# POLITICA GENERAL SEGURIDAD DE LA INFORMACIÓN

## CONTROL DE VERSIONES

| Fecha | Versión | Descripción | Autor | Responsable | Aprobado |
|---|---|---|---|---|---|
| 2023/07/08 | 001 | Inicio. | | Gerente general | Gerente general |
| 2024/05/03 | 002 | Se nombra la base de las políticas ISO 27001. | | Gerente general | Gerente general |
| 2025/06/25 | 003 | Se actualizan las responsabilidades para todo el personal. | | Gerente general | Gerente general |

| Fecha | Versión | Descripción | Revisado por | Aprobado por | Autor |
|---|---|---|---|---|---|
| 30/06/2026 | 004 | Actualización politica general seguridad de la información de acuerdo con los requisitos de la norma ISO/IEC 27001:2022, incorporación al Sistema de Control Documental y estandarización conforme a la plantilla institucional. | Gerente General y gerente TI | Gerente general y Gerente TI | Equipo de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI). |

CONTROL DE VERSIONES 1
1. DECLARACIÓN DE LA POLÍTICA 4
2. SEGURIDAD DE LA INFORMACIÓN 5
3. DIRECTRICES 5
4 OBJETIVO GENERAL DE LA POLÍTICA 6
4.1 OBJETIVOS ESPECÍFICOS DE LA POLÍTICA 6
5. ALCANCE DE LA POLÍTICA 6
6. DIFUSIÓN 7
7. PRINCIPIOS DE SEGURIDAD INFORMÁTICA 7
8. CUMPLIMIENTO 7
9. APLICABILIDAD 8
10. COMPROMISO DE LA DIRECCIÓN 8
11. MEJORA CONTINUA 9
12 REVISIÓN DE LA POLÍTICA GENERAL 9
13. ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN 10
14. ROLES Y RESPONSABILIDADES 11
15. LINEAMIENTOS DE ADMINISTRACIÓN DE SEGURIDAD INFORMÁTICA 30
16 POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN 31
17 IDENTIFICACIÓN DE ACTIVOS 34
18 IDENTIFICACIÓN DE AMENAZAS 35
19 IDENTIFICACIÓN DE VULNERABILIDADES 36
20. MARCO GENERAL DE POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN 37
37
21. ROLES Y RESPONSABILIDADES 40
22. EXCLUSIÓN DE LA POLÍTICA 41
23. VIOLACIONES DE LA POLÍTICA 41

## 1. **DECLARACIÓN DE LA POLÍTICA**

La política de seguridad de la información de Ideas Fractal S.A.S como proveedor del sector turístico tiene como objetivo garantizar la protección de los datos sensibles y los activos de información involucrados en la ejecución de los procesos que desarrolla la empresa en el ejercicio de su actividad, mediante un equipo calificado y comprometido con la seguridad de la información, garantizando la continuidad en las operaciones y procesos que soportan los objetivos del negocio y la mejora continua.

Ideas Fractal S.A.S, comprendiendo la importancia de la protección de la información como principal activo, se ha comprometido con la implementación, mantenimiento y mejora continua de la seguridad y privacidad de la Información llevando a cabo acciones para el buen uso de los datos de tarjetas aplicando la administración y gestión de riesgos para prevenir o minimizar el impacto sobre los activos de información. En este sentido, y de acuerdo con los lineamientos establecidos en la norma ISO/IEC 27001, ideas farctal S.A.S establece políticas de seguridad de la información, realiza procesos de identificación y análisis de riesgos, implementa controles de seguridad, desarrolla procesos de monitoreo, revisión continua, con el propósito de fortalecer el Sistema de Gestión de Seguridad de la Información. Así mismo, Ideas Fractal S.A.S. adopta los lineamientos del estándar de seguridad PCI DSS, el cual contribuye con el proceso de pago con tarjetas generando estrategias de buen uso y a la vez establecer controles de seguridad en la red.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de Ideas Fractal S.A.S con respecto a fortalecer los niveles de seguridad de la información y la protección de los activos de información que soportan los procesos de la organización y la implementación de un Modelo de Seguridad y Privacidad de la Información, mediante la generación y publicación de políticas, procedimientos, guías e instructivos, al igual, que la asignación de responsabilidades para

la gestión de la seguridad de la información y generar una cultura en seguridad y privacidad al interior de Ideas Fractal S.A.S.

## 2. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de políticas, procesos, procedimientos y controles orientados a proteger la información frente amenazas internas y externas. Al garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos, se asegura la continuidad del negocio y el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables

## 3. DIRECTRICES

- Verificar anualmente que las políticas de seguridad de la información se encuentren definidas, implementadas, mantenidas, revisadas y actualizadas.
- Confirmar anualmente que las políticas de seguridad de la información se encuentren comunicadas, comprendidas y aplicadas formalmente por todos los colaboradores.
- Establecer un Programa Integral de Seguridad de la Información y Cumplimiento PCI DSS, alineado con ISO/IEC 27001, que proteja los datos de tarjeta y la información crítica mediante un enfoque basado en riesgos, controles aplicables a todas las actividades, procesos y terceros que intervienen en la prestación del servicio.
- Contar con dispositivos y sistemas de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.
- Los lideres de área o dependencia deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su responsabilidad se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la Organización.
- Procesar, almacenar y transmitir datos implementando medidas de seguridad que prevengan la filtración de información asociada a tarjetas de pago.

## 4 OBJETIVO GENERAL DE LA POLÍTICA

El objetivo general de la presente política es establecer un marco de gestión de la seguridad de la información que garantice la protección de los activos de información de Ideas Fractal S.AS. asegurando la confidencialidad, integridad y disponibilidad de la información. Así mismo, busca promover el manejo seguro y responsable de los datos de los tarjetahabientes, cumpliendo con los lineamientos de la norma ISO/IEC 27001 y con los estándares de seguridad requeridos por PCI DSS, para minimizar riesgos, prevenir incidentes de seguridad y fortalecer la confianza de clientes, colaboradores y terceros vinculados a la organización.

### 4.1 OBJETIVOS ESPECÍFICOS DE LA POLÍTICA

- Fortalecer la postura de buen manejo de tarjetahabiente y de ciberseguridad a su vez a través de la implementación y sostenimiento de buenas prácticas de seguridad informática en Ideas Fractal S.A.S. con respecto al uso adecuado de los servicios informáticos puestos a disposición de los usuarios.
- Implementar controles físicos y lógicos en procura de la protección y privacidad, integridad, disponibilidad de la información de la organización.
- Garantizar la protección y tratamiento de datos personales, manejo adecuado de la información de reservas e información de las agencias de viaje conforme a la normativa vigente. en materia de protección de datos personales, especialmente la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás disposiciones aplicables, asegurando la confidencialidad, integridad y disponibilidad de la información.
- Optimizar los procesos de gestión en seguridad informática, estableciendo mecanismos que garanticen el mejoramiento continuo.
- Promover programas de formación y sensibilización en seguridad de la información dirigidos a los usuarios por parte del Coordinador de Calidad, Psicología Organizacional, Infraestructura y terceros, con el fin de crear y mantener una cultura organizacional orientada a la protección de la información.
- Desarrollar un plan de seguridad a través de la administración de riesgos que considere las amenazas y vulnerabilidades a los que se encuentra expuesta Ideas Fractal S.A.S para proteger toda aquella información crítica.
- Desarrollar y mantener un sistema de prevención alineado con los objetivos estratégicos de la organización, orientado a la protección y al uso eficiente de los recursos de información.

## 5. ALCANCE DE LA POLÍTICA

EL presente documento reglamenta y describe la **política general de seguridad y privacidad de la información**, definiciones, las políticas específicas, lineamientos, restricciones, proceso disciplinario y dependencias de apoyo para el fortalecimiento de los

procesos de gestión del riesgo informático y continuidad tecnológica en Ideas Fractal S.A.S. Adicionalmente esta política aplica a toda la información creada, procesado o utilizado a nivel corporativo, sin importar el medio, formato, presentación o lugar en cual se encuentre.

