y de los datos personales en sus empleados, asociados, proveedores y aliados estratégicos.
 - Propender por la implementación de las medidas que permitan la continuidad del negocio frente a incidentes.
- **Principio de confidencialidad.** Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende en este, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley y en los términos de esta.
 - **Principio de limitación de la recolección.** Sólo se deberán recolectar los datos personales que sean estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo del tratamiento. En consecuencia, se deberá hacer todo lo razonablemente posible para limitar el procesamiento de datos personales. Es decir, los datos deberán ser: adecuados, pertinentes y acordes con las finalidades para las cuales fueron previstos.
 - **Principio de temporalidad.** Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la

Cargo				Elaboró	Aprobó
Jefe	CAD	del	Grupo	Oficial de Protección de Datos Personales	Gerencia Administrativa
Empresarial GreenLand.					

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	12 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

información. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Una vez cumplida la finalidad del tratamiento y los términos establecidos anteriormente, se procederá a la supresión de los datos.

En el uso de recursos informáticos se aplicarán los siguientes principios:

- **Principio de propiedad de la información.** Los activos de información que sean propiedad de FEGREEN serán entregados para su uso, operación o custodia al personal a quien se aplica esta política, de acuerdo con las funciones específicas y necesidades derivadas de las actividades que deban realizar, sin que esto altere en ningún momento la específicas se nombre en la cadena de custodia u operación un propietario de cada activo de información. Este nombramiento permitirá que las únicamente haya un responsable y seguirá estando a nombre de FEGREEN; aunque dentro de las funciones, con el fin de asignar las responsabilidades operativas y de custodia sobre los diferentes activos.
- **Principio de protección de la información.** Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para FEGREEN y el Holding. La protección deberá acentuar la confidencialidad, integridad y disponibilidad de los activos de información.
- **Principio de protección de los recursos tecnológicos.** Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para FEGREEN y el Holding. Dichos recursos deberán ser utilizados exclusivamente para desarrollar actividades relacionadas con la operatividad de FEGREEN. Así mismo su utilización se hará en forma adecuada, con la máxima eficiencia y responsabilidad.
- **Principio de autorización de usuarios.** Todos los usuarios deberán ser identificados individualmente con permisos de acceso específicos e independientes, autorizados por razones básicas de sus funciones dentro de FEGREEN y/o la empresa vinculante. Los métodos de acceso de usuarios deberán exigir un proceso robusto de autenticación y autorización apropiada.

Cargo				Elaboró	Aprobó
Jefe	CAD	del	Grupo	Oficial de Protección de Datos Personales	Gerencia Administrativa
Empresarial GreenLand.					

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	13 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Principio de responsabilidad.** Los usuarios, depositarios y custodios de los activos de información de FEGREEN serán responsables por el uso apropiado, protección y privacidad de estos activos; por lo tanto, los sistemas de la empresa vinculante generarán y mantendrán unas apropiadas pistas de auditoria para identificar usuarios y documentar acciones relacionadas con situaciones violatorias de la seguridad.
- **Principio de integridad.** Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

6.3 LINEAMIENTOS GENERALES

6.3.1 POLÍTICA GENERAL

Entendiendo la importancia de una adecuada gestión de la información y que la protección de esta será de carácter personal y de conformidad con el marco regulatorio establecido; FEGREEN se comprometerá con la implementación de medidas de seguridad que permitan preservar la integridad, confidencialidad y la disponibilidad de la información, con la promoción de una cultura en seguridad y protección de los datos y con la gestión adecuada los incidentes para fomentar el mejoramiento continuo.

