Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

GEOPARK

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
AGOSTO 2025

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Control de Cambios

Versión	Fecha		Resumen de Cambios	Autor
	Emisión	Vigencia		
2	10/09/2016		Creación del documento	Gerencia de IT
3	14/07/2024	14/07/2025	Revisión y actualización 2024	Gerente de Seguridad de la Información
4	04/08/2025	04/08/2026	Revisión y actualización 2025	Líder de Gobierno y Cumplimiento

Responsabilidad	Nombre	Cargo
Actualización	Lina Gantiva	Líder de Gobierno y Cumplimiento Firmado por: Lina Gantiva López 63408619558E4C2... 8/4/2025
Revisión	Edgardo Arrieta	Gerente de Ciberseguridad y Cumplimiento Firmado por: Edgardo Arrieta 5BF8ADDC66D44DC... 8/4/2025
Aprobación	Cinthya Sánchez	Directora IThink Signed by: Cinthya Sánchez 7E1C6D5F76134B8... 8/4/2025

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

TABLA DE CONTENIDO

Tabla de contenido

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Introducción

En GeoPark consideramos que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de nuestra empresa, nuestros socios y nuestros clientes. La política de ciberseguridad ha sido orientada a gestionar eficazmente la seguridad de la información, garantizando la continuidad de nuestro negocio junto al cumplimiento de nuestras obligaciones legales y regulatorias, y la confianza de nuestros clientes, proveedores, socios y demás partes interesadas. Incluyendo políticas, prácticas, controles, formación de empleados, informes de incidentes y revisiones con el fin de mitigar el riesgo de pérdida y uso indebido de información. Su estructura se basa en diversos estándares y marcos de seguridad del sector, como el Instituto Nacional de Estándares y Tecnología (NIST), C2M2 o Modelo de Madurez de la Capacidad de Ciberseguridad y la Organización Internacional de Normalización (ISO).

Esta política establece el marco para la protección de la información en GeoPark y es aplicable a todos los empleados, contratistas, proveedores, socios y terceros que accedan, procesen o gestionen información en nombre de la empresa.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Objetivos

El propósito de esta política es el cumplimiento de las obligaciones legales y regulatorias aplicables a la información y a la seguridad de la información, así como con los requisitos contractuales del negocio establecidos por la organización y sus partes interesadas garantizando:

- Proteger la confidencialidad, integridad y disponibilidad de la información
- Implementación de medidas proactivas para restringir el acceso no autorizado y proteger la información sensible de GeoPark. Nuestro objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos, resguardándolos de posibles amenazas y ataques. Esto asegura que solo las personas y sistemas autorizados puedan acceder a la información, manteniendo la seguridad de nuestros activos más críticos.
- Sensibilizar a los empleados, contratistas y colaboradores acerca de los riesgos de ciberseguridad; junto con conocimientos, habilidades y experiencia básica en seguridad, lo cual fomentará el compromiso, la responsabilidad y la sensibilización de todos los miembros de la organización y de los terceros relacionados.
- Preservar los sistemas de información y telecomunicaciones, potenciando las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta e investigación frente a nuevas amenazas.
- Fortalecer la gobernanza de datos y la seguridad de la información en la organización, asegurando la confiabilidad, disponibilidad e integridad de los activos de información, y promoviendo una cultura de responsabilidad y cumplimiento normativo.
- Establecer mecanismos y procesos para registrar y documentar el origen, la transformación, el uso y el destino de los datos a lo largo de todo su ciclo de vida.
- Es fundamental estructurar, gobernar y optimizar los activos de datos de nuestra organización, así como para la Gestión de Almacenamiento y Operaciones de Datos, y la Gestión de Seguridad de Datos.
- Establecer roles y responsabilidades claras para la gestión de datos y mejora continua de la calidad de los datos, junto con la alineación de los objetivos de negocio.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Alcance

Esta política aplica a toda la información generada, procesada, almacenada o transmitida en el marco de las actividades de GeoPark, así como a los sistemas, tecnologías y procesos utilizados para gestionarla. Es de cumplimiento obligatorio para todos los empleados, contratistas, proveedores y terceros que accedan a información corporativa, independientemente de su ubicación geográfica o del medio utilizado para dicho acceso.

