POLITICA DE SEGURIDAD DE LA INFORMACIÓN

MONPEZA SAS

NIT. 900.448.332-9

Primera versión
Enero de 2024, Bogotá D.C

CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO GENERAL 3
3. OBJETIVOS ESPECIFICOS 3
4. ALCANCE Y APLICABILIDAD 4
5. DEFINICIONES Y/O GLOSARIO 4
6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN 6
7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 6
   7.1 Política de Responsabilidades de la Seguridad de la Información: 6
      7.1.1 Responsabilidades del Líder de Seguridad de la Información: 7
      7.1.2 Responsabilidades del Administrador de los Sistemas de Información: 8
      7.1.3 Responsabilidades del Líder de Protección de Datos Personales 8
      7.1.4 Responsabilidad de los Usuarios de los Activos de Información 8
   7.2 Política de Seguridad de los Recursos Humanos 9
   7.3 Política de Gestión de Activos de Información: 10
   7.4 Política de Control de Acceso: 11
   7.5 Política de Seguridad Física y del Entorno: 12
   7.6 Política de Seguridad de las Operaciones: 13
   7.7 Política de Seguridad para Relación con Proveedores: 13
   7.8 Política Gestión de Incidentes de Seguridad de la Información: 13
   7.9 Política de Revisión Periódica y Auditoria de la Política de Seguridad de la Información: 13
8. INCUMPLIMIENTO DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN 13
9. VIGENCIA 14

1. INTRODUCCIÓN

MONPEZA SAS, identificada con NIT 900448332-9 y domicilio principal en la ciudad de Bogotá D.C, es una empresa del sector ganadero dedicada a la producción cárnica y lechera con alta calidad, excelente genética y las mejores prácticas ambientales.

En el cumplimiento de su objeto social, MONPEZA SAS reconoce la importancia de la adecuada gestión y protección de sus activos de información, por lo tanto, se compromete a implementar una Política de Seguridad de la Información que le permita proteger la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información que gestiona en el ejercicio de sus operaciones.

2. OBJETIVO GENERAL

Esta política tiene como objetivo establecer las directrices necesarias para proteger la seguridad de la información a cargo de MONPEZA SAS, con el fin de evitar, prevenir y mitigar los riesgos que comprometan su confidencialidad, integridad, disponibilidad, autenticidad y privacidad.

MONPEZA SAS manifiesta su voluntad de trabajar constantemente para asegurar el cumplimiento de las políticas adoptadas en el presente documento y garantizar que formen parte de la cultura de la empresa.

Todo el personal de MONPEZA SAS, incluyendo operarios, coordinadores, funcionarios administrativos y directivos, deben conocer y cumplir esta política.

3. OBJETIVOS ESPECIFICOS

1. Garantizar que los empleados y/o contratistas usuarios de la información puedan acceder a la misma de forma ágil y segura, permitiéndose el desempeño eficiente de las funciones a cargo de MONPEZA SAS.

2. Asegurar que la información tenga la calidad óptima para la finalidad autorizada por su titular y la necesidad requerida por MONPEZA SAS.

3. Evitar pérdidas o alteración de la información a cargo de MONPEZA SAS.

4. Garantizar que el acceso de la información sea exclusivo de los empleados y/o contratistas asignados para su uso.

5. Generar un cambio organizacional a través de la generación de conciencia en seguridad y privacidad de la información por parte de los empleados y/o contratistas de MONPEZA SAS.

6. Establecer los mecanismos de aseguramiento físico y digital de la información para garantizar su confidencialidad, integridad, disponibilidad, autenticidad y privacidad.

7. Gestionar los riesgos de seguridad de la información.

8. Establecer las medidas para mitigar el impacto de los incidentes de seguridad de la información.

9. Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información.

4. ALCANCE Y APLICABILIDAD

Hace parte del alcance de la presente política, toda la información creada, procesada y/o utilizada por MONPEZA SAS en distintas formas, independientemente del medio (digital, manuscrita, fonética, impresa), presentación y/o lugar en el cual se encuentre ubicada.

Todos los empleados y/o contratistas de MONPEZA SAS, incluyendo operarios, coordinadores, funcionarios administrativos y directivos, deben conocer y cumplir esta política.

