ELABORÓ	REVISÓ Y APROBÓ
Nombre: *John Mario Restrepo*	Nombre: *Herney Darío Salazar*
Cargo: Ingeniero Senior de Infraestructura	Cargo: Gerente TI
Fecha: 03-05-2025	Fecha: 03-05-2025

CONTROL DE VERSIONES

Fecha	Versión Documento	Responsable	Aprobado	Cambios
2023/07/08	001	Director TI	Alta Dirección	Inicio
2024/05/03	002	Director TI	Alta Dirección	Se nombra la base de las políticas ISO 27001
2025/06/25	003	Director TI	Alta Dirección	Se actualizan las responsabilidades para todo el personal

1 DECLARACIÓN DE LA POLÍTICA

La política de seguridad de la información de IdeasFractal SAS 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.

IdeasFractal SAS, 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 llevado 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. Basándonos en las premisas de la ISO 27001, definir políticas, establecer alcance, analizar los riesgos, implementar controles y revisión continua. Así mismo la empresa IdeasFractal SAS se compromete con el estándar se 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 de la red.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de IdeasFractal SAS 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 la empresa.[1]

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_G2_POLÍTICA_General.pdf

2. DIRECTRICES

- Verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
- Establecer un programa PCI DSS que permita el fomento continuo de la creación de cultura y conciencia de seguridad informática con manejo de tarjeta en los empleados, contratistas, proveedores, personas, usuarios de los sistemas de información y telecomunicaciones de la empresa.
- Todos los usuarios de los sistemas de información y telecomunicaciones de IdeasFractal SAS, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en la presente política.
- 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 jefes 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 teniendo en cuenta evitar filtraciones de tarjetas.

3. OBJETIVOS 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 IdeasFractal SAS 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 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.
- Optimizar los procesos de gestión en seguridad informática, estableciendo mecanismos que garanticen el mejoramiento continuo.
- Promover programas de formación y sensibilización a los usuarios dirigidas por el Gerente TI de la organización, en torno a la seguridad de la información y a la continuidad del negocio.
- Crear y mantener una cultura organizacional en seguridad de la información.

4. 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 la organización IdeasFractal SAS

La **Política de Seguridad de la Información** vincula 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 acceden, ya sea interna o externamente a cualquier activo de información independiente de su ubicación.

Adicionalmente la presente Política aplica a toda la información creada, procesada o utilizada a nivel corporativo, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

4.1 DIFUSIÓN

Difundida a todo el personal relevante, así como a los proveedores y socios de negocios relevantes a través de los canales institucionales y nuestra página web.

5. 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.

6. 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 la organización.

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

Su incumplimiento acarreará las acciones a que hubiere lugar conforme a la naturaleza de la infracción, calidad del infractor y las formas del proceso disciplinario que están descrito en el reglamento interno de trabajo y en el presente documento.

7. APLICABILIDAD

La gestión de la seguridad, privacidad y continuidad tecnológica estará enfocada a controlar los riesgos actuales y potenciales de la información de acuerdo con el impacto sobre las operaciones y los objetivos de negocio de la empresa, bajo el marco del estándar PCI - DSS

8. COMPROMISO DE LA DIRECCIÓN

Las directivas de IdeasFractal SAS, declaran 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 *I*nformación y buen uso de los datos de tarjeta habiente.

Las directivas demostrarán su compromiso a través de:

- La revisión y aprobación de la política contenida en este documento.
- La divulgación de esta política a todos los miembros de la organización.
- El aseguramiento de los recursos adecuados para implementar y mantener la política de Seguridad de la Información.

9.REVISIÓN DE LA POLÍTICA GENERAL

La política es revisada anualmente o se actualiza cuando se presenten cambios en la estructura organizacional, cambios en los objetivos del negocio o cuando se identifiquen riesgos en los ambientes.

La revisión y actualización de la política es realizada por la alta dirección y el Director TI, y todos sus cambios son comunicados al interior de la empresa e incluida en los contratos que la organización celebre con empleados o contratistas.

El Gerente TI coordina el programa anual de auditoría informática al esquema de ciberseguridad implementado en la organización, con el fin de estimar el nivel de madurez y efectividad de los controles implementados.

10. ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN

Organización Interna

IdeasFractal S.A.S tiene definido en su estructura organizacional al Gerente TI quien cumple con las funciones y responsabilidades para la ejecución de las actividades de operación, gestión y administración de la seguridad de la información, alineado con las buenas prácticas de los estándares de ciberseguridad PCI DSS y manejo de los datos de tarjeta habiente.

El Gerente TI debe identificar las autoridades a contactar (ver plan de respuesta ante incidentes TI-P-005 para reportar de manera oportuna un incidente de seguridad de la información que lo amerite. Así mismo, debe mantener contactos apropiados con grupos de interés especial relacionados con la seguridad de la información que aporten a la identificación de riesgos.