La protección de la información abarca tanto los entornos físicos como digitales, e incluye todos los niveles de sensibilidad y criticidad de los datos conforme a las definiciones de clasificación establecidas por la organización.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Principios de seguridad para proteger nuestra empresa

GeoPark establece los lineamientos necesarios para implementar, mantener y mejorar la gestión de la seguridad de la información alineados a los principios fundamentales de seguridad:

- **Confidencialidad**: Asegurar que la información sea accesible sólo por aquellos individuos autorizados.
- **Integridad**: Proteger la exactitud y completitud de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sea necesario.
- **Gestión de Riesgos**: La seguridad de la información se gestionará mediante un proceso formal de evaluación y tratamiento de riesgos.
- **Cumplimiento Normativo**: Todas las actividades de seguridad de la información cumplirán con las leyes, regulaciones y requisitos contractuales pertinentes.
- **Concientización y Capacitación:** Todo el personal será concientizado y capacitado en sus responsabilidades de seguridad de la información.

La seguridad de la información se basa en el marco de referencia internacional NIST, que contempla las fases de identificar, proteger, detectar, responder y recuperarse frente a las amenazas cibernéticas.
La seguridad de la información es un pilar estratégico para GeoPark, especialmente dada la sensibilidad y el valor de los datos que manejamos en el sector petrolero. Si bien el área Ciberseguridad y TI establecen las políticas y herramientas, la efectividad de nuestra postura de seguridad depende de la responsabilidad compartida de cada colaborador como custodio de los datos.

Estos principios buscan guiar a cada trabajador en su rol diario como custodio de la información, asegurando que la protección de nuestros activos de datos sea una práctica inherente a todas las actividades:

- Principio de Responsabilidad Individual
- Principio de Finalidad y Acceso Mínimo
- Principio de Confidencialidad
- Principio de Integridad: Preservar la Precisión
- Principio de Disponibilidad: Asegurar el Acceso Oportuno
- Principio de Conciencia y Vigilancia
- Principio de Cumplimiento Normativo y Políticas Internas

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Normas de seguridad y uso para el personal de GeoPark

GeoPark ha establecido estándares de seguridad para sus empleados, socios y terceros con el fin de proteger los recursos de información de la Compañía. Para garantizar los principios de seguridad para proteger nuestra empresa, estaciones de trabajo y dispositivos móviles utilizados para realizar sus actividades o que estén conectados a la red interna. El objetivo de estas normas es proteger los datos y los activos de tecnología e información contra pérdida, modificación o destrucción.

Seguridad lógica (Clasificación y protección de datos)

En GeoPark, la seguridad de la información es un principio fundamental. Para garantizar una protección adecuada de nuestros datos, se ha establecido una revisión periódica de la clasificación de la información. Esta práctica es parte integral del modelo de Gobernanza de Datos y refuerza la responsabilidad de cada colaborador en la custodia de la información.

La gestión de accesos es esencial para proteger la información y los sistemas, tanto a nivel individual como por roles. GeoPark ha implementado procesos para controlar la asignación de derechos de acceso, impedir accesos no autorizados, autenticar adecuadamente a los usuarios y registrar y auditar eventos relevantes. Estas directrices, junto con la definición de contraseñas seguras, están detalladas en la “**Política de Contraseñas”**, documento clave para la aplicación de estos controles. **La clasificación de la información y los controles de seguridad** aplicables a cada categoría están definidos en el **Anexo 1**.

Seguridad Física

La seguridad física brinda mecanismos que permiten minimizar los riesgos de daños a GeoPark. Por lo tanto, se aplican perímetros de seguridad a los recursos informáticos a fin de evitar riesgos de acceso no autorizados. Todos los centros de procesamientos de datos de GeoPark cuentan con mecanismos de restricción de acceso ubicándose en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

GeoPark determinará realizar orientación específica destinada a mantener la seguridad física de sus estaciones de trabajo, dispositivos móviles y áreas de trabajo, y mantener la seguridad mientras viajan.