- **Identificación de base de datos personales.** FEGREEN, dentro del procedimiento para identificar, inventariar y actualizar sus bases de datos ha establecido como criterios generales:
 - **Finalidad y tipo de datos personales.** Se identifican las bases de datos de acuerdo con la finalidad y tipología del dato personal; en especial con la finalidad de establecer medidas de seguridad reforzada, especiales y más robustas respecto de las bases de datos que contengan datos sensibles y de menores.
 - **Forma de tratamiento.** FEGREEN establecerá las siguientes bases:

Cargo				Elaboró	Aprobó
Jefe	CAD	del	Grupo	Oficial de Protección de Datos Personales	Gerencia Administrativa
Empresarial GreenLand.					

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	14 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Base de datos automatizada.** Se identifican como base de datos automatizada aquella que se almacena y administra con la ayuda de herramientas informáticas o sistemas de información automatizados.
- **Base de datos física (papel).** Se identifican como base de datos física o manual cuando contienen archivos cuya información se encuentra organizada y almacenada de manera física. Estos archivos o carpetas pueden estar compuestos por cualquier tipo de soporte y/o conjunto documentos físicos vinculados a las personas y organizados por criterios específicos relativos a las personas. El tratamiento de estos documentos responde a una finalidad común y determinada.

El inventario de bases de datos personales de FEGREEN como objeto de registro ante la Superintendencia de Industria y Comercio será consolidado y registrado por el Oficial de Protección de datos personales del Holding, de conformidad con la reglamentación emitida por parte de esta Superintendencia.

6.3.2 POLÍTICAS ESPECÍFICAS

Teniendo presente que en virtud de la naturaleza jurídica, administrativa y operativa de FEGREEN, la operación física y tecnológica se desarrolla soportado por la infraestructura tecnológica y en las instalaciones de la empresa vinculante, serán complementarias y de obligatorio cumplimiento en lo que corresponda las políticas que se relacionan a continuación:

6.3.2.1 POLÍTICA PARA EL USO DE LOS RECURSOS INFORMÁTICOS DEL GRUPO EMPRESARIAL GREENLAND (PL_GR.GR.02-06 V3). Esta política incluye fundamentalmente los siguientes aspectos:

- Uso de las cuentas de acceso.
- Acceso y uso de internet.
- Uso del correo electrónico.
- Uso de los recursos físicos informáticos.
- Conexión de equipos a la red de la compañía.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	15 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

6.3.2.2 POLÍTICA CORPORATIVA PARA EL MANEJO DE LA INFORMACIÓN Y CONFIDENCIALIDAD V2.1.

Desarrolla aspectos relacionados con la protección de la información.

6.3.2.3 POLÍTICA DE GESTION DOCUMENTAL Y PROGRAMA DE GESTIÓN DOCUMENTAL

(PL_GR.GR.02-07 V.4). En FEGREEN se deberá atender los lineamientos para la administración documental en cualquier soporte físico y/o electrónico, basados en las metodologías y normas para la producción de información desde su creación, uso y mantenimiento; garantizando en todo momento la integridad, autenticidad y veracidad de la información, bajo parámetros técnicos de organización, tramite, gestión, conservación y disposición final, soportados en los principios archivísticos.

Lo anterior, en concordancia con lo señalado en la POLÍTICA DE PROVEEDORES DE FEGREEN, en lo referente a la conservación y retención de documento, la documentación del proveedor se conservará de forma física y digital. El folder físico se custodiará en Envigado para conservar su historial Y una vez finalizada la relación comercial con el proveedor, la información se conservará por un período diez (10) años, cumplido este tiempo se procederá con su eliminación.

En el Manual General del Sistema de Administración del Riesgo de Lavado de Activos y la Financiación del Terrorismo, SARLAFT de FEGREEN, se contempla procedimientos para mantener los documentos y registros que garanticen la integridad, oportunidad, confiabilidad, reserva y disponibilidad de la información que se genera durante la ejecución de sus actividades propias.