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

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 la organización, 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

- Responsable de la seguridad de la información
- Identificar vulnerabilidades y garantizar seguimiento.
- Supervisar la implementación de controles de seguridad.
- Liderar y analizar incidentes de seguridad.
- Validar soluciones antimalware/antivirus activas y actualizadas.
- Mantener listado de dispositivos sin riesgo de malware.
- Mantener actualizados los estándares de configuración de infraestructura.
- Garantizar la eficiencia de los sistemas.
- Dirigir, planificar y coordinar las estrategias, políticas y controles de seguridad de la información en la organización, garantizando la confidencialidad, integridad y disponibilidad de los datos, así como el cumplimiento de normativas legales vigentes
- Desarrollar, implementar y mantener políticas normas y procedimientos de seguridad
- Asegurar que los controles estén actualizados frente a nuevas amenazas y riesgos
- 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 las 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.
- Establecer estrategias para la identificación de amenazas potenciales
- Monitorear el plan de mitigación de riesgos de seguridad de la información
- Auditar los terceros dentro del alcance PCI DSS
- Reportar los avances a la alta dirección a la alta dirección de acuerdo con lo requerido en el estándar
- Analizar las evaluaciones de riesgo de seguridad de la información con el apoyo de Director TI.
- 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.
- Establecer soluciones técnicas seguras.
- Desarrollar requerimientos con enfoque en seguridad.
- Ejecutar acciones para mitigar riesgos.
- 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
- Asegurar que los entornos de desarrollo, pruebas y producción estén debidamente segmentados y protegidos.
- Promover la capacitación continua del equipo de desarrollo en prácticas de seguridad de software.
- 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 el manejo seguro del servicio hacia los clientes.
- Velar por el cumplimiento de políticas de seguridad.
- Sensibilizar sobre la importancia de adquirir confidencialidad de la información.
- Promover el buen uso de los recursos informáticos con el personal de la empresa
- Participar de los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- Garantizar que los estados financieros, informes contables
- Responder con rapidez ante incidentes que afecten la seguridad de la información financiera

Gerente Comercial

- Contribuir el manejo seguro del servicio hacia los clientes.
- Velar por el cumplimiento de políticas de seguridad.
- Controlar el uso y la divulgación de la información, especialmente en procesos de propuestas comerciales
- Promover el buen uso de los recursos informáticos con el personal de la empresa
- Garantizar la confidencialidad, integridad y disponibilidad de la información relacionada con los clientes.
- Supervisar que se protejan los datos sensibles de clientes.

Analista Senior Comercial

- Garantizar la confidencialidad y uso autorizado de la información.
- Reportar incidentes u oportunidades de mejora.
- Reportar incidentes relacionados con 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
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información
- Promover el buen manejo del servicio con los clientes

Coordinador de Calidad y seguridad y salud en el trabajo

- Cumplir y promover políticas y procedimientos de seguridad.
- Garantizar la confidencialidad y uso autorizado de la información.
- Reportar incidentes u oportunidades de mejora.
- Divulgar políticas de seguridad en el área.
- 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.

Psicología Organizacional

- Mantener la confidencialidad de la información.
- Usar la información exclusivamente con fines autorizados.
- Participar en capacitaciones sobre seguridad.
- Reportar incidentes y oportunidades de mejora.
- No divulgar información confidencial.
- 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.

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 la organización 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 la alta dirección.
- Informar al personal contratado con respecto a la importancia de cuidar, proteger la información suministrada en la organización
- 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.

Analista de Compras y Proveedores

- Cumplir con políticas de seguridad.
- Mantener confidencialidad.
- Reportar incidentes o mejoras de seguridad.
- No divulgar información sensible.
- 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
- 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.

Analista de Facturación y Cartera

- Cumplir políticas y procedimientos de seguridad.
- Mantener confidencialidad y uso correcto de la información.
- Reportar incidentes y contribuir al buen uso del servicio. 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.

Ingeniero Senior de Infraestructura

- Velar por la implementación de medidas de seguridad en infraestructura tecnológica.
- Supervisar configuraciones seguras en los sistemas y redes.
- Apoyar la continuidad del negocio mediante disponibilidad tecnológica.
- Participar en auditorías técnicas y controles internos. *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.

Coordinador de Desarrollo

- Velar por el cumplimiento de políticas de seguridad.
- Promover auditorías en el área.
- Asegurar que el personal conozca y cumpla las responsabilidades en seguridad.