Gestión de Activos

Todos los recursos de tecnología de la información (hardware y software) de GEOPARK y/o empresas vinculadas se proporcionan exclusivamente para uso en los negocios de GEOPARK. Cualquier otra utilización no está permitida, en cumplimiento de las restricciones dictadas por esta política:

- Control y registros de equipos informáticos con su información de configuraciones de Hardware y Software, se utilizarán herramientas informáticas de identificación y control de estos. Esta información generada servirá de complemento para el proceso de gestión de inventario de la empresa.
- No está permitida la instalación y/o utilización de software que no esté debidamente autorizado por IThink.
- Los recursos informáticos y de comunicaciones puestos por GEOPARK a disposición de sus empleados están destinados a ser utilizados en el desarrollo de las actividades laborales. El uso personal ocasional está permitido, la compañía reconoce que un uso personal mínimo y esporádico puede ser inevitable o incluso beneficioso para la moral del empleado. Sin embargo, este permiso está estrictamente condicionado a dos puntos críticos:
    - **Efecto Nulo sobre la Productividad:** Esto significa que el uso personal no debe interferir con las responsabilidades laborales, causar retrasos en el trabajo, ni ocupar un tiempo significativo que debería dedicarse a las tareas de la empresa.
    - **Efecto Nulo sobre la Seguridad de la Información:** Esta es la condición más crítica desde el punto de vista de la ciberseguridad. Implica que el uso personal no debe, en ninguna circunstancia, poner en riesgo la confidencialidad, integridad o disponibilidad de la información de la empresa. Esto incluye:
        - No visitar sitios web maliciosos o descargar contenido que pueda introducir malware o virus.
        - No compartir credenciales o información de la empresa.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

- No almacenar información personal excesiva o no relacionada con el trabajo que pueda comprometer la capacidad de la empresa para gestionar sus activos.
- No utilizar servicios en la nube personales no aprobados para manejar datos corporativos.

- Gestión y control de acceso de usuarios con privilegios y el respectivo retiro de estos cuando el empleado o contratista ya no necesite acceder. Los derechos de acceso se revisarán de forma periódica para garantizar la continuidad de la necesidad empresarial y la revalidación de privilegios.

  Control de acceso a aplicaciones y sistemas: utilice procedimientos de inicio de sesión seguro para controlar el acceso a aplicaciones y sistemas, incluida la autenticación multifactor.

  Uso de cifrado

  - Utilizar el cifrado según criterios de riesgo, como la sensibilidad o la clasificación de la información.
  - Proteger los datos en tránsito en redes públicas y privadas y asegurar la información en reposo en aplicaciones o sistemas para mitigar amenazas.
  - Proteger y cifrar las claves criptográficas durante todo el ciclo de vida de la gestión de claves.

En GeoPark, entendemos que, ocasionalmente, nuestros colaboradores puedan necesitar hacer un uso personal limitado de los activos de la compañía. Nuestro objetivo es fomentar un ambiente de confianza y productividad, mientras protegemos los recursos de GeoPark y aseguramos el cumplimiento de nuestras políticas.

Gestión de seguridad informática

Los sistemas y redes de información son activos importantes. Para minimizar el riesgo de daño de los sistemas operacionales, éstos se mantienen correctamente actualizados y configurados mediante un proceso de revisión y aplicación de parches. Se espera garantizar la seguridad de los sistemas informáticos, mantener los sistemas actualizados con los parches que cubren las últimas vulnerabilidades detectadas, según corresponda

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

con las necesidades operativas y con respectivas políticas de seguridad y estándares vigentes (sistemas operativos, bases de datos, aplicaciones, etc.).

Desarrollo y mantenimiento de sistemas

Dado que el software puede ser vulnerado con el objetivo de provocar incidentes o anomalías, se encuentran implementados procesos para que los cambios en los programas sigan un flujo controlado y de esta manera se asegure la inclusión de controles de seguridad y validación de protección de nuestros activos de información y la privacidad de los datos personales y sensibles deben ser consideraciones inherentes a todo el ciclo de vida del desarrollo y mantenimiento de nuestros sistemas, y no solo funcionalidades añadidas al final.

En GeoPark, la seguridad de la información y la privacidad de los datos no son opcionales; son pilares fundamentales que deben integrarse desde el inicio de cada proyecto. Para ello, nos alineamos con las mejores prácticas y consideraciones claves, definidas en el **Anexo 2**.