5. DEFINICIONES Y/O GLOSARIO

Con el propósito de facilitar la comprensión de la presente política se deben tener en cuenta las siguientes definiciones:

- **Activo de Información**: Es toda aquella información o elemento que reside en medio electrónico o físico, que tiene un significado y valor para MONPEZA SAS, y por ende necesita ser protegido.
- **Antivirus:** Software cuya función es detectar y/o eliminar virus informáticos
- **Ambiente:** Conjunto de elementos o componentes tecnológicos o, grupos de sistemas de información, en los cuales reside o fluye información y datos de negocio.
- **Ataques de denegación de servicio**: Un ataque de denegación de servicios, también llamado ataque DoS es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

- **Cifrado:** Proceso sistemático que convierte la información legible en formato ilegible mediante la utilización de algoritmos matemáticos y llaves criptográficas. El cifrado se utiliza para proteger la información de la divulgación no autorizada.
- **Código móvil:** Se trata de virus, troyanos, gusanos o programas "broma", es decir, que simulan ser virus sin serlo
- **Confidencialidad:** Es el principio de la seguridad de la información que busca asegurar que la información de la empresa sea accedida únicamente por el personal autorizado.
- **Componentes de infraestructura tecnológica**: Activos de información referentes a plataformas tecnológicas tales como bases de datos, servidores de aplicaciones, dispositivos de red, plataformas tecnológicas, entre otros.
- **Correo no deseado:** Mensaje de correo basura no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
- **Custodio o usuario de un equipo computacional**: Empleado de la compañía que tiene el control físico o tenencia del equipo computacional y es el responsable de vigilar o proteger el activo tecnológico en mención.
- **Dato Personal:** Información que identifique o permita identificar a una persona natural.
- **Disponibilidad:** Es el principio de la Seguridad de la Información que busca asegurar que la información de la empresa sea accesible y utilizable cuando sea requerida.
- **Escaneo de vulnerabilidades**: Proceso que ejecuta una solución tecnológica determinada para identificar las vulnerabilidades que presenta un componente de infraestructura tecnológica
- **Firma digital:** Esquema matemático que sirve para demostrar la autenticidad de un mensaje digital.
- **Incidente de seguridad:** Es un evento o serie de eventos no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Es el principio de la Seguridad de información que busca asegurar que la información esté protegida conta modificaciones no autorizadas para garantizar su constancia, exactitud y completitud.
- **Información confidencial:** Es la información de uso exclusivo por parte de usuarios claramente identificados y autorizados dentro de la entidad.
- **Incidente:** Una interrupción no planificada de un Servicio de TI o una reducción de la Calidad de un Servicio de TI.
- **Seguridad de la información:** Es el conjunto de medidas que busca preservar la Confidencialidad, Integridad y Disponibilidad de la información.

- **Sistemas de Información:** Conjunto de componentes tecnológicos tales como bases de datos, servidores de aplicaciones, dispositivos de red, datos y personas que permiten el almacenamiento, transmisión y procesamiento de la información
- **Virus:** Programa informático que puede reproducirse y puede infectar a otro programa para alterar su funcionamiento.
- **Vulnerabilidad:** Debilidad en un sistema que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Los principios que deben respetarse, en base a las dimensiones básicas de la seguridad de la información, son los siguientes:

- **Confidencialidad:** Propiedad por la cual únicamente puede acceder a la información gestionada por MONPEZA SAS, quién esté autorizado para ello, previa identificación, en el momento y por los medios habilitados.
- **Integridad:** Propiedad que garantiza la validez, exactitud y completitud de la información gestionada por MONPEZA SAS, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación y permitiendo que sea modificada únicamente por quién esté autorizado para ello.
- **Disponibilidad:** Propiedad de ser accesible y utilizable en los intervalos acordados. La información gestionada por MONPEZA SAS es accesible y utilizable por los clientes y usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- **Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta MONPEZA SAS, especialmente en materia de protección de datos personales.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se enumeran las políticas de seguridad de la información:

7.1 Política de Responsabilidades de la Seguridad de la Información: Esta política reconoce que la responsabilidad final de los activos de información de MONPEZA SAS está en quienes los “poseen” y “utilizan”. Por lo tanto, la responsabilidad de asegurar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información depende de cada una de las personas que utilizan, supervisan y administran los activos.