La **Política de Seguridad de la Información** cubre a todos los niveles de la organización, usuarios (que incluye empleados, agencias, y acompañantes) terceros (que incluye proveedores y contratistas) entes de control y entidades relacionadas que accedan ya sea interna o externamente a cualquier activo de información no importa su ubicación.

## 6. DIFUSIÓN

La política se publica y mantiene disponible a través de los canales institucionales definidos por la organización y en la página web corporativa, con el fin de garantizar su conocimiento, consulta y cumplimiento por parte de las partes interesadas. Adicionalmente, Ideas Fractal S.A.S promueve actividades de divulgación, formación y sensibilización para asegurar que los colaboradores comprendan y apliquen los lineamientos establecidos en la presente política

Así mismo, la Gerencia promoverá actividades de divulgación, formación y sensibilización para asegurar que los colaboradores comprendan y apliquen los lineamientos establecidos en la presente política.

## 7. PRINCIPIOS DE SEGURIDAD INFORMÁTICA

- **Confidencialidad:** La información solo podrá ser accedida, modificada y/o eliminada por quienes estén autorizados para ello.
- **Disponibilidad:** La información deberá estar accesible siempre que se requiera.
- **Integridad:** La información deberá preservar su veracidad y fidelidad a la fuente, independientemente del lugar y de la forma de almacenamiento y transmisión.
- **Autenticidad:** Principio que garantiza que la identidad de una persona, sistema o entidad es válida y verificable, y que la información proviene realmente de la fuente declarada, evitando suplantaciones o alteraciones no autorizadas.

## 8. CUMPLIMIENTO

La Política de Seguridad y Privacidad de la Información, la normatividad interna, procesos, procedimientos, estándares, controles y directrices derivados de aquella, son de obligatorio cumplimiento por los empleados, proveedores, agencias; al igual que propietarios,

custodios y usuarios de la información y, en general, toda persona natural o jurídica que acceda a cualquier activo de información de Ideas Fractal S.A.S.

Por consiguiente, se incorpora la observación, aplicación y cumplimiento de este documento en las funciones y asignaciones del personal que trabaja con Ideas Fractal S.A.S. de vinculación contractual y los procedimientos de reserva y confidencialidad de la información corporativa de la organización.

## 9. APLICABILIDAD

La gestión de la seguridad, privacidad y continuidad tecnológica se enfoca en el control de los riesgos actuales y potenciales de la información. Este enfoque se alinea con el impacto operativo y objetivos de la empresa, operando bajo el marco del estándar PCI-DSS y un SGSI conforme a la norma ISO/IEC 27001.

## 10. COMPROMISO DE LA DIRECCIÓN

La Gerencia de Ideas Fractal S.A.S., declara estar comprometida con la seguridad de la información, como uno de sus activos más importantes, por lo tanto, manifiesta su total compromiso con el establecimiento, implementación y gestión de buenas prácticas de seguridad de la información y buen uso de los datos de tarjeta habiente. En este sentido la Gerencia general reconoce la importancia de proteger la información como uno de los activos más valiosos de la organización.

Se compromete con la implementación, mantenimiento y mejora continua del sistema de Gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción de una cultura organizacional orientada a la seguridad de la información y la gestión de riesgos.
- Facilitar la divulgación de las políticas asociadas con seguridad de la información a todos los colaboradores de la organización.
- El ejercicio de liderazgo activo y la responsabilidad final sobre la eficacia del Sistema de Gestión de Seguridad de la Información.
- La integración de los requisitos del SGSI en los procesos estratégicos y operativos de la organización.
- La asignación y aseguramiento de los recursos necesarios para implementar, mantener y mejorar continuamente el SGSI.

- La verificación, seguimiento y evaluación del cumplimiento de las políticas y controles establecidos.
- La gestión adecuada de los riesgos de seguridad de la información, garantizando que toda decisión relacionada con la aceptación de riesgos sea evaluada y aprobada exclusivamente por el Gerente general.
- Ningún riesgo podrá ser asumido de manera individual por áreas, procesos o responsables del SGSI sin la debida aprobación formal del Gerente general.
- El compromiso de que todas las decisiones y actuaciones en materia de seguridad de la información se mantendrán alineadas con la legislación aplicable y demás requisitos regulatorios vigentes.

## 11. MEJORA CONTINUA

Ideas Fractal S.A.S. establece el compromiso de mejorar continuamente la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a los requisitos de la norma ISO/IEC 27001.

La mejora continua se garantizará mediante:

- El seguimiento, medición, análisis y evaluación del desempeño del SGSI y de sus objetivos de seguridad de la información.
- La ejecución de auditorías internas planificadas para verificar la conformidad del sistema con los requisitos normativos y organizacionales.
- La revisión por la gerencia general, asegurando su alineación con el direccionamiento estratégico y el contexto organizacional.
- La gestión oportuna por la gerencia general de no conformidades, incidentes de seguridad de la información y hallazgos, mediante la implementación de acciones correctivas eficaces.
- La actualización periódica de la evaluación y tratamiento de riesgos, considerando cambios internos y externos que puedan afectar la seguridad de la información.
- La organización aplicará un el enfoque basado en el ciclo PHVA (planificar, hacer, verificar, actuar) como modelo de gestión, fortaleciendo la capacidad del SGSI para proteger la confidencialidad, integridad, y disponibilidad de la información.

## 12 REVISIÓN DE LA POLÍTICA GENERAL

La presente política es revisada al menos una vez al año y se actualiza cuando se presenten cambios relevantes en la estructura organizacional, en los objetivos del negocio o cuando se identifiquen nuevos riesgos o cambios significativos en los entornos tecnológicos y de información.

La revisión y actualización de esta política es responsabilidad del Gerente General, en conjunto con representantes de Talento Humano, Calidad, Seguridad Salud en el Trabajo, y Tecnologías de la Información (TI). Estos responsables velarán por su adecuada actualización y por la comunicación oportuna de cualquier modificación al interior de Ideas Fractal S.A.S.

Así mismo, los cambios relevantes serán incorporados en los contratos y acuerdos que Ideas Fractal S.A.S. establezca con empleados, contratistas y terceros, con el fin de garantizar el conocimiento y cumplimiento de los lineamientos de seguridad de la información.

Adicionalmente, el Gerente General será responsable de coordinar y designar a los responsables para el cumplimiento del programa anual de auditoría informática y de ciberseguridad implementado en la organización, con el objetivo de evaluar el nivel de madurez, efectividad y cumplimiento de los controles de seguridad establecidos, así como identificar oportunidades de mejora para el fortalecimiento del Sistema de Gestión de Seguridad de la Información.

## 13. ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN

### Organización Interna

Ideas Fractal S.A.S. ha definido dentro de su estructura organizacional el rol de Gerente de TI, quien es responsable de liderar, coordinar y ejecutar las actividades relacionadas con la operación, gestión y administración de la seguridad de la información en la organización.

Estas funciones se desarrollan en alineación con las buenas prácticas establecidas en la norma ISO/IEC27001, asegurando la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de Ideas Fractal S.A.S. Entre sus responsabilidades se incluyen la identificación y valoración de los activos de información, la gestión de riesgos asociados, la definición de controles de seguridad adecuados y el seguimiento al cumplimiento de los mismos.

Adicionalmente, el Gerente de TI garantiza que las operaciones de seguridad informática y los controles de ciberseguridad estén alineados con los estándares de PCI DSS, con especial énfasis en la protección de los datos de los tarjetahabientes y la salvaguarda de los activos de información críticos de Ideas Fractal S.A.S.