Seguridad Gestión de operaciones

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos. Por lo tanto, se definen e implementan procesos de operaciones para una administración segura del tratamiento programado, garantizando el funcionamiento apropiado y seguro de las instalaciones donde se lleve a cabo el procesamiento de la información y su transmisión, asimismo el respectivo establecimiento de responsabilidades para su gestión y operación, incluyendo instrucciones operativas, y separación de funciones

Las operaciones diarias de TI deben seguir procedimientos seguros, incluyendo la gestión de cambios, copias de seguridad y monitoreo de eventos.

- Mantener los procedimientos operativos y ponerlos a disposición de los usuarios pertinentes.
- Los procedimientos operativos pueden incluir: Instalación y configuración de aplicaciones y sistemas
- Procedimientos de arranque y cierre

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

- Gestión de autenticación y autorización
- Procedimientos de mantenimiento y respaldo
- Procedimientos de manejo de información, tanto actividades automatizadas como manuales
- Determinación y manejo de problemas
- Registro y monitoreo
- Comunicación con contactos de soporte y escalamiento
- Manejo de incidentes de seguridad
- Pruebas de seguridad
- Gestión de vulnerabilidades y parches

Gestión de comunicaciones

En GeoPark, existen interacciones entre diversos sistemas informáticos, tanto internos como con terceros. Para estas comunicaciones, se han establecido mecanismos de seguridad que aseguran que el intercambio de datos se realice bajo condiciones que garanticen la confidencialidad, integridad y disponibilidad de la información. Por ello, se aplican controles específicos para proteger la información que transita por las redes de GeoPark.

Administración de la continuidad de los servicios de TI

Se implementan planes de contingencia para garantizar que todas las actividades soportadas por tecnologías de la información se restablezcan dentro de plazos razonables ante interrupciones de servicio no esperadas y con los niveles de pérdida de datos mínimos tolerables por el negocio.

Por lo anterior se minimizan los efectos de las posibles interrupciones de las actividades normales de GeoPark (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos, acciones de recuperación, análisis y medidas correspondientes para la prevención de hechos similares en el futuro.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Seguridad física y ambiental

Se producen y mantienen registros de auditoría de las actividades, excepciones y eventos de seguridad críticos. Se encuentran implementados procesos de revisión, auditoría y control de eventos y registros de actividades críticas a fin de garantizar el cumplimiento de los procesos de seguridad informática.

- Colocar los activos de infraestructura en zonas de acceso controlado, con excepción de aquellos destinados al uso público.
- Aplicar controles de acceso basados en riesgos, que pueden incluir el bloqueo o la protección de áreas para:
    - Permitir el acceso sólo a personas autorizadas
    - Mantener la seguridad física durante cortes de energía
    - Mantener el registro de acceso.

Gestión de Incidentes de Seguridad de la Información

Se monitorea eventos en los cuales se generen incidentes que puedan potencialmente comprometer la seguridad de la información. Con el objetivo de detectar y bloquear intentos de acceso a información o sistemas, intrusos, realizar tareas de rastreo e identificación y análisis forense sobre los sistemas informáticos en donde se hayan producido los incidentes.

Respuesta ante Incidentes de seguridad

En GeoPark, nuestra capacidad para responder eficazmente a los incidentes de seguridad es crucial. Sin embargo, una respuesta efectiva va más allá de la mitigación inmediata del daño. Para fortalecer continuamente nuestra postura de seguridad y el gobierno de nuestros datos, integramos explícitamente la gestión de incidentes al ciclo de mejora continua del gobierno del dato. Este enfoque se alinea con las mejores prácticas de estándares reconocidos.

Cuando la gravedad del incidente lo justifique y/o exceda la capacidad de respuesta del equipo interno, se contratarán los servicios de una empresa especializada que asegure la resolución de este y realizará la evaluación, revisión y actualizaciones correspondientes con el fin de incorporar las lecciones aprendidas en este ámbito en constante evolución.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Un equipo compuesto por el Equipo de Respuesta a Incidentes de Ciberseguridad (CSIRT) y el equipo de Ciberseguridad se reúne para evaluar la información sobre incidentes nuevos y reportados previamente. Los incidentes serán delegados a las personas adecuadas para su evaluación, investigación y resolución.

