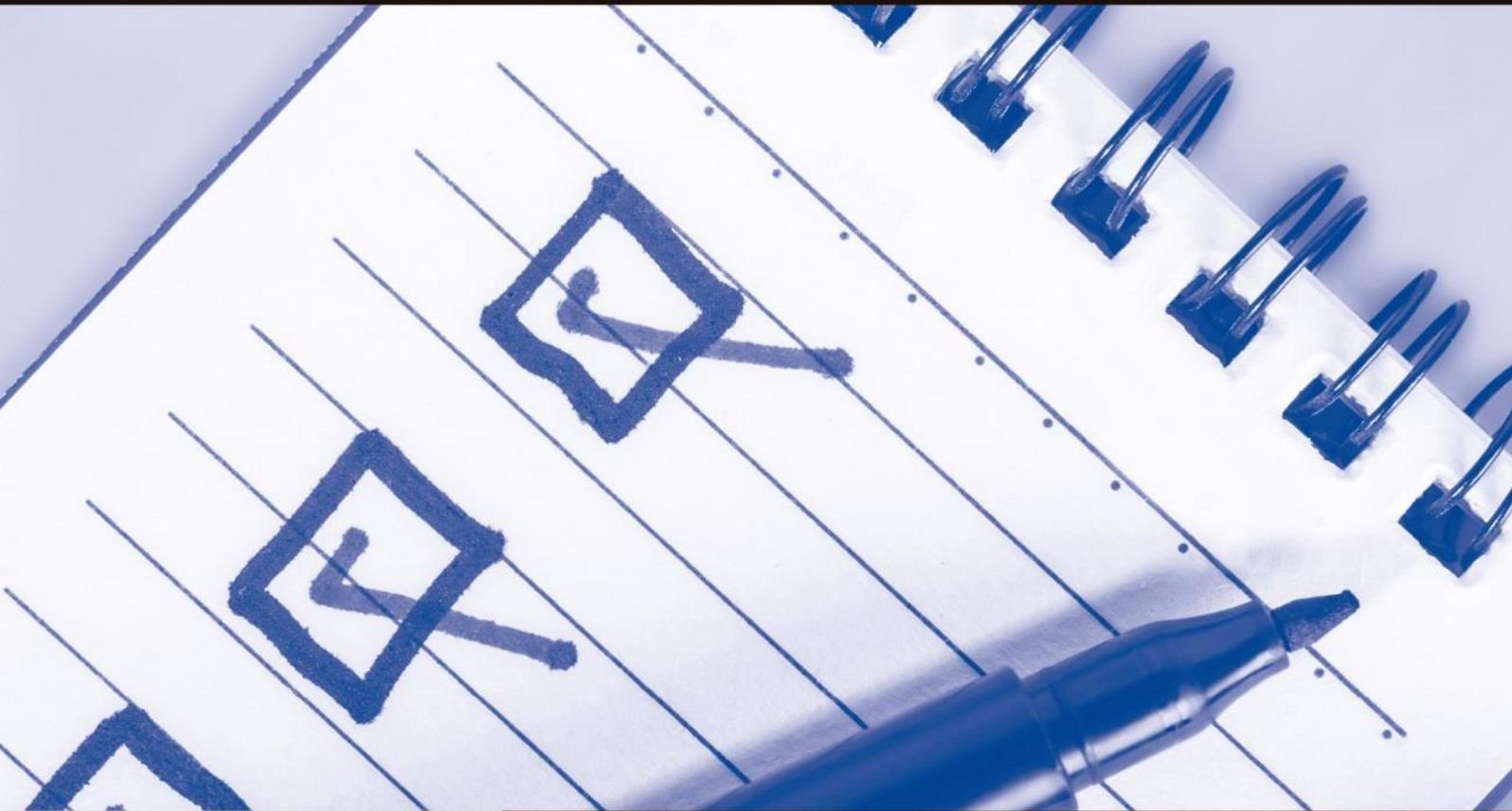


Febrero 2022



Política de Seguridad de la Información

COMPROMISO Y ACCIÓN MOURA

PRESENTACIÓN

Grupo Moura reconoce la importancia de la Seguridad de la Información como herramienta para cumplir con su misión, aspiración y valores, así como invierte constantemente en el crecimiento profesional de sus empleados y en tecnologías que garanticen la excelencia de sus productos y servicios.