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información, en especial las relacionadas con las dependencias involucradas en los diferentes procedimientos corporativos que permiten el acceso a la información protegida e información corporativa.

## 14. ROLES Y RESPONSABILIDADES

### Dependencia/ Roles

#### Gerente General

- Asignar responsabilidades sobre temas de seguridad de la información a las áreas y personas correspondientes.
- Apoyar, facilitar y mantener relaciones con entidades especializadas en seguridad de la información.
- Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información.
- Verificar el cumplimiento de los controles.
- Dirigir acciones específicas que promuevan un ambiente seguro.
- Gestionar recursos para programas de capacitación y formación.
- Dirigir, planificar y coordinar las estrategias, políticas y controles de seguridad de la información en Ideas Fractal S.A.S, garantizando la confidencialidad, integridad y disponibilidad de los datos, así como el cumplimiento de normativas legales vigentes
- Aprobar los lineamientos estratégicos y planes de acción en materia de seguridad.
- Promover una cultura organizacional orientada a la protección de la información.
- Revisar y aprobar planes de respuesta ante incidentes graves, planes de continuidad de negocio y recuperación ante desastres.

**Gerente TI**

- Liderar, coordinar y supervisar la gestión de la seguridad de la información asegurando la correcta implementación, mantenimiento y mejora continua.
- Identificar vulnerabilidades y garantizar seguimiento que puedan afectar la confidencialidad, integridad y disponibilidad de la información evaluando el riesgo y estableciendo acciones correctivas o preventivas.
- Supervisar la implementación de controles de seguridad verificando su adecuada aplicación, eficacia y alineación con los riesgos identificado.
- Liderar y analizar incidentes de seguridad garantizando un tratamiento oportuno, y acciones de mejora.
- Validar soluciones antimalware/antivirus activas y actualizadas.
- Verificar la actualización y exactitud del inventario de activos de información, garantizando su adecuada identificación, clasificación y control.
- Actualizar los estándares de configuración de infraestructura.
- Garantizar la eficiencia de los sistemas asegurando su adecuado funcionamiento mediante la implementación de controles de seguridad.
- Dirigir, planificar y coordinar las estrategias, políticas y controles de seguridad de la información en Ideas Fractal S.A.S., garantizando la confidencialidad, integridad y disponibilidad de los datos, así como el cumplimiento de normativas legales vigentes.
- Garantizar el cumplimiento de políticas normas y procedimientos de seguridad.
- Asegurar que los controles estén actualizados frente a nuevas amenazas y riesgos.
- Coordinar investigaciones ante brechas de seguridad y liderar las acciones correctivas.
- Definir y liderar la estrategia integral de seguridad de la información alineada con los objetivos del negocio.

**Ingeniero Senior de infraestructura**

- Dar cumplimiento al programa PCI DSS.
- Reportar a la alta dirección los controles del cumplimiento PCI DSS
- Proponer estrategias que garanticen la seguridad de la información
- Identificar y reportar los riesgos, eventos o incidentes para analizar el seguimiento y control.
- Formular procesos de control, calidad y protección de datos
- Planear estrategias para la seguridad de los datos, el acceso a la red y sistemas de la información.
- Actualizar los estándares de configuración de infraestructura.
- Establecer estrategias para la identificación de amenazas potenciales
- Monitorear el plan de mitigación de riesgos de seguridad de la información. *Y* analizar las evaluaciones de riesgo asociadas, en coordinación con Gerente TI, con el fin de asegurar la implementación y seguimiento de los controles definidos.
  • Auditar los terceros dentro del alcance PCI DSS
- Reportar los avances a Gerencia general de acuerdo con lo requerido en el estándar.
- Difundir la importancia de una gestión de seguridad de la información a las partes interesadas, cumpliendo con los requisitos PCI DSS.
- Sugerir y apoyar en la elaboración de lineamientos y procedimientos de seguridad de la información dentro de sus respectivas áreas de proceso

**Gerente de Desarrollo de Software**

- Promover el uso adecuado del servicio garantizando el cumplimiento de lineamientos y políticas relacionados con seguridad de la información.

- Establecer soluciones técnicas seguras que incorporen controles de seguridad desde su diseño, garantizando la protección de la información, la adecuada gestión de accesos y la mitigación de vulnerabilidades.

- Desarrollar requerimientos funcionales y no funcionales incorporando criterios de seguridad de la información, asegurando que desde la etapa de análisis se identifiquen riesgos, controles de acceso,
- Ejecutar acciones para mitigar riesgos identificados, conforme a los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información.
- Promover el buen uso de los recursos informáticos con el personal de la empresa
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información
- Promover la capacitación continua del equipo de desarrollo en prácticas de seguridad de software.
- Analizar que los entornos de desarrollo, pruebas y producción estén debidamente segregados, controlados y protegidos, evitando accesos no autorizados
- Sensibilizar sobre amenazas comunes y errores de codificación inseguros.
- Asegurar que los entornos de desarrollo, pruebas y producción estén debidamente segmentados y protegidos.

**Gerente Financiero**

- Contribuir a la prestación segura de los servicios ofrecidos a los clientes, asegurando el adecuado tratamiento de la información sensible.
- Velar por el cumplimiento de políticas de seguridad y controles de seguridad de la información asegurando la adopción de medidas correctivas cuando se identifiquen desviaciones.
- Sensibilizar al personal sobre la importancia de proteger la confidencialidad de la información y garantizar su adecuado tratamiento conforme a las políticas establecidas.
- Promover el buen uso de los recursos informáticos con el personal de Ideas Fractal S.A.S.

- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Garantizar que los estados financieros e informes contables sean elaborados, almacenados y transmitidos bajo condiciones de seguridad que aseguren su confidencialidad, integridad y disponibilidad, conforme a las políticas de seguridad de la información y a la normativa legal aplicable.
- Notificar y coordinar oportunamente la gestión de incidentes que afecten la información financiera, asegurando la implementación de acciones correctivas dentro de su ámbito de responsabilidad y colaborando con el equipo encargado del SGSI.

**Gerente Comercial**

- Contribuir al manejo seguro de los servicios prestados a los clientes, asegurando la protección de la información comercial y contractual durante su tratamiento, conforme a las políticas de seguridad de la información y a los acuerdos establecidos con los clientes.
- Velar por el cumplimiento de las políticas, lineamientos y controles de seguridad de la información dentro del área comercial, asegurando su adecuada aplicación en la gestión de clientes y procesos contractuales.
- Supervisar el uso, acceso y divulgación de la información comercial y estratégica en los procesos de propuestas y negociaciones, asegurando que únicamente sea compartida con partes autorizadas y bajo los mecanismos de confidencialidad definidos por Ideas Fractal S.A.S.
- Fomentar el uso adecuado de los recursos tecnológicos en la interacción con clientes, asegurando que el tratamiento de su información se realice bajo los controles establecidos en el SGSI y en cumplimiento de los acuerdos de confidencialidad y requisitos contractuales.
- Garantizar la confidencialidad, integridad y disponibilidad de la información relacionada con los clientes.
- Asegurar la adecuada protección de los datos sensibles de los clientes, verificando que su acceso, uso, almacenamiento y divulgación se realicen exclusivamente por personal autorizado y bajo los controles definidos en el SGSI.

**Analista Senior Comercial**

- Garantizar la confidencialidad y uso autorizado de la información dando cumplimiento con las políticas internas y regulaciones de protección de datos.
- Reportar incidentes incluyendo aquellos relacionados con la seguridad de la información, para permitir acciones correctivas o preventivas.
- Promover el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
- Promover buenas prácticas en la gestión del servicio al cliente, asegurando la confidencialidad, integridad y adecuado uso de la información del cliente.
- Contribuir al cumplimiento de controles relacionados con clasificación de la información, control de accesos y protección de datos personales.
- Utilizar el sistema CRM conforme a las políticas y procedimientos de seguridad de la información, protegiendo los datos de clientes y comerciales, y evitando compartir credenciales o permitir accesos no autorizados.
- Validar que la información incluida en el contrato sea completa, veraz y actualizada.
- Administrar y controlar la cartera de clientes/agentes, asegurando la correcta gestión de pagos, cobros y estados de cuenta, garantizando la confidencialidad de la información.
- Realizar el seguimiento a las propuestas comerciales presentadas a clientes, asegurando la adecuada gestión de la información.