El Centro de Operaciones de Seguridad (SOC) monitorea las amenazas a las redes y sistemas de la Compañía. Para identificar, monitorear y abordar las amenazas internas, el SOC se basa en diversas fuentes de inteligencia de amenazas. El SOC gestiona un amplio despliegue de tecnologías avanzadas de detección y respuesta.

Los detalles sobre el ciclo de vida del incidente y su integración como motor de mejora en el gobierno del dato se encuentran en el **Anexo 3**.

Concienciación de Seguridad de la información

GeoPark impartirá anualmente capacitación obligatoria y personalizada en ciberseguridad a todos sus empleados, incluyendo formación para reconocer, evitar y reportar actividades sospechosas y/o posibles incidentes de seguridad, que pueden abarcar desde la pérdida de teléfonos móviles hasta malware en portátiles, incidentes de phishing y correos electrónicos mal dirigidos. El equipo solicitará realizar simulacros de phishing para evaluar y practicar la preparación de los empleados para reconocer y responder a las amenazas del correo electrónico Adicional recibirán orientación y formación sobre el uso de activos de la compañía, para ayudar a los empleados a comprender los riesgos de seguridad y cumplir con las políticas de TI.

Política de seguridad de acceso remoto

Establece las normas y procedimientos en acceso remoto a la red corporativa y a los sistemas internos, solo será permitido a través de conexiones seguras (VPNs) con autenticación robusta y desde dispositivos que cumplan con los estándares de seguridad de la empresa.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Copias de seguridad

Gestionar copias de seguridad con periodicidad alineada al documento **“Políticas de Backup”** donde todas las máquinas que están en la nube de Azure tienen configurada alguna Política de Snapshot. La política aplicada depende del servicio que preste cada máquina, con el fin de proteger los datos asegurando su disponibilidad y recuperación en caso de pérdida o falla.

Medios de almacenamiento

Proteger la información almacenada en dispositivos físicos (como discos duros, USBs, etc.) y sistemas de almacenamiento en la nube o restricción del uso de estos, con el fin de prevenir accesos no autorizados, pérdidas de datos y otras amenazas, abarcando desde el uso de contraseñas seguras hasta la encriptación de datos y la gestión de accesos.

Sistemas de información externos

Sistemas o componentes sobre los cuales la organización no tiene control directo o supervisión en la aplicación de requisitos y controles de seguridad, o en la evaluación de su eficacia. Estos sistemas pueden incluir dispositivos personales, dispositivos de comunicación privados o sistemas pertenecientes a terceros con los que la organización interactúa.

Cumplimiento de política

Los empleados de GeoPark darán cumplimiento a la política de seguridad la cual será definida, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros resguardando la información creada, procesada, transmitida por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Roles y Responsabilidades

Los roles y responsabilidades relacionados con la seguridad de la información en GeoPark son los siguientes:

- La alta dirección es la responsable de aprobar, difundir y hacer cumplir esta política, así como de asignar los recursos necesarios para su implementación y mantenimiento.
- El responsable de Ciberseguridad es el encargado de coordinar, ejecutar y monitorear las actividades de seguridad de la información en la organización, así como de asesorar, capacitar y concientizar a los demás miembros de la organización y a los terceros relacionados.
- Los responsables de proceso son los encargados de identificar, clasificar y proteger la información que generan, procesan o almacenan en sus respectivos procesos, así como de reportar y gestionar los incidentes de seguridad de la información que les afecten.
- Los usuarios de la información son los encargados de cumplir con esta política y con las normas, procedimientos y buenas prácticas de seguridad de la información que les apliquen, así como de reportar cualquier situación o incidente que ponga en riesgo la seguridad de la información.
- Los proveedores de servicios de seguridad de la información son los encargados de cumplir con los requisitos de seguridad de la información establecidos por la organización y por los acuerdos de nivel de servicio suscritos, así como de reportar y gestionar los incidentes de seguridad de la información que les afecten.

- La figura del Data Owner (Propietario del Dato) es crucial para la seguridad y el cumplimiento de nuestra información. Este rol no sólo centraliza la responsabilidad, sino que también fortalece activamente nuestra postura de seguridad al asegurar que los datos sean gestionados con la máxima protección y conforme a las regulaciones.