Por lo tanto, MONPEZA SAS define las responsabilidades frente a la seguridad de la información para los empleados y/o contratistas y para los administradores de los componentes funcionales y técnicos, así:

7.1.1 Responsabilidades del Líder de Seguridad de la Información: El líder de Seguridad de la información de MONPEZA SAS será su representante legal y deberá cumplir con las siguientes responsabilidades:

- Evaluar, identificar y estimar la situación de MONPEZA SAS frente a la seguridad y privacidad de la información.
- Actualizar los documentos técnicos de seguridad de la información (Políticas, Manuales, lineamientos)
- Incluir dentro de los documentos jurídicos vinculantes con empleados y/o contratistas sus responsabilidades y las de MONPEZA SAS en cuanto a seguridad de la información.
- Promover y mantener un ambiente de cultura y sensibilización de la seguridad de la información para los empleados y/o contratistas usuarios de los sistemas, archivos, datos, e información de MONPEZA SAS.
- Coordinar que todos los empleados y/o contratistas de MONPEZA SAS reciban educación, formación y sensibilización sobre la importancia de la seguridad de la información.
- Garantizar que los empleados y/o contratistas comprenden sus responsabilidades frente a la seguridad de la información y la idoneidad de acuerdo con el rol que desempeñan.
- Exigir a todos los empleados y/o contratistas la aplicación de la Política de Seguridad de la Información de acuerdo con los procedimientos establecidos.
- Coordinar revisiones periódicas para verificar el cumplimiento de las políticas de seguridad de la información de los activos y sistemas de información de MONPEZA SAS.
- Levantar e identificar los riesgos de seguridad de la información.
- Coordinar las actividades correspondientes a la gestión de incidentes seguridad de la información y seguridad digital.
- Coordinar la implementación de las mejoras en las plataformas frente a la seguridad de la información (hardware, software, canales de comunicación de datos e infraestructura IT)
- Definir los marcos de tiempo aceptables para recuperar la información, así como, identificar los impactos en caso de una interrupción extendida del servicio y/o un ataque.
- Definir la continuidad del objeto misional MONPEZA SAS mediante el establecimiento de planes de contingencia, continuidad del negocio y requerimientos de recuperación de información en caso de emergencia.

- Realizar la aprobación a las modificaciones de la política, manuales, lineamientos y/o procedimientos relacionados con seguridad de la información.

7.1.2 Responsabilidades del Administrador de los Sistemas de Información: MONPEZA SAS contará con un administrador de los sistemas de información quien deberá:

- Identificar los activos de información, incluyendo los requerimientos de confidencialidad, integridad, disponibilidad, autenticidad y privacidad.
- Clasificar la información de MONPEZA SAS, identificando la existencia de datos personales.
- Definir los empleados y/o contratistas que deben tener acceso a la información, de acuerdo con sus funciones dentro de MONPEZA SAS.
- Realizar junto con el Líder de Seguridad de la Información una evaluación anual de riesgos con el fin de estimar los controles establecidos para mantener la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de los activos de información de MONPEZA SAS.
- Con el soporte de un concepto técnico en la materia, definir los requerimientos de seguridad para proporcionar un nivel adecuado de protección a los documentos, datos y aplicaciones críticas de conformidad con los estándares y procedimientos de seguridad.
- Apoyar al Líder de Seguridad de la Información con las capacitaciones requeridas para la creación de la cultura de seguridad y privacidad de la información.

7.1.3 Responsabilidades del Líder de Protección de Datos Personales: De acuerdo con lo establecido por la Política de Tratamiento de Datos Personales de MONPEZA SAS, se designará a un Líder de Protección de Datos Personales que deberá:

- Garantizar el ejercicio de los derechos de los titulares de la información personal.
- Tramitar, proyectar y contestar las consultas y reclamos de protección de datos personales ante las autoridades y/o titulares de la información.
- Implementar y supervisar el cumplimiento de las obligaciones para la protección de datos personales, de acuerdo con la Política de Tratamiento de Datos Personales de MONPEZA SAS.
- Coordinar con el Líder de Seguridad de la Información y el Administrador de los Sistemas de Información que se cumpla con las medidas de seguridad y privacidad para los activos de información que contengan datos personales.

7.1.4 Responsabilidad de los Usuarios de los Activos de Información: Los usuarios son todos los empleados y/o contratistas de MONPEZA SAS que utilizan

los activos de información con ocasión a sus funciones y tienen la responsabilidad de cumplir con los lineamientos y políticas de seguridad de la información.