- Identificar y gestionar los cambios que deban ser notificados (tarifas, condiciones, alcance del servicio.

- Gestionar la aplicación, recolección y análisis de encuestas de satisfacción de clientes externos, garantizando el tratamiento adecuado de los datos y la protección de la información.

- Brindar atención oportuna y efectiva a clientes, garantizando la correcta gestión de sus solicitudes, consultas y reclamos, asegurando la protección de la información.

- Diseñar y ejecutar estrategias para promover el uso de productos o servicios.

- Desarrollar e implementar estrategias de fidelización que fortalezcan la relación con los clientes, promoviendo la retención y lealtad, garantizando el uso adecuado y seguro de la información.

- Garantizar que solo el personal autorizado tenga acceso a la información.

**Coordinador de Calidad y seguridad y salud en el trabajo**

- Sugerir y apoyar en la elaboración de lineamientos y procedimientos de seguridad de la información dentro de sus respectivas áreas de proceso
- Garantizar la confidencialidad y uso autorizado de la información.
- Informar y registrar oportunamente incidentes de seguridad de la información, no conformidades y oportunidades de mejora identificadas en los procesos a su cargo, asegurando su análisis y seguimiento conforme a los lineamientos del SGSI y promoviendo acciones correctivas que fortalezcan la mejora continua.
- Divulgar políticas de seguridad de la información a todo el personal de la Ideas Fractal S.A.S., asegurando su adecuada comprensión.
- Promover el buen uso de los recursos informáticos con el personal de Ideas Fractal S.A.S.
- Participar, diseñar, coordinar y ejecutar los entrenamientos, capacitaciones y programas de sensibilización en temas de seguridad de la información, asegurando la toma de conciencia del personal y el fortalecimiento de la cultura organizacional conforme a los lineamientos del SGSI.

- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
- Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
- Apoyar el cumplimiento de controles relacionados con concienciación, gestión documental y mejora continua.
- Vigilar y monitorear los riesgos de seguridad de la información identificados, realizando seguimiento periódico a los controles implementados y al cumplimiento del plan de tratamiento de riesgos definido por Ideas Fractal S.A.S.
- Administrar el control documental de la organización, asegurando la creación, revisión, aprobación, actualización y distribución de los documentos del sistema de gestión, así como mantener actualizado el libro maestro de documentos, garantizando el control de versiones y la disponibilidad de la documentación vigente para los procesos de Ideas Fractal S.A.S.

**Psicología Organizacional**

- Garantizar el manejo reservado y seguro de la información del personal, laboral y sensible a la que tenga acceso en el ejercicio de sus funciones, evitando su divulgación no autorizada y asegurando su tratamiento conforme a los lineamientos del SGSI y la normativa aplicable en protección de datos.
- Usar la información exclusivamente con fines autorizados conforme a los lineamientos del SGSI.
- Asistir y participar activamente en las capacitaciones y actividades de sensibilización en seguridad de la información definidas por el SGSI.
- Reportar incidentes y oportunidades de mejora conforme a los lineamientos del SGSI.
- Promover el buen uso de los recursos informáticos con el personal de Ideas Fractal S.A.S.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Apoyar, planificar, implementar y evaluar los entrenamientos, capacitaciones y programas de sensibilización en seguridad de la información, garantizando la toma de conciencia y el cumplimiento de los lineamientos del SGSI

**Analista de Talento Humano**

- Recibir y custodiar documentos con información sensible.
- Informar al personal sobre el buen uso de la información.
- Asegurar que los empleados y contratistas durante el proceso de selección, comprendan sus responsabilidades, los términos y las condiciones de contratación.
- Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
- Notificar a coordinación de calidad sobre el personal que ingresa a laborar en Ideas Fractal S.A.S. con el fin de liderar sus obligaciones respecto del cumplimiento de las Políticas de Seguridad de la información y de todas las normas, procedimientos y prácticas que de ella se deriven.
- Dar cumplimiento con la firma de un acuerdo de confidencialidad definido, y aprobado por gerente general.
- Informar al personal contratado con respecto a la importancia de cuidar, proteger la información suministrada en Ideas Fractal S.A.S.
- Velar por el cuidado de la información, informando al personal que ingresa sobre la importancia sobre el buen manejo del servicio.
- Contribuir con el buen uso de la información relacionada con los clientes como con personal interno.
- Promover el buen uso de los recursos informáticos con el personal de la empresa.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

- Vigilar y monitorear los riesgos de seguridad de la información identificados, realizando seguimiento periódico a los controles implementados y al cumplimiento del plan de tratamiento de riesgos definido por Ideas Fractal S.A.S.
- Utilizar el sistema CRM conforme a las políticas y procedimientos de seguridad de la información, protegiendo los datos de clientes y comerciales, y evitando compartir credenciales o permitir accesos no autorizados.
- Validar que la información incluida en el contrato sea completa, veraz y actualizada.
  .

**Analista de Compras y pago a Proveedores**

- Ejecutar las verificaciones de seguridad y validación documental (Cámara de Comercio, RUT, documento de identidad, entre otros), según corresponda, para mitigar riesgos asociados a terceros.
- Mantener confidencialidad de proveedores y pagos, asegurando su manejo seguro y restringido únicamente a personal autorizado.
- Proteger la información financiera y bancaria evitando accesos no autorizados o divulgación indebida.
- Reportar de manera inmediata cualquier incidente, evento sospechoso o situación que pueda comprometer la seguridad de la información, especialmente aquellos relacionados con proveedores, transacciones financieras, accesos no autorizados, fraude o uso indebido de información.
- No divulgar información sensible de proveedores o transacciones, garantizando su uso exclusivo para fines laborales y por personal autorizado.
- Promover el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Gestionar el inventario de activos de información de la organización, garantizando su identificación, clasificación, actualización y control, así como la asignación de responsables y la implementación de medidas que contribuyan a la protección de los activos frente a riesgos de seguridad de la información.
- Administrar y mantener actualizado el inventario de proveedores de Ideas Fractal S.A.S., asegurando el registro, clasificación y control de los terceros que suministran bienes o servicios, así como la actualización de su información y la verificación del cumplimiento de los requisitos establecidos por Ideas Fractal S.A.S.

**Analista de Facturación y Cartera**

- Aplicar y dar cumplimiento a las políticas, procedimientos y controles de seguridad de la información establecidos por el SGSI en la gestión de facturación, cartera y manejo de información financiera.
- Garantizar la confidencialidad y el uso adecuado de la información financiera y de clientes bajo su responsabilidad, conforme a los lineamientos del SGSI.
- Reportar oportunamente incidentes de seguridad de la información y promover el uso adecuado y seguro de los servicios y recursos asignados, conforme a los lineamientos del SGSI.
- Promover el buen uso de los recursos informáticos conforme a las políticas y controles establecidos en el SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
- Gestionar la información relacionada con procesos de facturación, recaudo y cartera dentro de las plataformas autorizadas por la organización, garantizando el uso adecuado, confidencialidad, integridad y disponibilidad de la información a la que tiene acceso.

- Administrar y controlar la cartera de clientes/agentes, asegurando la correcta gestión de pagos, cobros y estados de cuenta, garantizando la confidencialidad de la información.