Por eso, es fundamental proteger sus activos, ya que, si se utilizan de forma inadecuada, pueden provocar un daño irreparable al Grupo Moura, además de afectar su imagen en el mercado. De esta forma, preservar activos como: la información (manuscrita e impresa, transmitida física o por medios electrónicos, los equipos tecnológicos y su reputación se vuelven imprescindibles).

Así, se creó la Política de Seguridad de la Información para asegurar el cumplimiento de la legislación vigente y los requisitos comerciales.

Es responsabilidad de todos, independientemente del cargo o función, conocer y cumplir la Política de Seguridad de la Información del Grupo Moura, además de aplicarla constantemente en su actividad diaria, respetando y difundiendo su contenido.

Esta Política se mejorará periódicamente para mantenerla alineada con las necesidades comerciales y nuestros crecientes desafíos.

DocuSigned by:

E73F0A63687043F...
Moacy Freitas
Dirección de Personas e Organización

DocuSigned by:

77C6E93CDB7437...
Tiago Tasso
Dirección Financiera, Compras y TI

DocuSigned by:

4CD7DD77C98D4FF...
Eduardo Lepold

DocuSigned by:

84C12296AAA5444...
Tiago Macedo
Gestión de Auditoría y Riesgos

POL_007_Política de Seguridad de la Información**HOJA DE CONTROL****Informaciones Generales**

Título	Política de Seguridad de la Información
Número de referencia	POL_007
Edición	Ed.02
Estatus	Revisión
Aprobador	Comité de Auditoria y Riesgo
Validez	Indeterminado
Área Propietaria de la Política	Seguridad de la Información
Alcance del negocio	Grupo Moura
Alcance de la Geografía	Global
Palabras clave	Seguridad de la Información; Política;

Aprobada en 22-02-22

SUMÁRIO

1. OBJETIVO	5
2. ALCANCE	5
3. PRINCÍPIOS DE SEGURIDAD DE LA INFORMACIÓN	5
4. TERMINOS Y DEFINICIONES	5
5. PROVISIONES GENERALES	7
6. RESPONSABILIDADES	12
7. PENALIDADES	15
8. DISPOSICIONES FINALES	15
9. TERMINO DE CIENCIA E RESPONSABILIDAD	15

1. OBJETIVO

Esta Política de seguridad de la información (**PSI**) tiene como objetivo:

Declarar formalmente el compromiso de la Dirección de Grupo Moura en promover lineamientos estratégicos, responsabilidades, competencias y apoyo al Sistema de Gestión de Seguridad de la Información (SGSI), a fin de garantizar la protección de sus activos tangibles e intangibles;

Establecer las responsabilidades y límites operativos de los empleados de Grupo Moura en materia de seguridad de la información, reforzando la cultura interna y priorizando las acciones necesarias de acuerdo con el negocio.

2. ALCANCE

Esta **PSI** es un documento interno, con valor legal y aplicabilidad inmediata e indistinta, a partir de su publicación, a todos los empleados del Grupo Moura controlados en Brasil y en el exterior, independientemente de su empresa, ubicación, función y cargo. También es aplicable a cualquier empresa o individuo que tenga o haya tenido una relación con Moura.

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- a) Conservar y proteger la información de Grupo Moura o bajo su responsabilidad, a lo largo de su ciclo de vida, contenida en cualquier soporte o formato de vulnerabilidades y amenazas;
- b) Prevenir y reducir los impactos generados por los incidentes de seguridad de la información, asegurando la confidencialidad, integridad, disponibilidad, autenticidad y legalidad en el desarrollo de las actividades profesionales;
- c) Asegurar relaciones transparentes y éticas y frenar todas las formas de corrupción, fraude, soborno, favorecimiento y extorsión practicados por los empleados;
- d) Cumplir con la legislación brasileña y otros instrumentos regulatorios relacionados con el negocio en materia de Seguridad de la Información.

4. TÉRMINOS Y DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, que podría resultar en daños al Grupo Moura.

Aplicaciones de Comunicación: Conjunto de códigos e instrucciones compilados, ejecutados o interpretados por un recurso de tecnología de la información y la comunicación, almacenados en un dispositivo o en la nube, que se utilizan para el intercambio rápido de mensajes, contenido e información multimedia.

Activo: Todo aquello que tenga valor para el Grupo Moura y necesite una protección adecuada.

Activo Intangible: Cualquier elemento que tenga valor para el Grupo Moura y que se encuentre en soporte digital o esté constituido de forma abstracta, pero registrable o perceptible, por ejemplo, pero no limitado a datos, reputación, imagen, marca y conocimiento.