  Sus responsabilidades clave son:

  - Clasificación del Dato
  - Definición de Controles de Acceso
  - Autorización de Accesos de Terceros
  - Gestión del Ciclo de Vida del Dato
  - Aprobación de Usos y Propósitos
  - Alineación Estratégica

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

- Participación en la Gestión de Incidentes

Cumplimiento de la Política de Seguridad en GeoPark

En GeoPark, nuestra Política de Seguridad de la Información no es solo un conjunto de directrices; es un compromiso activo con la protección de nuestros activos más valiosos. Para asegurar su efectividad y nuestra adherencia constante, hemos establecido un marco robusto de evaluación y mejora continua. Este marco se apoya en revisiones y en la medición de indicadores clave de rendimiento.

Verificación y Validación Constante

El cumplimiento de nuestra política de seguridad será evaluado sistemáticamente a través de:

- **Revisiones Periódicas:** Anualmente se revisará la implementación y la efectividad de nuestras políticas y procedimientos de seguridad. Estas evaluaciones, llevadas a cabo por equipos o personal capacitado dentro de GeoPark, nos permitirán identificar de manera proactiva las áreas de mejora, detectar posibles desviaciones y asegurar que nuestros controles operen según lo esperado.

Indicadores Clave de Cumplimiento (KPIs): Midiendo el Desempeño

Para asegurar que nuestro SGSI sea dinámico y basado en datos, estableceremos y monitoreamos **Indicadores Clave de Cumplimiento (KPIs)**. Estos KPIs nos permitirán medir de forma cuantitativa la eficacia de nuestra política de seguridad y el grado de cumplimiento en toda la organización. Los resultados de los KPIs serán revisados regularmente por la alta dirección para tomar decisiones informadas y asignar recursos estratégicamente.

Algunos ejemplos de KPIs relevantes incluirán:

- Porcentaje de incidentes de seguridad resueltos dentro de los tiempos SLA.
- Número de vulnerabilidades críticas identificadas y remediadas.
- Tasa de cumplimiento en la capacitación de seguridad y concientización del personal.
- Resultados de las pruebas de penetración y evaluaciones de vulnerabilidad.
- Porcentaje de datos clasificados correctamente y con revisiones al día.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

- Cumplimiento de los controles de acceso de terceros según lo establecido en contratos y políticas.

Compromiso con la Mejora Continua

La evaluación mediante auditorías y KPIs es fundamental para nuestro compromiso con la mejora continua. Los hallazgos de las auditorías y el análisis de los KPIs no son solo reportes; son el motor que impulsa la revisión, actualización y optimización constante de nuestras políticas, procedimientos y controles de seguridad. Este ciclo de retroalimentación nos permite adaptarnos a las nuevas amenazas, tecnologías y requisitos de negocio y regulatorios, asegurando que nuestra postura de seguridad se mantenga siempre resiliente y eficaz.

En GeoPark, la seguridad de la información es una responsabilidad compartida y un proceso en constante evolución, y su cumplimiento es evaluado para garantizar la protección de todo lo que valoramos.

El incumplimiento de la política de Seguridad y Privacidad de la Información conlleva consecuencias legales que se derivan de la normativa de la entidad y de las leyes nacionales y territoriales aplicables en materia de seguridad y privacidad de la información. Estas consecuencias pueden incluir sanciones disciplinarias, multas, y acciones legales por parte de terceros afectados.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

GLOSARIO

- **Administrador de Datos:** Encargado de la gobernanza y gestión del ciclo de vida de los datos de una organización.

- **Hardware:** Se refiere a los componentes físicos y tangibles de un sistema informático o de comunicaciones.

- **Software:** Es el conjunto de programas, aplicaciones, instrucciones y datos intangibles que le dicen al hardware qué hacer. Incluye desde los sistemas operativos (Windows, Linux), aplicaciones empresariales (ERP, CRM), bases de datos, hasta programas de seguridad y utilidades.

- **Activos:** Son todo aquello que tiene valor para la organización y necesita ser protegido. Esto incluye no solo la información en sí misma (datos, bases de datos, documentos), sino también el hardware, el software, los servicios, la infraestructura.

- **Cifrado:** Es un método criptográfico que transforma la información (texto plano) en un formato ilegible (texto cifrado), de modo que solo las personas autorizadas que poseen una clave secreta pueden descifrar y acceder a su contenido original.