6.3.2.4 POLÍTICA DE SEGURIDAD Y PROTECCIÓN DE DATOS EN LA CONTRATACIÓN.

Teniendo presente que en virtud de la naturaleza jurídica, administrativa y operativa de FEGREEN, la operación física y tecnológica se desarrolla soportado por la infraestructura tecnológica y en las instalaciones de la empresa vinculante, serán complementarias y de obligatorio cumplimiento a la POLÍTICA DE PROVEEDORES DE FEGREEN en lo que corresponda, las políticas de contratación del Grupo Empresarial GreenLand que se relacionan a continuación:

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	16 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Política de contratación.** Las funciones y obligaciones generales de los usuarios (empleados, asociados, proveedores y aliados estratégicos) que para el correcto desarrollo de su labor o actividad tienen autorizado el acceso a datos personales o información, tienen las siguientes obligaciones:
 - Velar por la integridad, confidencialidad y disponibilidad de la información que administran, gestionan y/o custodian.
 - Guardar en secreto cualquier tipo de información en función del trabajo o actividades desarrolladas, incluso una vez concluida la relación laboral o contractual con FEGREEN.
 - Los empleados no divulgarán ante terceros, a quienes no les ha sido confiada la información de carácter sensible, confidencial de menores (salvo la información pública) y/o reservada, salvo en los casos de requerimiento judicial y/o administrativo y con previa autorización de la Gerencia.
 - El almacenamiento de la información que tenga carácter reservado, sensible de menores y/o confidencial, será conservado en las instalaciones de FEGREEN o donde éste considere conveniente, de tal manera, que impidan el acceso a terceros y/o funcionarios de las empresas no autorizados, conforme con las normas que para tal efecto tenga establecido el área de sistemas y/o Gestión Documental del Grupo Empresarial GreenLand. En consecuencia, se considerará violación a esta política, la negligencia y/o descuido que permita el acceso de la información por personas no autorizadas.
 - Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
 - Comunicar al Jefe y/o Gerencia de Fegreen, al Oficial de protección de datos y a la Gerencia de TIC'S del Holding, de acuerdo con el procedimiento de gestión de incidentes, aquellos eventos de seguridad

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	17 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

de las que se tenga conocimiento de que puedan afectar las bases de datos, soportes o documentos que contengan información personal.

- Velar por el cumplimiento de las diferentes políticas, procedimientos, manuales y reglamentaciones de FEGREEN y aquellas del Grupo Empresarial Greenland que apliquen con ocasión de su operación técnica y administrativa.

6.3.2.5 POLÍTICA DE PRIVACIDAD, DATOS PERSONALES Y CONFIDENCIALIDAD. Será política de FEGREEN, el cumplimiento frente a la Legislación vigente en cada lugar donde se tiene presencia y los empleados no deberán realizar, permitir, tolerar o incitar a actividades, operaciones o actos que infrinjan o incumplan la legislación vigente del país. De igual manera, FEGREEN velará porque las entidades externas con las que tiene relaciones o contratos; también cumplan la legislación que rige en el país.

Con base en lo anterior, en materia de protección de datos personales será de obligatorio cumplimiento para FEGREEN las normas, leyes y reglamentos expedidos por las respectivas entidades públicas, así como los lineamientos definidos en la Política de privacidad de datos personales, manuales y procedimientos definidos por él, y en lo que corresponda a la POLÍTICA CORPORATIVA PARA EL MANEJO DE LA INFORMACIÓN Y CONFIDENCIALIDAD V 2.1. del Grupo Empresarial GreenLand.

6.3.2.6 POLÍTICA DE CAPACITACIÓN DE EMPLEADOS. FEGREEN implementará programas anuales de capacitación y concientización en protección de datos personales y seguridad de la información para sus empleados y en el caso de nuevo personal, al momento de vincularse, este deberá recibir capacitación sobre protección de datos personales y seguridad de la información dejando constancia de su asistencia y conocimiento.