Autenticidad: Garantizar que la información sea válida y confiable, pudiendo generar evidencia irrefutable de la identificación de quienes la crearon, editaron o emitieron.

Backup: Resguardo de la información, que se realiza a través de la reproducción y / o reflejo de una base de archivo, con el propósito de su plena capacidad de recuperación en caso de incidencia o necesidad de restauración, o incluso, constitución de una infraestructura de activación inmediata en caso de un incidente o una necesidad justificada del Grupo Moura

Colaborador: Empleado, becario, prestador de servicios, subcontratado, proveedor, menor aprendiz o cualquier otra persona u organización que pueda tener relación profesional, directa o indirectamente, con el Grupo Moura.

Confidencialidad: Garantizar que solo accedan a la información aquellos expresamente autorizados y que se encuentra debidamente protegida del conocimiento de terceros.

Disponibilidad: Garantizar que la información y los Recursos de Tecnología de la Información y Comunicación estén disponibles siempre que sea necesario y con la debida autorización de acceso o uso.

Dispositivos móviles: equipos que se pueden transportar fácilmente debido a su portabilidad, con capacidad para registrar, almacenar o procesar información, además de la posibilidad de establecer conexiones a Internet y otros sistemas, redes o cualquier dispositivo.

Dispositivos de almacenamiento de información extraíbles: dispositivos capaces de almacenar información que se puede eliminar del equipo, lo que permite la portabilidad de datos, como CD, DVD y pendrive.

Responsable de información: Colaborador responsable de crear / recibir, clasificar, divulgar, compartir, eliminar y destruir información. También es responsable de gestionar la validación, liberación y cancelación del acceso a su información. Cabe mencionar que dichas actividades pueden ser delegadas a otro empleado, siempre que sean otorgadas por el Responsable de Información.

Homologación: Proceso de evaluación y aprobación técnica de los Recursos de Tecnologías de la Información y la Comunicación para su uso en el entorno del Grupo Moura.

Identidad digital: Es la identificación del empleado en entornos lógicos, consistente en su usuario (*login*) y contraseña u otros mecanismos de identificación y autenticación como placa magnética, certificado digital, *token* y biometría.

Incidente de seguridad de la información y las comunicaciones: Ocurrencia identificada de un sistema, datos, información, servicio o estado de la red, que indica una posible violación de la Política de Seguridad de la Información o Normas complementarias, falla de los controles o una situación previamente desconocida que puede ser relevante para la seguridad de la información. .

Información: Conjunto de datos que, procesados o no, pueden ser utilizados para la producción, transmisión e intercambio de conocimientos, contenidos en cualquier medio, soporte o formato.

Integridad: garantizar que la información esté completa durante todo su ciclo de vida.

Internet: Red mundial de ordenadores interconectados por protocolo TCP / IP cuya infraestructura es abierta y colaborativa, accesible a través de dispositivos con conexión y autorizaciones suficientes y que permite obtener información de cualquier otro dispositivo que también esté conectado a la red, siempre que esté debidamente configurado.

Legalidad: Garantizar que toda la información sea elaborada y gestionada de acuerdo con las disposiciones del Régimen Jurídico vigente.

Recursos de Tecnología de la Información y Comunicación (Recursos TIC): *hardwares, softwares*, servicios de conexión y comunicación o infraestructura física necesaria para la creación, registro, almacenamiento, manipulación, transporte, intercambio y eliminación de información.

Repositorios digitales (Cyberlockers): Plataformas de almacenamiento de Internet, como *Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare* y *Scribd*.

Riesgo: combinación de la probabilidad de materialización de una amenaza y sus impactos potenciales.

Seguridad de la información: es la preservación de la confidencialidad, integridad, disponibilidad, legalidad y autenticidad de la información. Su objetivo es proteger la información de diferentes tipos de amenazas para garantizar la continuidad del negocio, minimizar el daño comercial, maximizar el retorno de las inversiones y las nuevas oportunidades de transacciones.

Intento de Fraude: Actos que buscan violar los lineamientos establecidos en los documentos normativos del Grupo Moura y son frustrados por un error durante la planificación o durante su ejecución.

TIC: Tecnología de la información y comunicaciones

Infracción: Cualquier actividad que no respete las reglas establecidas en los documentos normativos del Grupo Moura.

5. PROVISIONES GENERALES

Interpretación: Esta **PSI** y sus documentos complementarios deben ser interpretados de manera restrictiva, es decir, las actividades que no estén contempladas en la normativa sólo deben realizarse previa autorización formal y previa del Gerente del empleado.