- **TI:** (Tecnologías de la Información) es el departamento o conjunto de funciones dentro de una organización encargado de la gestión, operación y mantenimiento de la infraestructura tecnológica (hardware, software, redes, sistemas) que soporta las operaciones del negocio.

- **Vulnerabilidades:** Son debilidades o fallos en un sistema, software, hardware, proceso o incluso en la gestión humana, que podrían ser explotados por una amenaza para causar un daño o comprometer la seguridad.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

- **VPN:**(Red Privada Virtual) es una tecnología que crea una conexión segura y cifrada sobre una red pública (como internet). Permite a los usuarios acceder a recursos de una red privada.

- **Nube:** Es un modelo de almacenamiento y acceso a datos y servicios a través de internet,

- **SGSI:**(Sistema de Gestión de Seguridad de la Información) es un marco de trabajo sistemático y documentado de políticas, procedimientos y controles para gestionar los riesgos de seguridad de la información de una organización.

- **SLA:** (Acuerdo de Nivel de Servicio) es un contrato o parte de un contrato que define el nivel de servicio que un proveedor (interno o externo) se compromete a ofrecer a un cliente.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

ANEXOS

Anexo 1

Seguridad lógica (Clasificación y protección de datos)

- **Clasificación y controles** de seguridad adecuados a las categorías de información, datos y activos. Toda la información debe ser clasificada según su sensibilidad y criticidad (Público, Reservado, Confidencial, Estrictamente Confidencial) para determinar el nivel de protección requerido.

    - **Público**: Información apta para ser compartida tanto interna como externamente, que no representa un impacto operativo ni riesgo para la continuidad de las actividades de GeoPark.
    - **Reservado**: Información de uso exclusivo del personal de GeoPark y/o sus proveedores o aliados. La divulgación no autorizada podría generar un impacto negativo en la operación de GeoPark, solo quien aplica la etiqueta puede retirarla.

        - ***Reservado / Externo***: Información de uso exclusivo del personal de GeoPark y sus aliados o proveedores externos.
        - ***Reservado / Interno:*** Información de uso exclusivo del personal de GeoPark. No puede ser accedida por personal externo (no geo-park.com o ext.geo-park.com).

    - **Confidencial**: Información que solo puede ser utilizada por personal específico del área, pues su divulgación no autorizada, incluso dentro de GeoPark, podría tener un impacto negativo en las operaciones, solo quien aplica la etiqueta puede retirarla.
        - ***Confidencial / Área:*** Información que solo puede ser accedida por personas del área.

      Nota: Cada área tendrá su propia subetiqueta, restringiendo el acceso a la información etiquetada a quien haga parte de dicha área.
    - **Estrictamente Confidencial**: Información cuya distribución está limitada a los usuarios internos o externos autorizados por quien aplique la etiqueta. Su divulgación no autorizada podría generar un impacto negativo grave en la operación de GeoPark.
        - Quien aplica la etiqueta definirá permisos personalizados para usuarios internos o externos a GeoPark, estos permisos pueden ser:

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

- Visor: El usuario puede ver. No puede editar, imprimir, copiar contenido ni cambiar o quitar la protección.
- Editor restringido: El usuario puede ver y editar. No puede imprimir, copiar contenido ni cambiar o quitar la protección.
- Editor: El usuario puede ver, editar, imprimir y copiar contenido. No puede cambiar ni quitar la protección.
- Propietario: el usuario puede hacer cualquier cosa con el documento, incluida la eliminación de la protección.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Anexo 2

Mejores prácticas y consideraciones clave:

1. **Enfoque Proactivo, no Reactivo:**
    - La seguridad y la privacidad se anticipan y se previenen. No esperamos a que ocurran incidentes o a que surjan problemas de cumplimiento para actuar. Desde la concepción de un sistema, se identifican y mitigan los riesgos de seguridad y privacidad.

2. **Privacidad como Configuración Predeterminada (Privacy by Default):**
    - Los sistemas y aplicaciones de GeoPark deben configurarse de forma predeterminada para ofrecer el nivel más alto de privacidad posible, especialmente en el tratamiento de datos personales. Esto significa que la configuración por defecto debe ser la más restrictiva, minimizando la recolección, el uso y la divulgación de datos.