**Ingeniero Senior de Infraestructura**

- Velar por la implementación de medidas de seguridad en infraestructura tecnológica.
- Supervisar configuraciones seguras en los sistemas y redes.
- Garantizar la disponibilidad de los servicios tecnológicos para apoyar la continuidad del negocio.
- Participar en auditorías técnicas y controles internos.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Promover y garantizar el uso adecuado, seguro y eficiente de la infraestructura tecnológica, implementando y supervisando controles que aseguren la protección de los activos de información conforme a los lineamientos del SGSI.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

**Coordinador de Desarrollo**

- Velar por la aplicación y cumplimiento de las políticas y controles de seguridad de la información en los procesos de desarrollo de software, conforme a los lineamientos del SGSI. Promover auditorías en el área.
- Asegurar que el personal a su cargo conozca, comprenda y cumpla sus responsabilidades en materia de seguridad de la información conforme a los lineamientos del SGSI.
- Promover el uso adecuado del servicio conforme a los lineamientos del SGSI.

- No divulgar información confidencial a terceros no autorizados y garantizar su protección conforme a los lineamientos del SGSI.
- Promover con el personal el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información

**Ingeniero Senior de Desarrollo**

- Promover y asegurar el uso adecuado, seguro y controlado de los recursos tecnológicos en los procesos de desarrollo, conforme a los lineamientos del SGSI.
- Garantizar la ejecución de pruebas de software y el análisis de implementaciones seguras, asegurando que los desarrollos cumplan con los controles de seguridad definidos en el SGSI.
- Dar cumplimiento a las políticas, procedimientos y controles de seguridad de la información establecidos por el SGSI en el desarrollo y mantenimiento de software.
- Verificar la correcta implementación y funcionamiento de los controles de acceso a sistemas, aplicaciones y entornos de desarrollo, conforme a los lineamientos del SGSI.
- Promover el buen uso de los recursos informáticos con el personal de Ideas Fractal S.A.S.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Utilizar la información confidencial recibida únicamente para fines autorizados al momento de su entrega, conforme a los lineamientos del SGSI.

**Ingeniero Junior de Desarrollo**

- Analizar el funcionamiento del servicio y reportar fallas, vulnerabilidades o desviaciones que puedan afectar la seguridad o disponibilidad, conforme a los lineamientos del SGSI.
- Orientar de manera eficaz sobre la asignación y uso adecuado de accesos a sistemas y aplicaciones, conforme a los lineamientos del SGSI.
- Ejecutar pruebas y análisis técnicos bajo criterios de seguridad, asegurando el cumplimiento de los lineamientos del SGSI.
- Identificar y corregir oportunamente deficiencias del sistema que puedan afectar la seguridad, integridad o disponibilidad de la información, conforme a los lineamientos del SGSI.
- Promover el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

**Técnico de Desarrollo**

- Promover uso adecuado del servicio conforme a los lineamientos del SGSI.
- Proponer mejoras técnicas. que fortalezcan la seguridad, estabilidad y desempeño del servicio, conforme a los lineamientos del SGSI.
- Verificar el correcto funcionamiento del servicio y desarrollar requerimientos técnicos bajo criterios de seguridad, conforme a los lineamientos del SGSI.
- Ejecutar acciones orientadas a mitigar riesgos de seguridad de la información identificados en su proceso, conforme a los lineamientos del SGSI.

- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Promover con el personal el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

**Director de soporte**

- Asegurar el cumplimiento de las políticas, procedimientos y controles de seguridad de la información en el proceso de soporte técnico.
- Supervisar la atención, registro, análisis y cierre de incidentes de seguridad de la información relacionados con la operación del servicio.
- Verificar la correcta gestión de accesos a sistemas y plataformas bajo su responsabilidad.
- Garantizar la continuidad y disponibilidad de los servicios tecnológicos gestionados por el área de soporte.
- Asegurar que el personal de soporte conozca y cumpla sus responsabilidades en materia de seguridad de la información.
- Informar oportunamente vulnerabilidades, riesgos u oportunidades de mejora identificadas en la operación del servicio.

- Promover con el personal el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.

- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.

- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

**Coordinador de soporte**

- Supervisar que el equipo de soporte cumpla las políticas y procedimientos de seguridad de la información.

- Coordinar el registro, atención y escalamiento oportuno de incidentes de seguridad de la información.

- Asegurar el manejo confidencial de la información de clientes y usuarios durante la prestación del soporte.

- Monitorear el funcionamiento del servicio e informar riesgos o vulnerabilidades detectadas.

- Promover con el personal el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.

- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.

- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

**Analista de Soporte Nivel I**

- Realizar pruebas técnicas bajo criterios de seguridad, verificando que los cambios o soluciones implementadas no afecten la confidencialidad, integridad o disponibilidad de la información, conforme a los lineamientos del SGSI.
- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos por el SGSI en la ejecución de sus funciones.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Promover con los usuarios el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Mantener la confidencialidad de la información a la que tenga acceso, evitando su divulgación no autorizada y cumpliendo los lineamientos del SGSI.
- Reportar oportunamente incidentes de seguridad de la información y abstenerse de divulgar información confidencial sin autorización, conforme a los lineamientos del SGSI.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

**Analista de Soporte Nivel II**

- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos por el SGSI en el desarrollo de sus funciones.

- Participar activamente en los programas de capacitación y sensibilización en seguridad de la información definidos por el SGSI.
- Reportar oportunamente cualquier incidente o evento que pueda afectar la seguridad de la información, conforme a los lineamientos del SGSI.
- Mantener confidencialidad de la información y utilizarla únicamente para fines autorizados por Ideas Fractal S.A.S.
- Promover el uso adecuado, seguro y responsable de los recursos informáticos conforme a los lineamientos del SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.

.

**Coordinador de QA**

- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos por el SGSI en las actividades de aseguramiento de calidad.
- Implementar procedimientos de análisis de calidad
- Promover el uso correcto, seguro y conforme a los lineamientos del SGSI en la prestación y operación del servicio.
- Promover el buen uso de los recursos informáticos con el personal a cargo.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
- Hacer uso de los elementos de seguridad y doble factor de autenticación.

**Asistente QA**

- Monitorear continuamente el desempeño y la disponibilidad de los sistemas críticos para garantizar su funcionamiento seguro.
- Asegurar que las pruebas y controles de calidad cumplan con los estándares de seguridad establecidos.
- Restringir el acceso a información sensible únicamente al personal autorizado y supervisar su correcto uso.
- Promover el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
- Reportar inmediatamente cualquier incidente o vulneración de seguridad detectada.

**Diseñador Web**

- Asegurar que los accesos se otorguen únicamente a personas autorizadas y de acuerdo con las políticas de seguridad.
- Garantizar que las actividades de diseño y desarrollo se realicen de acuerdo con los estándares de seguridad y calidad de Ideas Fractal S.A.S.
- Aplicar los procesos de control y validación antes de implementar cualquier cambio en sistemas o plataformas web.
- Reportar cualquier desviación o dificultad en la aplicación de los procedimientos para que se tomen acciones correctivas.

- Aplicar buenas prácticas de seguridad al manejar información digital, tanto en sistemas internos como en plataformas web.
- Promover el uso adecuado, responsable y seguro de los recursos informáticos, conforme a los lineamientos del SGSI.
- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
- Asegurar que el contenido publicado en el sitio Wed oficial, correo electrónico, redes sociales, y piezas digitales no se revele información sensible, ni datos personales.
- Velar porque el uso de la imagen corporativa, logotipos y materiales institucionales se realice de acuerdo con los lineamientos establecidos en la empresa y evitar el uso indebido en contextos no autorizados.
- Utilizar de forma segura las herramientas de diseño, CMS, gestores de contenido, o plataformas de redes sociales, protegiendo credenciales evitando compartir accesos no autorizados.
- Verificar que los componentes sociales implementados en el sistema (formularios, Landing, Pages, correos HTML, etc) no generen vulnerabilidades o exposición de información especialmente en campos de captura de datos.