Publicidad: Esta **PSI** y sus documentos complementarios deben ser divulgados a los empleados mediante Comunicación Interna, con el objetivo de dar a conocer a todas las personas que tengan una relación profesional con Grupo Moura.

Propiedad: La información generada, accedida, manipulada, almacenada o descartada en el ejercicio de las actividades realizadas por los empleados, así como otros activos intangibles y tangibles puestos a disposición, son propiedad o están bajo la responsabilidad y derecho



exclusivo de uso de Grupo Moura y deben ser utilizado únicamente con fines profesionales.

Interpretación: Esta **PSI** y sus documentos complementarios deben ser interpretados de manera restrictiva, es decir, las actividades que no estén contempladas en la normativa solo deben realizarse previa autorización formal y previa del Gerente del empleado.

Publicidad: Esta **PSI** y sus documentos complementarios deben ser divulgados a los empleados a través de Comunicación Interna, con el objetivo de dar a conocer a todas las personas que tengan una relación profesional con el Grupo Moura.

Propiedad: Las informaciones generadas, accedidas, manipuladas, almacenadas o descartadas en el ejercicio de las actividades realizadas por los empleados, así como otros activos intangibles y tangibles puestos a disposición, son propiedad o están bajo la responsabilidad y derecho exclusivo de uso del Grupo Moura y deben ser utilizados únicamente con fines profesionales.

Propiedad Intelectual: El uso de obras intelectuales, software, diseños industriales, marcas, identidad visual o cualquier otro signo distintivo actual o futuro del Grupo Moura en cualquier soporte, incluido Internet y redes sociales, debe ser previamente autorizado por Grupo Moura y vinculado a actividades profesionales.

Clasificación de la información: Toda la información de propiedad o responsabilidad de Grupo Moura debe ser clasificada y protegida con controles específicos a lo largo de su ciclo de vida.

Confidencialidad: Está prohibido, en cualquier momento, divulgar información de propiedad o responsabilidad del Grupo Moura sin la autorización previa y formal del Responsable de la Información, a excepción de la información pública.

Uso de Activos: Los activos propiedad o bajo la responsabilidad de Grupo Moura solo deben ser utilizados con fines profesionales y de acuerdo con los lineamientos de los fabricantes y Grupo Moura.

Uso de Recursos TIC: Los Recursos TIC propiedad o bajo la responsabilidad de Grupo Moura solo deben ser utilizados con fines profesionales, de manera lícita, ética y moral y de acuerdo con las normas de Grupo Moura.

Mantenimiento de Activos: La gestión de activos en Grupo Moura debe cumplir con las recomendaciones de fabricantes y desarrolladores, y cualquier necesidad de mantenimiento, actualización o corrección de fallas técnicas solo puede ser realizada por DTISS, según el tipo de activo.

Inventario de Activos: El Grupo Moura debe realizar un inventario de *hardwares* y *softwares* de su propiedad, y DTISS debe indicar la información necesaria y ser responsable de su registro, almacenamiento y actualización.

Dispositivos móviles corporativos: Los dispositivos móviles deben ser utilizados cuando sean provistos o autorizados previa y expresamente por la Gerencia del empleado y aprobados por la Dirección, de acuerdo con el rol del empleado y las necesidades comerciales.

Uso de Recursos TIC / Dispositivos Móviles Privados: No está permitido el uso de Recursos TIC / Dispositivos Móviles Privados en la ejecución de cualquier actividad profesional, salvo autorización y justificación del Director del área.

Repositorios Digitales y Dispositivos Removibles: Está prohibido que los empleados utilicen repositorios digitales o dispositivos removibles no autorizados o aprobados por Grupo Moura para almacenar o transmitir información propiedad o bajo la responsabilidad de Grupo Moura.

Aplicaciones de comunicación instantánea: El uso de aplicaciones de comunicación instantánea para el intercambio de información corporativa debe cumplir con las normas establecidas por la **Norma de Uso de Recursos Informáticos**.

Medios sociales: El uso de los medios sociales para llevar a cabo actividades profesionales en nombre del Grupo Moura debe ocurrir solo cuando sea necesario y estrictamente para fines comerciales, de acuerdo con el Código de Ética de Moura. Dichas actividades deben realizarse a través de los Recursos TIC de Grupo Moura.

Conducta del empleado en el uso de los medios sociales: El empleado debe ser cauteloso, ético y seguro en relación con su exposición de una manera que no afecte la reputación del Grupo Moura, como rutinas, rutas y contactos, además del deber para preservar la confidencialidad profesional en las redes sociales.