3. **Seguridad y Privacidad Integradas en el Diseño:**
    - Las consideraciones de seguridad y privacidad se incorporan en cada fase del ciclo de vida del desarrollo de software (SDLC): desde la planificación y el diseño, pasando por la codificación, las pruebas, la implementación, hasta la operación y el desmantelamiento. Esto incluye:
        - **Análisis de requisitos:** Identificación de las necesidades de seguridad y privacidad desde el inicio.
        - **Diseño seguro:** Implementación de arquitecturas y patrones de diseño seguros.
        - **Codificación segura:** Uso de prácticas de programación segura para prevenir vulnerabilidades comunes.
        - **Pruebas de seguridad (SAST, DAST, pruebas de penetración):** Realización de pruebas exhaustivas para identificar y corregir fallos de seguridad y privacidad antes del despliegue.

4. **Visibilidad y Transparencia:**
    - Los procesos de tratamiento de datos, así como las medidas de seguridad y privacidad implementadas, deben ser transparentes y comprensibles. Esto facilita la auditoría, el cumplimiento y la confianza de los usuarios.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

5. **Ciclo de Vida Completo de la Información:**
    - La seguridad y la privacidad deben aplicarse a lo largo de todo el ciclo de vida de los datos, desde su recolección y almacenamiento hasta su procesamiento, uso, transferencia y eliminación segura. Esto incluye la gestión adecuada de la retención de datos.

6. **Protección de Extremo a Extremo (End-to-End Security):**
    - La seguridad debe proteger todos los puntos de la cadena de valor de los datos, desde la interfaz de usuario hasta la base de datos y cualquier sistema externo con el que interactúe la aplicación. Esto implica asegurar las comunicaciones, el almacenamiento y el procesamiento de la información.

7. **Respeto por el Usuario:**
    - Siempre que sea posible, los sistemas deben diseñarse para empoderar a los usuarios (internos y externos) con control sobre sus datos, facilitando el ejercicio de derechos como el acceso, la rectificación, la supresión y la portabilidad de sus datos personales.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

Anexo 3:

Ciclo de Vida del Incidente como Motor de Mejora:

En GeoPark, consideramos cada incidente de seguridad, sin importar su magnitud, como una oportunidad para fortalecer nuestras capacidades, políticas y procesos. Por ello, el ciclo de vida de gestión de incidentes está integrado directamente en nuestro enfoque de mejora continua, alineado con principios de ISO/IEC 27035 y el gobierno del dato.

1. Preparación

- **Gobierno del Dato**: Definición de roles y responsabilidades, establecimiento de políticas de clasificación de información y capacitación del personal en la custodia de los datos.
- **Seguridad**: Elaboración de planes de respuesta, desarrollo de kits de herramientas, comunicación segura y simulacros de incidentes.

2. Detección y Análisis

- **Gobierno del Dato**: Participación de administradores de datos para detectar anomalías mediante el conocimiento de patrones normales de uso y trazabilidad de metadatos.
- **Seguridad**: Monitoreo continuo, análisis de logs, uso de herramientas de detección (IDS/IPS), y análisis forense.

3. Erradicación y Recuperación

- **Gobierno del Dato**: Priorización de acciones de contención según la clasificación de la información, asegurando restauraciones confiables.
- **Seguridad**: Aislamiento del incidente, eliminación de amenazas, restauración segura del servicio, aplicación de parches y controles compensatorios.

4. Post-Incidente (Lecciones Aprendidas y Mejora Continua)

- **Análisis Post-Incidente**:
  - Evaluación de causas raíz y fallas en controles.
  - Revisión de la efectividad de la respuesta.
- **Ajustes al Gobierno del Dato**:
  - Revisión de políticas de tratamiento, acceso y clasificación.

Docusign Envelope ID: 14EBDA54-85D2-4CA3-97AD-6755B3B28935

  - Mejora de flujos, procesos y herramientas.
  - Fortalecimiento del rol del Administrador de Datos.
  - Reevaluación del mapa de riesgos de la información.
  - Ajustes a la arquitectura de datos para mayor resiliencia.
- **Mejoras de Seguridad Técnica**:
  - Nuevas tecnologías, controles adicionales y ajustes en monitoreo y detección.
- **Revisión de Clasificación de Datos**:
  - Reevaluación de sensibilidad de los datos expuestos y ajustes correspondientes.