## 15. LINEAMIENTOS DE ADMINISTRACIÓN DE SEGURIDAD INFORMÁTICA

El Gerente TI de Ideas Fractal S.A.S. desarrolla un proyecto orientado a la implementación de las mejores prácticas, mediante el cual se gestionará la Seguridad de la información como un proceso sistemático, documentado y conocido por Ideas Fractal S.A.S.

Los lineamientos de seguridad de la información complementan el procedimiento que gestiona y define los niveles de seguridad, analizando las brechas de seguridad existentes y los incidentes presentados, a partir de los cuales genera planes que permiten reducir los niveles de riesgo a los cuales está expuesta Ideas Fractal S.A.S.

El Gerente TI debe garantizar que las políticas de seguridad sean revisadas regularmente y que refleje las necesidades de Ideas Fractal S.A.S., al igual que establecer una estructura organizacional en términos de seguridad basada en roles y responsabilidades.

Así mismo, establece mecanismos que permiten proteger los activos claves de Ideas Fractal S.A.S. por tanto, estos activos deben ser claramente identificados y analizados para comprender el nivel de criticidad de cada uno de ellos frente a los impactos que puedan generar por pérdidas en la confidencialidad, integridad y disponibilidad de los mismos.

La implementación de los controles debe realizarse mediante un procedimiento formal de gestión de cambios y liberaciones, garantizando la ejecución de las pruebas requeridas, así como la elaboración y establecimiento formal de los procedimientos necesarios para su adecuada operación.

Así mismo, este proceso mantiene una relación estrecha con los lineamientos de gestión de incidentes y monitoreo de seguridad, dada la necesidad de identificar, registrar y gestionar de manera oportuna los incidentes de seguridad de la información que puedan presentarse.

## 16 POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Ideas Fractal S.A.S considera como normas básicas de seguridad que deben ser garantizadas las siguientes:

- La información y los sistemas informáticos y telemáticos que la generan, procesan, almacenan e intercambian información con clientes, proveedores y otras sociedades en el desempeño de sus funciones y servicios serán considerados activos de información de Ideas Fractal S.A.S.
- Los activos de información de Ideas Fractal S.A.S. serán adecuadamente protegidos conforme a su valor y criticidad. Para determinar qué medidas de protección son necesarias, debe realizarse una estimación y evaluación del riesgo al que dichos activos se encuentran expuestos utilizando para ello la metodología utilizada en la construcción del PCI DSS y los criterios establecidos por la propia Entidad como actividad previa al análisis y gestión del riesgo.
- Debe también asegurar la confidencialidad, integridad y disponibilidad y autenticidad de la información y de los sistemas de información relacionados con los servicios que ofrece utilizando para ello el marco de los requisitos de la norma PCI DSS. Para ello se desarrollarán las diferentes normas y procedimientos que se consideren necesarias para cumplir con los principios de protección y normas definidas en la presente Política de Seguridad.

- El acceso de todo usuario a información de Ideas Fractal S.A.S. deberá ser autorizado y la asignación de sus privilegios de seguridad estará determinada por la necesidad de utilización de dicho activo en el desempeño de sus funciones.
- El personal de Ideas Fractal S.A.S. y cualquier otro personal que trabaje bajo contrato para la misma deberá acceder exclusivamente a aquella información que sea estrictamente necesaria para el desempeño de sus funciones y la utilizará exclusivamente para la realización de las distintas funciones operativas que desempeña para Ideas Fractal S.A.S. Cualquier acceso o utilización para finalidades distintas a las establecidas se considerará una infracción de la política de seguridad.
- Ideas Fractal S.A.S. garantizará que la información y la capacidad de su procesamiento manual y automático, sean resguardada y recuperada eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de los servicios de la empresa tal como se defina en su estrategia de continuidad de negocio.
- Ideas Fractal S.A.S. cumplirá los requisitos de seguridad establecidos por las leyes y reglamentos en vigor en sus diferentes ámbitos de actuación.
- Todos los empleados de Ideas Fractal S.A.S. participarán de forma activa en esta cultura de prevención y protección de activos. Deben para ello actuar de acuerdo a la presente política y aquellas normas y procedimientos de seguridad elaborados y comunicados por Ideas Fractal S.A.S.

- Ideas Fractal S.A..S concienciará y formará a su personal sobre la importancia que tiene para el desarrollo de sus actividades y servicios el garantizar la seguridad de la información que maneja y procesa.
- Los empleados de las compañías y terceros que presten servicios de cualquier índole a Ideas Fractal S.A.S. que tengan acceso a los recursos informáticos y telemáticos, así como a información de Ideas Fractal S.A.S. estarán igualmente obligados en sus acciones a que éstas cumplan con los requisitos de seguridad que se establezcan en la presente Política de Seguridad y en los documentos derivados de ella.
- Para asegurar la continuidad y sistemática adecuación de la seguridad a sus requisitos se ha implantado un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme con la norma PCI DSS.
- El área de infraestructura es la única facultada para administrar y configurar el acceso a los recursos de infraestructura tecnológica.
- Las credenciales de acceso de los usuarios administradores de la infraestructura tecnológica, servidores, aplicaciones y en general cualquier componente de tecnología, debe ser entregada en sobre sellado a la Gerencia para ser almacenada en caja fuerte de la compañía.
- Se monitorea el tráfico entrante y saliente, así como el tráfico de red interna para todas las plataformas de la compañía a través de una herramienta para detectar posibles intrusos e incidentes de seguridad.

- El manejo de la información y los servicios en la nube están autorizados siempre y cuando se cumpla con los niveles de seguridad y confidencialidad, de tal forma que se garantice que la información esté y se maneje a través de sitios seguros, que exista un contrato de servicio y el proveedor cumpla con los requerimientos de la norma ISO 27001: y PCI DSS DSS
- Todo aplicativo que se libere en el ambiente de producción y preproducción debe salir con certificado digital emitido por una entidad certificadora autorizada, utilizar el protocolo https y TLS según lo establecido en el estándar PCI DSS DSS, así como cumplir con el ciclo de seguridad para desarrollo de aplicaciones que incluye pruebas de seguridad y análisis estático al código fuente.
- La información que sea extraída de las bases de datos y que corresponda a información de los clientes y de lo cual se guarda backup a través de medios removibles como cintas, dvd, cd, u otro dispositivo de almacenamiento deben permanecer cifrada con criptografía sólida y bajo custodia, en condiciones de seguridad.
- Para la asignación de privilegios en el ambiente de producción su acceso estará sujeto a la aprobación y solicitud del jefe inmediato.
- El uso de internet es únicamente para actividades relacionadas con las funciones del negocio, manteniéndose las restricciones de seguridad establecidas por Ideas Fractal S.A.S.
- El uso de servicios de mensajería instantánea como hangouts y Skype entre otros se utilizan para actividades de Ideas Fractal S.A.S así como el acceso a las redes sociales, estará autorizado solo a usuarios específicos teniendo en cuenta sus funciones y necesidades del negocio.
- Solo se permite el acceso a la red de internet corporativa a los equipos que están en el inventario de Ideas Fractal S.A.S. y tengan control absoluto por parte del área de infraestructura, cualquier otro equipo deberá contar con autorización previa según los criterios de seguridad de Ideas Fractal S.A.S.
- Para clientes, visitantes como aliados estratégicos, consultores, freelance y proveedores se habilitará el acceso a la red pública de internet mediante una solicitud vía correo electrónico por parte del funcionario responsable al gerente TI su respectiva aprobación. El área de infraestructura es la responsable de habilitar y deshabilitar el usuario de acuerdo con el periodo autorizado.
- No se permite el uso de los recursos de internet corporativa para la descarga, distribución y/o reproducción de música, videos y similares.
- No se permite la creación de usuarios genéricos en la plataforma tecnológica de Ideas Fractal S.A.S., todo usuario es nombrado y tiene un responsable de su acceso y contraseña con los privilegios que le han sido otorgados.
- Los directores o jefes de área son los únicos autorizados para solicitar y retirar los accesos a los aplicativos corporativos de producción.