Control de acceso: El Grupo Moura controla el acceso físico y lógico a sus entornos, activos e información. De esta forma, el empleado recibe una identidad digital para uso individual, intransferible y, en su caso, de conocimiento exclusivo.

El empleado es responsable del uso, protección y confidencialidad de su identidad digital, no pudiendo compartir, revelar, guardar, replicar, publicar o hacer uso no autorizado de sus credenciales, así como de terceros.

Para garantizar el control de acceso a los entornos físicos y lógicos del Grupo Moura, se deben utilizar los criterios del conjunto mínimo necesario (*least privilege*) y estrictamente necesario (*need to know*) a la hora de definir los accesos de cada empleado.

Entornos Lógicos: Los sistemas y recursos TIC que soportan los procesos e informaciones del Grupo Moura deben ser confiables, completos, seguros y disponibles para quienes los necesiten para el desarrollo de su actividad profesional. Para garantizar la seguridad establecida anteriormente, Grupo Moura utiliza los siguientes sistemas de protección activos y actualizados:

- Contra programas maliciosos y accesos no autorizados, como antivirus y *firewall*;
- Para indicar los intentos de intrusión realizados en entornos lógicos, como los Sistemas de Detección de Intrusiones (*Intrusion Detection Systems*) o IPS (*Intrusion Protection Systems*);
- Contra mensajes electrónicos no deseados o no autorizados como Antispam

Entornos Físicos: El Grupo Moura debe establecer perímetros de seguridad para proteger sus activos, especialmente aquellos que procesan o almacenan información / activos críticos para el negocio, e implementar controles para identificar y registrar el acceso a sus entornos.



Audio, Videos e Imágenes: Se prohíbe a los empleados cualquier actividad relacionada con la captura de audio, video o imágenes dentro de las instalaciones de Grupo Moura, sin la autorización previa y formal del **Departamento de Marketing**, excepto en eventos oficiales de Grupo Moura.

Contratación de Empleados y Proveedores de Bienes y Servicios: Los contratos en los que ocurre el compartimiento de información de propiedad o bajo la responsabilidad del Grupo Moura o se le da acceso a sus entornos o activos críticos deben estar precedidos por términos de confidencialidad y cláusulas contractuales relacionadas con la seguridad de la información.

Desarrollo y Adquisición de Software: Tanto el desarrollo interno y externo de softwares como las adquisiciones de mercado deben asegurar el cumplimiento de los requisitos de seguridad de la información y controles de acceso previstos en esta Política y otras Normas Complementarias, además de ser realizados únicamente por el **área DTISS**.

Salvaguardia (*Backup*): El Grupo Moura mantiene un proceso de salvaguardia de la información y los datos necesarios para la recuperación completa de sus sistemas (*backup*), con el fin de cumplir con los requisitos operativos y legales, además de asegurar la continuidad del negocio en caso de fallas, incidencias o su recuperación lo antes posible.

Análisis de Procesos y Recursos TIC: Los Gerentes de Área deben analizar sus procesos y Recursos TIC, a intervalos regulares, para asegurarse de que estén debidamente inventariados y sus gerentes identificados y conscientes, así como sus vulnerabilidades mapeadas y amenazas a la seguridad.

Monitoreo: El Grupo Moura monitorea sus entornos físicos y lógicos, buscando la efectividad de los controles implementados, la protección de sus activos, la reputación y la identificación de eventos o alertas de incidentes relacionados con la seguridad de la información.

Auditoría e Inspección: El Grupo Moura puede auditar o inspeccionar los Recursos TIC que se encuentran en sus instalaciones o que interactúan con sus entornos lógicos siempre que lo considere necesario, cumpliendo con los principios de proporcionalidad, razonabilidad y privacidad de sus propietarios o titulares.

Gestión de Riesgos: El **Área de Seguridad de la Información** debe identificar y evaluar los riesgos relacionados con la seguridad de la información y adoptar las mejores prácticas para su gestión.

Gestión del cambio: El avance y resultado de un cambio, especialmente en los sistemas y la infraestructura tecnológica del Grupo Moura, debe preservar los controles relacionados con la disponibilidad, integridad, confidencialidad y autenticidad de la información y realizados únicamente por DTISS.

Continuidad del negocio: Los procedimientos de gestión de la Continuidad del Negocio deben realizarse de acuerdo con los requisitos de seguridad de la información del Grupo Moura.

