I. INTRODUCCIÓN

En GeoPark, somos conscientes de que la información es un activo estratégico que debe ser protegido adecuadamente para garantizar la continuidad de nuestro negocio, el cumplimiento de nuestras obligaciones legales y regulatorias, y la confianza de nuestros clientes, proveedores, socios y demás partes interesadas. Por ello, hemos establecido esta política de seguridad de la información, que define los principios, objetivos, roles y responsabilidades que rigen la gestión de la seguridad de la información en nuestra organización.

II. OBJETIVO

- Preservar la confidencialidad de la información, evitando que sea accedida por personas, entidades o procesos no autorizados.
- Preservar la integridad de la información, evitando que sea modificada, manipulada o reproducida por personas, entidades o procesos no autorizados.
- Preservar la disponibilidad y la continuidad de la información y de los servicios asociados, asegurando que estén accesibles cuando sean requeridos por las personas, entidades o procesos autorizados.
- Garantizar el no repudio de la información, asegurando que su origen y destino sean verificables y que no haya sido alterada en su tránsito.
- Cumplir con las obligaciones legales y regulatorias aplicables a la información y a la seguridad de la información, así como con los requisitos contractuales y de negocio establecidos por la organización y sus partes interesadas.
- Mejorar la cultura de seguridad de la información en la organización, fomentando el compromiso, la responsabilidad y la sensibilización de todos los miembros de la organización y de los terceros relacionados.

III. ALCANCE

Esta política aplica a toda la información que posee, procesa, transmite o almacena GeoPark, independientemente de su formato, medio o ubicación. Asimismo, aplica a todos los empleados, contratistas, consultores, socios y terceros que acceden, usan o gestionan la información de GeoPark, o que prestan servicios relacionados con la seguridad de la información a la organización.

IV. GENERAL

La seguridad de la información en GeoPark se basa en los siguientes principios:

- La información es un activo de la organización que debe ser identificado, clasificado, inventariado y protegido de acuerdo con su valor, criticidad y sensibilidad.

- La seguridad de la información es responsabilidad de todos los miembros de la organización, quienes deben cumplir con las políticas, normas, procedimientos y buenas prácticas establecidas para tal fin.
- La seguridad de la información se gestiona de forma integral, considerando los aspectos técnicos, organizativos, humanos, legales y éticos que la afectan.
- La seguridad de la información se alinea con los objetivos estratégicos de la organización y se integra con los procesos de negocio, de gestión de riesgos y de mejora continua.
- La seguridad de la información se basa en el marco de referencia internacional NIST, que contempla las fases de identificar, proteger, detectar, responder y recuperar frente a las amenazas cibernéticas.
- La seguridad de la información se mantiene mediante la capacitación, la concientización, la auditoría, la revisión y la actualización periódica de las medidas de protección implementadas.

V. POLÍTICA

Esta Política establece los lineamientos necesarios para implementar, mantener y mejorar la gestión de la seguridad de la información en GEOPARK con el fin de proteger los recursos de información de la Compañía. Para garantizar los principios mencionados, se desarrollan los siguientes dominios:

- **Control de accesos informáticos**

  Para impedir el acceso no autorizado a los sistemas informáticos, bases de datos o servicios informáticos, se encuentran implementados procesos para controlar la asignación de derechos de acceso. Las autorizaciones de acceso a la información se agrupan en perfiles de acceso de acuerdo con las actividades que se deban realizar con cada rol, a fin de evitar una falta de segregación de funciones.

  Objetivos

  - Impedir el acceso no autorizado a los sistemas informáticos e implementar mecanismos de seguridad en los accesos de usuarios.
  - Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los diferentes sistemas de GeoPark.

- **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.

Objetivos

- Garantizar la seguridad de los sistemas informáticos.
- Mantener los sistemas actualizados con los parches que cubran las últimas vulnerabilidades detectadas, según corresponda con las necesidades operativas.
- Mantener los sistemas configurados con políticas de seguridad y estándares vigentes (sistemas operativos, bases de datos, aplicaciones, etc.).

- **Desarrollo y mantenimiento de sistemas**

El desarrollo y mantenimiento de los sistemas es un punto crítico de la seguridad. 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.

Objetivos

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo o adquisición de los sistemas informáticos.
- Definir y documentar los controles que se aplicarán durante el ciclo de vida de los sistemas y en la infraestructura de base en la cual se apoyan.

- **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 procesamiento programado.

Objetivos

- Garantizar el funcionamiento apropiado y seguro de las instalaciones donde se lleve a cabo el procesamiento de la información y su transmisión.
- Establecer responsabilidades para su gestión y operación, incluyendo instrucciones operativas, y separación de funciones.

- **Gestión de comunicaciones**

Los sistemas informáticos están comunicados entre sí, tanto dentro de GeoPark como con terceros. Por lo tanto, se encuentran establecidos mecanismos de seguridad que aseguran en el intercambio de datos las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe.

Objetivos

- Establecer controles especiales para salvaguardar la confidencialidad y la integridad de la información que fluye a través de las redes de GeoPark.

- **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 físico no autorizados. Todos los centros de procesamientos de datos de GeoPark cuentan con mecanismos de restricción de acceso.

Objetivos

- Prevenir e impedir accesos no autorizados, daños o interferencia en las áreas de procesamiento informático.
- Proteger el equipamiento de procesamiento crítico de GeoPark ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

- **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.

Objetivo

- Minimizar 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 y acciones de recuperación.
- Analizar las causas de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

- **Revisión de seguridad de los sistemas**

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

Objetivos

- Controlar los eventos de seguridad.
- Mantener un registro de las actividades críticas de los sistemas.
- Auditar el cumplimiento de los procesos de seguridad informática.

- **Gestión de Activos**

Todos los recursos de Tecnología (hardware y software) de la Información de GEOPARK y/o empresas vinculadas son provistos para su uso en los negocios de GEOPARK. La utilización de cualquiera de ellos para otros fines, en principio, no está permitida. No obstante, la Compañía permite el uso de estos recursos con fines personales, siempre y cuando dicho uso no afecte la productividad laboral de la propia persona o de las personas que comparten los mismos recursos y que se dé cumplimiento a las restricciones dictadas por esta Política.

Objetivos

- Para tener un control y registros de equipos informáticos con su información de configuraciones de Hardware y Software, se utilizarán herramientas informáticas de identificación y control de los mismos. 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, siempre y cuando tenga efecto nulo sobre la productividad y sobre la seguridad de la información.

- **Gestión de Incidentes de Seguridad de la Información**

Se monitoreará eventos en los cuales se generen incidentes que puedan potencialmente comprometer la seguridad de la información.

Objetivos

- Se debe tener la capacidad 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.

- 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 del mismo.

- **Relación con Proveedores**

  Los proveedores deberán alinearse a los requisitos de seguridad de la información de GeoPark.

  Objetivos

  - Los proveedores deben cumplir con la Política de Seguridad de la Información.
  - Los proveedores deben implementar en caso de ser necesario controles de seguridad que protejan la información de la compañía que quede bajo su responsabilidad.

- **Concienciación de Seguridad la información**

  Serán creadas y mantenidas acciones de concientización referidas a la seguridad de la información para todos los colaboradores de GEOPARK.

  Objetivos

  - Coordinar campañas y acciones de concientización periódicas.

VI. 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 seguridad de la información 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.

VII. TABLA DE CONTROL DE VERSIONES

Versión	Fecha	Autor	Descripción
2	01/09/2016	Gerencia de IT	Creación del documento
3	25/06/2024	Richard Garcia Gerente de Seguridad de la Información	Revisión y actualización de la política