- Por la naturaleza de las aplicaciones de la compañía existen usuarios administradores, los cuales están a cargo del personal que asigna Gerente general.
- Todo usuario asignado a un funcionario de Ideas Fractal S.A.S. queda deshabilitado cuando se encuentra en periodo de vacaciones, licencia e incapacidades mayores a un (1) día, a excepción de aquellos en donde exista una autorización por la gerencia y avalada por el Gerente TI.
- Todos los usuarios que no haya ingresado a los servicios o aplicaciones por más de 3 meses se informaran a los responsables de los accesos para validar su vigencia a la fecha.
- El Ingeniero Senior de infraestructura es el responsable de agregar, modificar o eliminar las cuentas de usuario para acceso a la red corporativa de Ideas Fractal S.A.S según lo definido por coordinadores de área.
- No se autoriza asignación de usuarios (ID) a proveedores sin autorización expresa de la gerencia y Gerente TI
- En los puestos de trabajo no se tiene documentos clasificados como privado o confidencial
- Retirar inmediatamente cualquier documento enviado a las impresoras que contenga información sensible, secreta o confidencial.
- Los documentos electrónicos o físicos que contienen información sensible, secreta, privada o confidencial se guarda en condiciones de seguridad y con acceso de lectura por personal autorizado.

## 17 IDENTIFICACIÓN DE ACTIVOS.

Ideas Fractal S.A.S. cuenta con una política específica de gestión de activos, la cual establece lineamientos para la identificación, clasificación, uso, protección y control de todos los activos que poseen valo**r.**

Los activos constituyen componentes fundamentales sobre los que se sustenta la actividad del negocio y, por lo tanto, requieren protección frente a posibles amenazas.

Los activos pueden incluir infraestructura tecnológica, documentos electrónicos y físicos, y talento humano, entendiéndose en general como todos los recursos necesarios para el cumplimiento de los objetivos organizacionales.

| TIPO DE ACTIVO | | DESCRIPCION |
|---|---|---|
| Infraestructura | Infraestructura física | Centro de datos, oficinas. |

| | | |
|---|---|---|
| | Tecnología Hardware | Servidores, dispositivos de comunicaciones, computadoras de escritorio, laptops, impresoras, copiadoras, faxes, teléfonos, grabadoras de CD/DVD. |
| | Tecnología Software | Aplicaciones comerciales, aplicaciones desarrolladas en casa y open source. |
| Información | Electrónica | Información importante para el negocio (bases de datos) e información de soporte (información de tarifas, agencias, empleados, procesos, políticas, procedimientos, guías y estándares) en medios electrónicos |
| | Papel | Información importante para el negocio (reportes) e información de soporte (procesos, políticas, procedimientos, guías, contratos, información de clientes y estándares) en papel. |
| Personas | Propietario de la información | Nivel directivo o jerárquico son dueños de la información que asigna permisos para leer utilizar y modificar la información. |
| | Usuarios | Personal que utiliza la información para el desempeño de su trabajo diario y que da soporte a los sistemas de información. |
| Servicios | | Correo electrónico, Acceso a red privada virtual (VPN), |

## 18 IDENTIFICACIÓN DE AMENAZAS

Las amenazas son resultados de actos deliberados o mal intencionados que pueden afectar nuestros activos, sin embargo, existen eventos naturales o accidentales que deben ser considerados por su capacidad de generar incidentes no deseados.

Las amenazas a la cuales están expuestos los diferentes activos pueden ser según su origen las siguientes:

| ORIGEN | AMENAZA |
|---|---|
| Condiciones Naturales | Incendios, inundaciones, sismos, tormentas. |

| | |
|---|---|
| Condiciones externas | Aspectos regulatorios, caída de energía, campos electromagnéticos, contaminación, crisis financieras, daño de agua, excesivo calor, excesivo frio, explosiones, perdida de proveedores, problemas de transporte, sobrecargas. |
| Condiciones internas | Campos electromagnéticos, contaminación, daños en los equipos, escapes, fallas en la red, fallas en líneas telefónicas, fallas mecánicas, falta de insumos, fugas, humedad, mala publicidad, pérdida de acceso, perdida de proveedores, polvo, problemas de transporte, registros errados, sobrecargas, suciedad, vibraciones. |
| Entorno Social | Motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo. |
| Actos deliberados | Abuso privilegios de acceso, análisis de tráfico, ataque físico a los equipos, bombas lógicas, código malicioso, destrucción de información, divulgación de información, errores en código, espías (spyware),extorsión, espionaje industrial, fallas de hardware, fallas de software, fallas en la red , fallas en líneas telefónicas, gusanos, incendios, ingeniería social, interceptación de información, manipulación de programas, perdida de datos, robo de información, suplantación de identidad, troyanos, usos no autorizados, Virus. |
| Actos accidentales | Destrucción de información, Incendios, pérdida de claves, perdida de dispositivos. **Errores de operación o manipulación de sistemas**, Fallas eléctricas o de hardware, mala configuración |
| Humano | Epidemias, pandemias huelgas, indisponibilidad de personal, perdida de personal clave. |

## 19 IDENTIFICACIÓN DE VULNERABILIDADES

La identificación de vulnerabilidades es el proceso mediante el cual se detectan, analizan y documentan las debilidades existentes en los activos de información, los sistemas, los procesos, la infraestructura tecnológica o el factor humano que podrían ser explotadas por una amenaza y generar un riesgo. Debe identificarse la forma como cada una de las amenazas podría materializarse, es decir, que vulnerabilidades permiten que las amenazas se conviertan en situaciones de riesgo reales.

Algunas vulnerabilidades pueden ser:

- Ausencia de políticas.
- Configuraciones no seguras.
- Empleado actual descontento.
- Empleado antiguo descontento.
- Empleado deshonesto (sobornado o víctima de chantaje).
- Empleado desinformado.
- Empleado negligente.
- Errores de configuración.
- Errores de mantenimiento.
- Errores del administrador.
- Errores en código.
- Exposición a materiales peligrosos.
- Ausencia de mantenimiento y actualizaciones de sistemas.
- Fallas de usuarios.
- Manuales de uso no documentados.
- Medidas de protección de acceso inadecuadas.
- Medidas de protección física inadecuadas.
- Procesos o procedimientos no documentados.
- Usuario desinformado.
- Tecnología inadecuada.
- Debilidad o inexistencia de controles.

## 20. MARCO GENERAL DE POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

La política general se apoya a través de las políticas específicas que se presentan a continuación, las cuales establecen directrices, controles y responsabilidades orientadas a la protección de la información, el uso adecuado de los sistemas y el cumplimiento del Sistema de Gestión de Seguridad de la Información (SGS) de Ideas Fractal S.A.S.

### Política gestión de incidentes

La política de respuesta a incidentes establece los lineamientos para la identificación, reporte, análisis, contención, erradicación y recuperación ante eventos que puedan

comprometer la seguridad de la información, la continuidad operativa o los activos de Ideas Fractal S.A.S.

Su propósito es asegurar una gestión oportuna y efectiva de los incidentes, minimizando su impacto, preservando la evidencia y garantizando la comunicación adecuada a las partes interesadas.

Para tal efecto, Ideas Fractal S.A.S. designará personal responsable y competente encargado de la gestión y análisis de los incidentes, quien evaluará su naturaleza, impacto y causa, y definirá las acciones necesarias para su tratamiento y mejora continua.

Todos los individuos con roles definidos en el Plan de Respuesta a Incidentes deben recibir capacitación sobre sus funciones y responsabilidades al menos una vez al año, o con la frecuencia establecida mediante un Análisis de Riesgo Dirigido (TRA).