Inversiones: Las inversiones en Seguridad de la Información en Grupo Moura deben ser estudiadas y deliberadas por el área de **Seguridad de la Información** a la Dirección, alineadas con las áreas de negocio, considerando la viabilidad de las inversiones (costo x beneficio) y los

impactos de su aplicación a la calidad de los procesos de negocio

Reporte de Incidentes: El Grupo Moura tiene un canal de comunicación divulgado a sus empleados para reportar posibles casos de incidentes de seguridad de la información: seguranca.informacao@grupomoura.com.

Protección de datos personales: El Grupo Moura respeta la privacidad. Así, debe garantizar la disponibilidad, integridad y confidencialidad de los datos personales, a lo largo de su ciclo de vida, en cualquier formato de almacenamiento o soporte, con el mismo nivel de tratamiento de la información confidencial. El Grupo Moura deberá evaluar las siguientes medidas de seguridad de la información respecto al tratamiento de datos personales:

- I. Tratamiento autorizado de acuerdo con la legislación vigente en materia de protección de datos personales;
- II. Adopción de medidas de seguridad para proteger los datos personales del acceso no autorizado, situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o tratamiento inadecuado o ilícito;
- III. Elaboración de plan de análisis y respuesta a violaciones de datos personales;
- IV. Almacenamiento seguro, controlado y protegido, especialmente cuando se trata de datos personales confidenciales;
- V. Procesos de anonimización y seudonimización, cuando sea necesario;
- VI. Protocolos de cifrado en transmisión y almacenamiento, cuando se verifique que sea necesario;
- VII. Registro lógico de operaciones de procesamiento de datos personales;
- VIII. Eliminación segura de los datos personales al final de su finalidad y su conservación de acuerdo con hipótesis legales y reglamentarias;
- IX. Transferencia a los Agentes de Tratamiento de manera segura y estipulada por contrato;
- X. Mapeo y mantenimiento del inventario del flujo de datos personales;
- XI. Elaboración de informes de impacto de protección de datos personales, cuando sea necesario;
- XII. Gestión y tratamiento adecuado de las incidencias relacionadas con datos personales.

Capacitación: El Grupo Moura cuenta con un plan de capacitación periódico y anual dirigido a desarrollar y mantener las habilidades de los empleados en Seguridad de la Información.

Excepciones: Las excepciones solo se permitirán excepcionalmente a esta **Política**, y deben ser temporales y previamente aprobadas por el Director para que entren en vigor.

Las solicitudes de excepción deben enviarse por escrito al Gerente del empleado y, si se considera pertinente, se enviarán al Director para su análisis de factibilidad. Si es necesario, la solicitud de excepción se presentará a la Dirección Ejecutiva para su aprobación o rechazo.

Las excepciones pueden ser revocadas en cualquier momento por mera liberalidad del Gerente o del Director del empleado, debiendo informar inmediatamente a las áreas relacionadas de la denegación por parte de la persona que las hizo actuar, bajo pena de responsabilidad de quienes omitieron los daños sufridos por Grupo Moura, sus clientes o terceros.

6. RESPONSABILIDADES

Dirección

- I. Analizar, aprobar y declarar formalmente su compromiso con esta Política;
- II. Aprobar las inversiones en seguridad de la información en Grupo Moura, considerando la viabilidad e impactos de su aplicación en la calidad de los procesos de negocio;
- III. Analizar y aprobar, o no, excepciones excepcionales a esta Política.

Gestión de Auditoría y Riesgos

- I. Conocer esta Política y otros documentos complementarios de Grupo Moura;
- II. Analizar y aprobar esta Política y otras Normas Complementarias;
- III. Promover y llevar a cabo la gestión del SGSI, asegurando la implementación de controles, modelos, estándares y recursos necesarios para la protección de la información;
- IV. Promover la cultura de seguridad de la información en el Grupo Moura;
- V. Analizar y priorizar las acciones necesarias, equilibrando costo y beneficio;
- VI. Asistir, cuando sea necesario, al área de T&D - Capacitación y Desarrollo, en la capacitación de los empleados en seguridad de la información;
- VII. Orientar para que las actividades realizadas por DTISS sean adecuadas al negocio del Grupo Moura;
- VIII. Aprobar las inversiones en seguridad de la información en Grupo Moura junto con el Directorio Ejecutivo, considerando la factibilidad e impactos de su aplicación en la calidad de los procesos de negocios;
- IX. Analizar los incidentes de seguridad de la información reportados y presentar un informe para la deliberación del Directorio, cuando sea necesario;
- X. Establecer, cuando corresponda, procedimientos disciplinarios para determinar las responsabilidades de los involucrados en violaciones a la seguridad de la información y aplicar sanciones, cuando sea necesario.