Para el desarrollo de los programas de capacitación y concientización deberán asegurar que los usuarios entiendan sus responsabilidades con respecto a la protección de datos personales y seguridad de la información.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	18 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

6.3.2.7 POLÍTICA DE TRATAMIENTO DE DATOS Y SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

EXTERNOS A FEGREEN. Para la contratación de proveedores y terceros en general que implique un tratamiento de datos personales se establecerá lo siguiente:

Todos los usuarios externos que realizan tratamiento de datos o acceden a los datos personales por cuenta de FEGREEN deberán cumplir en su totalidad con las obligaciones establecidas en la Ley y en las políticas aprobadas por el Grupo Empresarial GreenLand y FEGREEN, con la finalidad de proteger los datos personales y otorgar seguridad a la información.

Para el caso de transmisión de datos personales se deberá incluir, además, de las obligaciones que impongan normas aplicables dentro del contrato de transmisión/instrumento jurídico, las siguientes obligaciones en cabeza del respectivo encargado:

- Dar Tratamiento a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
- Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- Guardar confidencialidad respecto del tratamiento de los datos personales.

Dentro del contrato se definirá la utilización, la finalidad y el tiempo que se le dará a la información; la cual una vez se haya realizado el servicio objeto del contrato, la información deberá ser devuelta, destruida o conservada por el encargado del tratamiento, debidamente bloqueados los datos, en tanto se pudieran derivar responsabilidades de su relación con el responsable de la base de datos. Se tendrá en cuenta entre otros aspectos:

- Los datos facilitados únicamente serán tratados conforme a las instrucciones especificadas por el responsable en el propio contrato.
- Deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	19 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- Los datos no se aplicarán o utilizarán con distinto fin al que figure en dicho contrato.
- Los datos no serán comunicados bajo ningún concepto a otras personas, excepto que se autorice la posibilidad de subcontratación de servicios.
- Si la empresa contratada destina los datos a otra finalidad, los comunica o realiza cualquier uso distinto a lo estipulado en el contrato, deberá responder legalmente de las infracciones en que hubiera incurrido.
- La empresa contratada deberá implementar, sobre los datos facilitados, las medidas de seguridad que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- No se registrarán datos de carácter personal en bases de datos que no reúnan las condiciones de integridad y seguridad determinadas en la organización.
- El encargado adoptará las medidas necesarias para que las personas que tengan acceso a sus datos personales cumplan con la Política de Tratamiento de Datos Personales adoptadas y con los principios de protección de datos personales establecidos en la Ley.
- La posibilidad de que la organización verifique por cuenta propia o a través de terceros independientes, por lo menos una (1) vez al año de forma aleatoria y en consideración de la sensibilidad de los datos tratados, el adecuado manejo de información de los diferentes usuarios externos en los términos establecidos en el contrato y la Ley como “Encargados del tratamiento de datos personales”.

En caso de transferencia de datos, la cual tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país, se atenderán los lineamientos de la Ley 1581 de 2012, Decreto 1074 de 2015 y normas reglamentarias.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	20 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

6.3.2.8 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO. Los diferentes sistemas de información estarán a disposición de todos los empleados como herramientas de trabajo, quienes serán responsables por la integridad de estos recursos y tendrán el deber de respetar los derechos de otros usuarios, la integridad de las instalaciones físicas y sus métodos de control, además de respetar los derechos de autor y la propiedad intelectual.

Todo el personal deberá tener asociado una cuenta de usuario y la asignación de perfiles de acceso, la cual deberá ser tramitada por el personal de gestión humana del Grupo Empresarial GreenLand, previamente autorizado.

Teniendo presente la naturaleza jurídica, administrativa y operativa de FEGREEN, la operación física y tecnológica se desarrolla soportado por la infraestructura tecnológica y en las instalaciones de la empresa vinculante, lo anterior será complementario y de obligatorio cumplimiento en lo que corresponda la POLÍTICA DE USO DE RECURSOS INFORMÁTICOS del Grupo Empresarial GreenLand.