- Promover el uso adecuado del servicio.
- No divulgar información confidencial.
- 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

Ingeniero Senior de Desarrollo

- Ejecutar mantenimiento y soporte del servicio.
- Garantizar pruebas de software y análisis de implementaciones seguras.
- Cumplir con políticas de seguridad.
- Verificar controles de acceso.
- Corregir deficiencias en los sistemas.
- 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.
- Usar la información confidencial que se entregue únicamente para los efectos señalados al momento de la entrega de dicha información.

. **Ingeniero Junior de Desarrollo**

- Analizar funcionamiento del servicio.
- Orientar sobre accesos de forma eficaz.
- Ejecutar pruebas y análisis seguros.
- Corregir deficiencias del sistema.
- 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.

Técnico de Desarrollo

- Promover uso adecuado del servicio.
- Proponer mejoras técnicas.
- Verificar funcionamiento y desarrollar requerimientos seguros.
- Ejecutar acciones que mitiguen riesgos.
- 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.

Analista de Soporte Nivel I

- Realizar pruebas seguras.
- Cumplir con políticas establecidas.
- 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
- Mantener la confidencialidad de la información
- Reportar incidentes y no divulgar información confidencial.
- 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 políticas y procedimientos de seguridad.
- Participar en programas de sensibilización.
- Reportar incidentes.
- Mantener confidencialidad y uso autorizado 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
- Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

Coordinador de QA

- Cumplir políticas de seguridad.
- Implementar desarrollos seguros.
- Promover uso adecuado del servicio.
- Participar en sensibilizaciones de seguridad.
- 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.

Asistente QA

- Supervisar el rendimiento del sistema.
- Ejecutar pruebas seguras.
- Revisar el buen funcionamiento del servicio.
- Cumplir políticas de seguridad y confidencialidad.
- 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.

Diseñador Web

- Orientar sobre accesos de servicio.
- Cumplir procedimientos establecidos.
- Reportar incidentes o mejoras en seguridad.
- No divulgar información confidencial.
- 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.

11. LINEAMIENTOS DE ADMINISTRACIÓN DE SEGURIDAD INFORMÁTICA

El Gerente TI de IdeasFractal SAS 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 toda la organización.

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 la organización.

El Gerente TI debe garantizar que las políticas de seguridad sean revisadas regularmente y que refleje las necesidades de la organización, 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 la organización, 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 a la organización por pérdidas en la confidencialidad, integridad y disponibilidad de los mismos.

La implementación de los controles debe ser realizada a través de un procedimiento adecuado de cambios y liberaciones, garantizando que las pruebas requeridas son ejecutadas al igual que los procedimientos necesarios para operación son elaborados y formalmente establecidos. Es importante mencionar que existe una relación estrecha tanto con los lineamientos de incidentes y de monitoreo, dada la necesidad de gestionar de forma adecuada de los incidentes de seguridad que puedan presentarse.

12.OBJETIVOS

El objetivo general es alinear la seguridad de la organización garantizando la confidencialidad, integridad y disponibilidad de la información en las actividades realizadas para gestionar servicios de TI.

Los objetivos específicos de la Administración de Seguridad son:

- Producir y mantener un Sistema de Prevención alineada con a los objetivos estratégicos de la organización en relación con la protección y el uso efectivo de los recursos de información.
- Establecer controles de seguridad a través de la implantación de políticas, estándares, guías y procedimientos, que permitan la protección de los recursos de la información de la organización.
- Desarrollar un plan de seguridad a través de la administración de riesgos que considere las amenazas y vulnerabilidades a los que se encuentra expuesta la institución para proteger toda aquella información crítica.
- Garantizar que el intercambio de información entre varios involucrados sea confiable

13.ALCANCE

El alcance de la Administración de Seguridad cubre los lineamientos de Gerente TI que soportan el diseño, transición y operación de los servicios establecidos a continuación:

1. Internet.
2. Correo electrónico.
3. Diseño y publicación de páginas web.
4. Sistemas de información propios.
5. Video conferencia.
6. Sistema de Gestión de Talento Humano.
7. Sistema de archivos compartidos (LAN).

14.IDENTIFICACION DE ACTIVOS

Un activo es: “cualquier elemento al cual se le asigna un valor y por lo tanto requiere protección".

Los activos pueden ser: infraestructura tecnológica, documentos electrónicos y físicos, personas”, lo cual puede entenderse igualmente como aquello que requiere la organización para el cumplimiento de sus objetivos.

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),

15.IDENTIFICACION 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.
Humano	Epidemias, huelgas, indisponibilidad de personal, perdida de personal clave.

16.IDENTIFICACION DE VULNERABILIDADES

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.

17. ROLES Y RESPONSABILIDADES

Todos los empleados, contratistas y demás partes interesadas de IdeasFractal SAS 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	ASIGNACION
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 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.

19. Política de Capacitación sobre Respuesta a Incidentes

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.