7.2 Política de Seguridad de los Recursos Humanos: MONPEZA SAS mantendrá los mecanismos necesarios para asegurar que sus empleados y/o contratistas cumplan con las responsabilidades frente a los temas de seguridad de la información durante la relación laboral y/o contractual y al momento de su finalización. Para lo anterior, tendrá en cuenta lo siguiente:

- MONPEZA SAS definirá los roles y controles de acceso a la información de la empresa según el cargo y las responsabilidades de los empleados y/o contratistas.
- Será el Líder de Seguridad de la Información, quien deberá desplegar esfuerzos para generar conciencia y apropiación de los empleados y/o contratistas sobre sus responsabilidades en el marco de la Política de Seguridad de la Información, con el fin de mitigar los riesgos frente al mal uso de los recursos tecnológicos y así asegurar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información.
- En el proceso de selección de empleados y/o contratistas de prestación de servicios, MONPEZA SAS debe incorporar mecanismos para establecer la idoneidad del candidato, y asegurar que conozca su deber de confidencialidad y seguridad para el manejo de la información a la cual deba acceder en ejercicio de su función y/o responsabilidad.
- Todos los empleados y/o contratistas que identifiquen cualquier anomalía, debilidad, mal funcionamiento y/o incidente de seguridad de la información deberán reportarlo de forma inmediata al Líder de Seguridad de la Información.
- Se incluirán en las minutas de los contratos laborales o de prestación de servicios cláusulas y obligaciones referentes al cumplimiento de la Política de Seguridad de la Información.
- La presente Política de Seguridad de la Información deberán ser divulgada a todos los empleados y/o contratistas, proveedores, o terceros que, debido al cumplimiento de sus funciones y/o obligaciones, compartan, utilicen, recolecten, procesen, intercambien y/o consulten información.
- Cuando un empleado y/o contratista termine su relación laboral y/o contractual con MONPEZA SAS, el Líder de Seguridad de la Información, coordinará lo correspondiente al retiro a los accesos lógicos a las plataformas y los activos de información. Los accesos deben ser removidos de forma inmediata y las cuentas de acceso deben colocarse en estado inactiva.
- Cuando un empleado y/o contratista termine su relación laboral y/o contractual, el Líder de Seguridad de la Información (Representante legal) deberán verificar la entrega de la información en los repositorios de red autorizados para garantizar su preservación y conservación.

- Cuando un empleado y/o contratista termine su relación laboral y/o contractual, el Líder de Seguridad de la Información deberá verificar que los activos de Información asignados a los funcionarios, contratistas, pasantes o proveedores sean devueltos.
- Cuando se requiera retirar de las instalaciones de MONPEZA SAS activos informáticos, se deberá solicitar autorización Líder de Seguridad de la Información, con el fin de registrar, controlar y hacer seguimiento a los mismos. El usuario que retire el activo será el responsable de la custodia, salvaguarda de la información que allí este almacenada.
- Los empleados y/o contratistas que tengan activos informáticos a su cargo, son responsables de la pérdida o daño que sufran, cuando lo anterior no se ocasione por el deterioro natural, por su uso normal o por otra causa justificada.
- Los sistemas y herramientas de trabajo que le han sido asignados por MONPEZA SAS a sus empleados y/o contratistas, que incluyen, sin limitarse, computadores de escritorio y portátiles, teléfonos celulares, correo electrónico corporativo y demás sistemas de internet, son herramientas de trabajo que contienen información de interés no solo para los empleados y/o contratistas, sino así mismo para MONPEZA SAS, la cual es considerada como material clasificado de propiedad de esta última. Por lo anterior, estas herramientas deben ser utilizadas exclusivamente para el desarrollo de sus actividades laborales o de las obligaciones contractuales, y el empleado y/o contratista autoriza, por razones de seguridad para que, directamente o por medio de terceras personas, MONPEZA SAS efectúe revisiones periódicas inconsultas de los sistemas, de la información contenida en el correo electrónico y/o celular institucional, así como de los archivos contenidos en los equipos asignados, sin que ello conlleve la violación de la intimidad o privacidad de la información.
- Cuando un empleado y/o contratista termine su relación laboral y/o contractual, el Líder de Seguridad de la Información deberán verificar que el usuario entregue copia de los mensajes electrónicos institucionales almacenados en su buzón de correo, para que estos puedan ser consultados posteriormente.