La capacitación debe incluir, como mínimo:

- Tipos de incidentes esperados
- Procedimientos de escalamiento y comunicación
- Preservación de evidencia
- Herramientas y canales disponibles para la respuesta
- Roles individuales y de equipo

La capacitación podrá realizarse en modalidad presencial, virtual o como ejercicios prácticos (tabletop, simulacros, red team/blue team, etc.).

La evidencia de participación debe ser registrada (firmas, logs, capturas, certificados de finalización, etc.).

Cualquier cambio en el entorno tecnológico, estructura del equipo, procesos o herramientas de respuesta requerirá una revisión del contenido de la capacitación.

**Política Teletrabajo y Trabajo remoto:** Establece los lineamientos para el acceso y uso seguro de la información y los sistemas fuera de las instalaciones de Ideas Fractal S.A.S. Su objetivo es mitigar riesgos asociados a conexiones no seguras, uso de redes domésticas y manejo de información en entornos no controlados.

**Política clasificación y etiquetado de la información:** Política clasificación y etiquetado de la información. Define los criterios para clasificar la información según su nivel de sensibilidad (pública, interna, confidencial, critica), así como su adecuado etiquetado. Permite aplicar controles proporcionales para proteger la información y prevenir su divulgación no autorizada.

**Política continuidad del negocio:** Define directrices para garantizar la operación de los procesos críticos ante eventos disruptivos. Incluye la identificación de riesgos, planes de

contingencia y recuperación, con el fin de minimizar impactos y asegurar la continuidad de los servicios.

**Política seguridad física y ambiental:** Regula la protección de las instalaciones, equipos e infraestructura Ideas Fractal S.A.S. frente a accesos no autorizados, daños o interferencias. Incluye controles como acceso restringido, vigilancia y protección de áreas críticas.

**Política uso aceptable de activos:** Define las condiciones bajo las cuales los trabajadores y terceros pueden utilizar los activos de Ideas Fractal S.A.S. (equipos, sistemas, información). Busca prevenir el uso indebido, garantizar la seguridad y asegurar que los recursos se utilicen exclusivamente para fines laborales autorizados.

**Política contratación de proveedores:** Contratación de proveedores. Establece los lineamientos para la selección, evaluación y gestión de proveedores, incluyendo criterios de seguridad de la información. Su objetivo es asegurar que los terceros cumplan con los requisitos organizacionales y no representen un riesgo para la información o la operación.

**Política recursos humanos:** Define los controles relacionados con el ciclo de vida del trabajador (vinculación, permanencia y retiro), incluyendo aspectos como confidencialidad, capacitación y gestión de accesos. Busca reducir riesgos asociados al factor humano.

**Política protección de la privacidad:** Establece los lineamientos para el tratamiento adecuado de los datos personales, garantizando su confidencialidad, integridad y uso conforme a la normativa vigente. Su objetivo es proteger los derechos de los titulares de la información y evitar sanciones legales.

**Política transferencia de información:** Establece los lineamientos y controles necesarios para garantizar que el intercambio de información dentro y fuera de Ideas Fractal S.A.S. se realice de manera segura, confidencial y conforme a las normativas aplicables.

**Política control Criptográfico:** Establece los lineamientos para el uso adecuado de mecanismos criptográficos con el fin de proteger la confidencialidad, integridad y autenticidad de la información, asegurando la correcta gestión de claves, la selección de algoritmos seguros y el cumplimiento de requisitos legales.

**Inteligencia artificial:** Ideas Fractal S.A.S. establece lineamientos sobre el uso de la Inteligencia Artificial debe realizarse de manera responsable, ética y segura, garantizando la protección de la información.

## 21. ROLES Y RESPONSABILIDADES

Todos los empleados, contratistas y demás partes interesadas de Ideas Fractal S.A.S. son responsables de la seguridad de la información; adicionalmente, se establecen los siguientes roles y responsabilidades con respecto a la privacidad y seguridad de la información:

| ROL | RESPONSABLE | ASIGNACIÓN |
|---|---|---|
| Gerente TI | Director de la seguridad de la información. | Será el responsable general de la seguridad de la información y del funcionamiento de la Política General de Seguridad y Privacidad de la información, además de realizar el seguimiento, actualizaciones y verificación de la implementación de la misma. |
| Ingeniero Senior de infraestructura | Planeación de estrategias que permitan llevar a cabo mecanismos para el cumplimiento de lo requerido. | Tendrá la responsabilidad de coordinar la implementación y cumplimiento de las políticas específicas asociadas a la seguridad de la información. |
| Propietario | Directores, jefes y coordinadores. | Serán los responsables de la gestión apropiada del activo de información, como clasificar y definir la criticidad del mismo. |
| Custodio | Empleados o contratista. | Serán los responsables de administrar y hacer efectivos los controles y clasificaciones definidos por el propietario |
| Usuario | Empleados, contratistas, terceros autorizados, agencias, acompañantes | Serán los responsables del buen uso de los activos de información y los datos corporativos sensibles durante el cumplimiento de sus labores o compromisos. |

Se establecen las siguientes asignaciones en pro de la seguridad y privacidad de la información:

- Los propietarios, custodios y usuarios son los responsables de asegurar que la información de la organización mediante el cumplimiento de las políticas para la protección y preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información

- Cada activo de información de la organización debe tener asignado un propietario y este debe ser responsable de su seguridad.

- La asignación se realizará por escrito por parte de (dependencia Administrativa, almacén o quien haga el control de inventarios de activos físicos).
- El uso de la información de la organización por parte de proveedores, contratistas y/o instituciones relacionadas, ya sea local o remotamente, debe ser formalizado por medio de acuerdos de confidencialidad que hagan obligatorio el cumplimiento de la presente política.
- Todas las personas vinculadas contractualmente con la organización en calidad de empleados, contratistas, proveedores están sujetos a las sanciones conforme a la naturaleza de la infracción por desacato a las restricciones y obligaciones de la política de seguridad de la información.
- El cumplimiento de los niveles de servicio en seguridad de la información de terceros debe ser verificado periódicamente.

## 22. EXCLUSIÓN DE LA POLÍTICA

Los gestores de apoyo quedan excluidos de las actividades relacionadas con auditorías y del acceso o manejo de información sensible, en consideración a la naturaleza de sus funciones.

Esta disposición será revisada periódicamente por Gerente general con el fin de evaluar posibles cambios en los procesos, responsabilidades o necesidades operativas que puedan requerir ajustes en los niveles de acceso o participación en dichas actividades.

## 23. VIOLACIONES DE LA POLÍTICA

Se considera violación a la política de seguridad de la información cualquier acción u omisión que implique el incumplimiento de los controles, normas, procedimientos y lineamientos establecidos por la organización para proteger la confidencialidad, integridad y disponibilidad de la información y de los activos asociados. Esto incluye el uso indebido de la información, accesos no autorizados, divulgación de datos sensibles, manipulación o alteración de información, así como el incumplimiento de los controles definidos en el Sistema de Gestión de Seguridad de la Información y en los requisitos aplicables de ISO/IEC 27001 y PCI DSS.

El incumplimiento de estas disposiciones podrá dar lugar a las acciones disciplinarias, administrativas o legales correspondientes, de acuerdo con la naturaleza de la infracción, la calidad del infractor y los procedimientos establecidos en el reglamento interno de trabajo y en el presente documento.

La Gerencia manifiesta su compromiso con la protección de la información y el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), aprobando la presente política para su implementación y cumplimiento dentro de Ideas Fractal S.A.S En este sentido, la política deberá ser divulgada, aplicada y mantenida por todo el personal, contratistas y terceros que tengan acceso a la información de Ideas Fractal S.A.S.

**ARIULFO SANCHEZ GUTIERREZ**

Gerente general