6.3.2.9 POLÍTICA DE SEGURIDAD FÍSICA. Considerando que la operación física y tecnológica de FEGREEN se desarrolla soportado por la infraestructura tecnológica y en las instalaciones de la empresa vinculante, se complementará de forma obligatoria el cumplimiento en lo que corresponda las políticas de Seguridad BASC (Business Alliance for Secure Commerce) y al Código Internacional PBIP.

En torno a la seguridad se aplicarán los siguientes lineamientos:

- **Visitantes.** Para el ingreso de los visitantes a las instalaciones se hará un registro de la visita de conformidad con -los lineamientos señalados por el Grupo Empresarial GreenLand. Para este efecto, el ingreso que haga uso de biometría cumplirá lo establecido en la Ley 1581 de 2012 y normas reglamentarias.
- **Control de acceso.** Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida o zonas de especial protección deberán contar con controles de acceso que sólo permitan el ingreso a los colaboradores o personal autorizado.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	21 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

- **Centro de cómputo.** Considerando que la operación tecnológica de FEGREEN se desarrolla soportado por la infraestructura tecnológica y en las instalaciones de la empresa vinculante, por lo anterior, serán complementarias y de obligatorio cumplimiento las políticas señaladas en la materia por parte del Grupo Empresarial GreenLand.
- **Videovigilancia.** Con la finalidad de brindar seguridad a las personas, instalaciones y bienes, FEGREEN lo acoge el sistema de videovigilancia, grabaciones de la empresa vinculante, que serán de acceso restringido sólo al personal autorizado y cuentan con las medidas requeridas en cumplimiento a la ley 1581 de 2012 y normas reglamentarias.

6.3.2.10 POLÍTICA DE SISTEMA DE ADMINISTRACIÓN DE RIESGOS. FEGREEN gestionará los riesgos asociados con la seguridad de información y protección de los datos personales, esto, conforme a la estructura de control que enmarca integralmente los componentes de su ambiente de control, la gestión de riesgos, el sistema de control interno, la información, la comunicación y el monitoreo; que apoyan la gestión y desempeño organizacional para alcanzar los objetivos estratégicos.

La gestión integral de riesgos contribuye al logro de los objetivos estratégicos de FEGREEN y se extiende a la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los diferentes riesgos a los que pueda estar expuesto. También, a la gestión de los riesgos que puedan estar asociados a la estrategia, los procesos, los proyectos y la protección de recursos físicos y humanos, así como los relacionados con la sostenibilidad y continuidad de su actividad.

6.3.2.11 POLÍTICA DE GESTIÓN DE INCIDENTES. FEGREEN gestionará adecuadamente los incidentes de seguridad de la información y de datos personales garantizando la continuidad su actividad y el cumplimiento de las obligaciones legales y reglamentarias frente a la Superintendencia de Industria y Comercio.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa

	FONDO DE EMPLEADOS GREENLAND FEGREEN	Página:	22 de 22
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de Aprobación:	01 de agosto de 2022
		Versión:	2.0

7. MONITOREO Y CUMPLIMIENTO

El cumplimiento de esta política será revisada y evaluada periódicamente por la Gerencia y Jefe Fegreen. El incumplimiento se calificará como **FALTA GRAVE** y dará lugar a la terminación del vínculo laboral, de manera unilateral, con **JUSTA CAUSA**. En el caso de usuarios externos, el incumplimiento a la Política de Seguridad de la Información traerá consigo las consecuencias legales a que hubiere lugar.

8. VIGENCIA Y DIVULGACIÓN

Esta política fue aprobada por la Gerencia Administrativa, su vigencia se dará a partir de la fecha de aprobación y deroga cualquier política o procedimiento anterior contrario a esta.

Cargo	Elaboró	Aprobó
Jefe CAD del Grupo Empresarial GreenLand.	Oficial de Protección de Datos Personales	Gerencia Administrativa