7.3 Política de Gestión de Activos de Información: El Líder de Seguridad de la Información establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información con el objetivo de garantizar su protección. Dichos lineamientos se impartirán teniendo en cuenta lo siguiente:

- MONPEZA SAS mantendrá un inventario de los activos de información que soportan los procesos del negocio, cada activo de información tendrá un responsable que esté en capacidad de clasificarlo y definir el nivel adecuado

de protección que requiera, así como deberá detallar la información contenida y las instalaciones de procesamiento de información.

- Los empleados y/o contratistas deben actuar con diligencia en la custodia, cuidado y buen uso de los activos físicos y tecnológicos que se les haya asignado.
- Los activos de información serán identificados y clasificados siguiendo los criterios de confidencialidad, integridad y disponibilidad.
- Se debe llevar un inventario de los activos tecnológicos (inventario de los servidores, y equipos de comunicación activos existentes dentro de las instalaciones de la empresa o fuera de ella, y equipos de cómputo)
- Todos los equipos de cómputo, impresoras, equipos activos y servidores deberán estar etiquetados para su identificación, control e inventario.
- Se deben establecer procedimientos para la movilización, adquisición y baja (de manera técnica) de los equipos.
- El Líder de Seguridad de la Información debe autorizar el acceso a la red interna por parte de los dispositivos personales de sus empleados y contratistas (teléfonos inteligentes, tabletas, portátiles, entre otros).
- Para el caso de re-uso de activos tecnológicos, se realizará la generación de copias de respaldo de la información y borrado seguro de medios.
- Todos los empleados y contratistas deberán devolver todos los activos de información que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

7.4 Política de Control de Acceso: El Líder de Seguridad de la Información en conjunto con los responsables de los activos de información, teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de tecnologías e infraestructura física (instalaciones y oficinas), con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física en pro de salvaguardar la integridad, disponibilidad y confidencialidad de la información de acuerdo con los siguientes lineamientos:

- Todos los empleados y/o contratistas que accedan a las plataformas tecnológicas de MONPEZA SAS dispondrán de un usuario y una contraseña (credencial) que deben proteger para garantizar su confidencialidad, está credencial es de uso personal e intransferible.
- Las contraseñas asignadas deben cumplir con las condiciones de complejidad que garanticen su seguridad.
- Los empleados y/o contratistas deben solicitar la creación, modificación, inhabilitación o eliminación de credenciales siguiendo el proceso de gestión de acceso lógico siendo responsables de las actuaciones realizadas con dichas credenciales.

- MONPEZA SAS asignará, modificará o revocará los permisos de acceso de los usuarios a las plataformas tecnológicas, siguiendo el proceso de gestión de acceso lógico y teniendo en cuenta las matrices de roles y perfiles definidas para cada plataforma.
- MONPEZA SAS establecerá las situaciones en las que permitirá el acceso remoto a los recursos tecnológicos y a los activos de información, así como, los mecanismos de autorización y conexión a la red interna. Es responsabilidad de los empleados y/o contratistas hacer el uso adecuado del recurso o la información otorgada.
- MONPEZA SAS debe autorizar el acceso a la red interna de los dispositivos personales de los empleados y/o contratistas como teléfonos inteligentes, tabletas o portátiles.
- Los derechos de acceso de todos los empleados y/o contratistas a la información y a las instalaciones de procesamiento de información se debe retirar al terminar su empleo, contrato o acuerdo, o se debe ajustar cuando se hagan cambios.

7.5 Política de Seguridad Física y del Entorno: MONPEZA SAS, a través del Líder de Seguridad de la Información, debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas y controlar el acceso y permanencia del personal en las oficinas e instalaciones con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad y disponibilidad de la información, de acuerdo con los siguientes lineamientos:

- Todos los empleados y/o contratistas que se encuentren en las instalaciones físicas de MONPEZA SAS deben estar debidamente identificados con su carné, documento y/o distintivo que acredite su tipo de vinculación; en caso de carné debe portarse en un lugar visible.
- MONPEZA SAS debe asegurar todas sus áreas físicas acorde con el valor de la información que allí sea procesada, almacenada y trasmitida. Los sitios restringidos y/o cualquier otro lugar donde se procese información deberán tener controles de acceso y estar señalizados.
- El acceso de personal no autorizado debe ser aprobado por parte de Líder de Seguridad de la Información.
- Todos los empleados y/o contratistas de MONPEZA SAS son responsable de bloquear la sesión de su equipo de cómputo en el momento de dejarlo desatendido.
- En el caso que los empleados y/o contratistas de MONPEZA SAS tenga bajo su custodia un documento físico clasificado como información confidencial, deberá mantenerlo bajo llave cuando su puesto de trabajo se encuentre desatendido.