Departamento do DTISS (Departamento de Tecnología de la Información)

- I. Hacer cumplir esta Política y otros documentos complementarios por parte de todos los empleados del Grupo Moura;
- II. Identificar y evaluar los riesgos relacionados con la seguridad de la información y proponer las mejoras y los recursos necesarios para las acciones de seguridad de la información;
- III. Realizar y monitorear estudios de tecnología, con el apoyo del Gestión de Auditoría y Riesgos, sobre posibles impactos en la seguridad de la información;
- IV. Elaborar y mantener actualizados los documentos que integran el SGSI, además de someterlos a la aprobación del Directorio o Gestión de Auditoría y Riesgos;
- V. Proponer, junto con el Gestión de Auditoría y Riesgos, normas y procedimientos internos relacionados con la seguridad de la información en el Grupo Moura;
- VI. Realizar la gestión, mantenimiento y administración de los Recursos TIC propiedad o bajo la responsabilidad de Grupo Moura;
- VII. Asegurar que todos los Recursos TIC utilizados en Grupo Moura cumplan con las

- recomendaciones de sus fabricantes o desarrolladores;
- VIII. Definir, analizar y priorizar las acciones necesarias, equilibrando costo y beneficio;
 - IX. Realizar el registro y monitoreo de acceso a los entornos lógicos de Grupo Moura;
 - X. Proporcionar y gestionar las identidades digitales para acceder al entorno lógico de Grupo Moura;
 - XI. Analizar o ayudar en el análisis de incidentes de seguridad de la información notificados;
 - XII. Evaluar si los requisitos de seguridad de la información están presentes antes de la adquisición, el mantenimiento o el desarrollo de softwares;
 - XIII. Asegurar que el avance y resultado de los cambios conserven controles relacionados con la disponibilidad, integridad, confidencialidad, autenticidad y legalidad de la información, especialmente en los sistemas e infraestructura tecnológica del Grupo Moura;
 - XIV. Asegurar la rápida recuperación de sus sistemas y procesos en situaciones de contingencia que involucren los Recursos TIC del Grupo Moura;
 - XV. Desarrollar y / o mantener procedimientos para resguardar la información y los datos necesarios para la recuperación de los sistemas del Grupo Moura;
 - XVI. Asegurar que los procedimientos de Gestión de la Continuidad del Negocio se lleven a cabo de acuerdo con los requisitos de seguridad de la información;
 - XVII. Asistir al área de **T&D - Capacitación y Desarrollo** en la capacitación de empleados en seguridad de la información.

Departamento legal

- I. Participar, apoyar y orientar, de acuerdo con los aspectos legales, los procesos de contratación y los requisitos legislativos relacionados con la seguridad de la información;
- II. Validar los borradores que deban cumplir con los controles de seguridad de la información aplicables a los contratos.

Departamento de GPM – Gestión de Personas Moura

- I. Realizar campañas de capacitación y difusión en seguridad de la información;
- II. Estipular controles de seguridad específicamente relacionados con los procesos de contratación, cierre y modificación de las actividades de los empleados;
- III. Asegurar la publicidad y disponibilidad de los documentos que integran el SGSI en el Grupo Moura;
- IV. Poner a disposición la normativa del Grupo Moura, además de resguardar y firmar el "Término de Ciencia y Responsabilidad" para la admisión de nuevos empleados.

Departamento de marketing y comunicación

- I. Autorizar o no, el uso de marcas, identidad visual y cualquier otro signo distintivo actual o futuro de Grupo Moura;
- II. Autorizar o no la grabación de audio, video o foto del local de Grupo Moura.

Gerente de información

- I. Autorizar o no la divulgación de cualquier información que sea propiedad o esté bajo la responsabilidad de Grupo Moura;
- II. Identificar violaciones o cualquier acción dudosa tomada por los empleados en el uso de la información del Grupo Moura y notificar al Gestión de Auditoría y Riesgos y al Gerente del empleado.