- Los equipos de cómputo tendrán configurado un fondo de pantalla y un protector de pantalla. Este último se debe activar después de 3 minutos de inactividad y se desbloqueará mediante el uso de las credenciales del usuario.

7.6 Política de Seguridad de las Operaciones: El Líder de Seguridad de la Información será el encargado de la operación y administración de los recursos tecnológicos que soportan la operación y velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, y deberá realizar y mantener copias de seguridad de la información en medio digital.

7.7 Política de Seguridad para Relación con Proveedores: MONPEZA SAS comunicará a sus proveedores las políticas de seguridad de la información.

7.8 Política Gestión de Incidentes de Seguridad de la Información: Se deberá desarrollar y difundir entre los empleados y/o contratistas un mecanismo claro y efectivo para reportar incidentes a la seguridad de la información. Los incidentes de seguridad de la información deben registrarse de manera exacta y reportarse al Líder de Seguridad de la Información de forma inmediata y sin dilación. El Líder de Seguridad de la Información debe proyectar y registrar el proceso de reporte de incidentes de seguridad de la información, así como debe tomar las acciones correctivas, para mitigar los riesgos que surjan. A los usuarios, internos y externos, involucrados en el incidente, se le respetará el debido proceso apropiado a cada nivel de incidente. Los incidentes que involucren acciones legales o disciplinarias serán remitidos a la instancia que corresponda

7.9 Política de Revisión Periódica y Auditoria de la Política de Seguridad de la Información: El Líder de Seguridad de la Información será el responsable de coordinar revisiones periódicas al cumplimiento de la Política de Seguridad de la Información. Estas revisiones podrán realizarse con el apoyo del Administrador de los Sistemas de Información o mediante la contratación de un tercero experto en la materia.

8. INCUMPLIMIENTO DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El Líder de Seguridad de la Información deberá velar por el cumplimiento de las responsabilidades y deberes frente a la seguridad de la información por parte del recurso humano de la empresa, por lo tanto, las siguientes son algunas las actuaciones que pueden causar un incumplimiento de la presente Política:

- No firmar los acuerdos de confidencialidad o incumplir dicho acuerdo.
- Incumplir los lineamientos de la Policita de Seguridad de la Información.

- No reportar oportunamente los incidentes de seguridad y/o violaciones a la Política de Seguridad de la Información cuando se tenga conocimiento de ello.
- No cumplir con los controles establecidos por MONPEZA SAS para la protección de los activos de información.
- Ingresar a sitios restringidos o áreas sensibles sin previa autorización o acompañamiento de personal autorizado.
- No mantener la confidencialidad en sus credenciales de acceso a los sistemas de información.
- Hacer uso de la red interna para obtener, mantener o difundir material relacionado con pornografía, hacking o cualquier otro contenido que vaya en contra del Reglamento Interno de Trabajo.
- Recibir o enviar información confidencial de MONPEZA SAS a través de correos electrónicos personales, diferente al asignado por la empresa.
- Permitir el acceso a la red interna a dispositivos no autorizados.
- Distribuir o enviar software malicioso utilizando la plataforma tecnológica de la empresa.
- Retirar de las instalaciones de la entidad Información confidencial sin previa autorización.
- Instalar software no autorizado en los equipos de trabajo.
- No cumplir con la Política de Tratamiento de Datos Personales definida por la empresa.

En caso de incumplimiento de la Política de Seguridad de la Información se procederá de acuerdo con lo establecido en el Reglamento Interno de Trabajo y el Código Sustantivo del Trabajo.

9. VIGENCIA

La presente Política de Seguridad de la Información rige a partir de su aprobación.

Aprobada y suscrita el 23 de enero de 2024

LUIS ERNESTO MONTOYA PEÑALOZA
Representante Legal
MONPEZA SAS
NIT. 900.448.332-9