Gerente de Empleados

- I. Asegurar y gestionar el cumplimiento de esta PSI y otros documentos complementarios por parte de sus empleados;
- II. Identificar y medir las vulnerabilidades y amenazas en los procesos y actividades bajo su responsabilidad, las cuales deben ser tratadas con diligencia para reducir los impactos en el negocio;
- III. Autorizar, o no, el uso de Recursos TIC o dispositivos móviles privados por parte de sus empleados para el desempeño de cualquier actividad profesional en el Grupo Moura;
- IV. Asegurar que los activos propiedad o bajo la responsabilidad de Grupo Moura se utilicen con cuidado y de acuerdo con las pautas del fabricante y Grupo Moura;
- V. Aplicar, previa definición con el área de GPM, las sanciones por violación de esta PSI y documentos adicionales;
- VI. Identificar incidentes de seguridad de la información o cualquier acción cuestionable tomada por sus empleados, informando al Gestión de Auditoría y Riesgos de inmediato.

Colaboradores

- I. Conocer y mantenerse actualizado con esta PSI y otros documentos complementarios;
- II. Conocer y firmar el "Término de ciencia y responsabilidad";
- III. Utilizar los activos propiedad de Grupo Moura o bajo su responsabilidad de acuerdo con las directrices del fabricante, el desarrollador y Grupo Moura, con cuidado y celo;
- IV. Utilizar los activos e información de Grupo Moura únicamente con fines profesionales, de manera ética y legal, respetando los derechos y permisos de uso otorgados;
- V. Conservar la integridad, disponibilidad, confidencialidad, autenticidad y legalidad de la información a la que se acceda o manipule, no utilizándola, enviándola, transmitiéndola o compartiéndola de manera inapropiada, en ningún lugar o medio, incluido Internet;
- VI. No revelar información que sea propiedad o responsabilidad de Grupo Moura sin autorización previa y formal;
- VII. Utilizar las marcas y demás signos distintivos, patentes, diseños industriales, software y demás derechos de propiedad intelectual titularidad de Grupo Moura únicamente para fines profesionales y autorizados por Grupo Moura, de acuerdo con la actividad y función que desempeñe
- VIII. Garantizar la seguridad de su identidad digital, no compartir, divulgar o transferir a terceros;
- IX. Responder de todas y cada una de las actividades que se realicen en los Recursos TIC del Grupo Moura realizadas con su identidad digital;
- X. Cumplir con la legislación nacional vigente y otros instrumentos regulatorios relacionados con la actividad profesional;

XI. Informe formalmente a su Gerente de cualquier evento relacionado con la violación o posible violación de la seguridad o actividad sospechosa.

7. PENALIDADES

Infracciones: Cualquier actividad que intente eludir o faltar al respeto a los lineamientos establecidos en esta PSI o en cualquiera de los documentos complementarios del Grupo Moura debe ser considerada como una infracción y tratada por el Gestión de Auditoria y Riesgos a fin de determinar las responsabilidades de los involucrados de acuerdo con las "Medidas disciplinarias" del Grupo Moura, encaminadas a la aplicación de las sanciones aplicables previstas en las cláusulas contractuales y en la legislación vigente.

8. DISPOSICIONES FINALES

Este documento debe ser leído e interpretado de acuerdo con las leyes vigentes en cada país donde Grupo Moura opera, junto con las Normas y Procedimientos aplicables por Grupo Moura.

Esta Política, así como el resto de las Normas y Procedimientos de Grupo Moura están disponibles en *Sharepoint* o, en caso de indisponibilidad, se pueden solicitar a DTISS.

Cualquier consulta relacionada con esta **Política** deberá dirigirse al área de Seguridad de la Información a través de la dirección de correo electrónico: seguranca.informacao@grupomoura.com.

Esta **PSI** entra en vigor en la fecha de su publicación.

9. TERMINO DE CIENCIA Y RESPONSABILIDAD

Formato *Disclaimer* (para ciencia electrónica)

La conciencia del empleado debe recopilarse a través de una barrera de navegación en el inicio de sesión de la red o publicarse en la Intranet con el envío al correo electrónico corporativo de todos, como se describe a continuación:

Término de ciencia y responsabilidad

Confirmando que conozco el contenido de la Política de Seguridad de la Información del Grupo Moura, y reafirmo mi deber de cumplir, difundir y mantenerme siempre actualizado con las normas allí establecidas.

Formato Impreso (para firmar)

Término de Ciencia e Responsabilidad

Yo, _____ por la presente, Confirmando que conozco el contenido de la Política de Seguridad de la Información del Grupo Moura, y reafirmo mi deber de cumplir, difundir y mantenerme siempre actualizado con las normas allí establecidas.

Lugar, Fecha

Firma del Empleado
Código de Identificación del Empleado