

POLÍTICA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



En **GESTORÍA MONTERO-RÁEZ, S.L.P.** empresa dedicada a los **servicios de asesoría fiscal, laboral, contable y gestoría especializada en tramitación de escrituras**, nos comprometemos a implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) basado en la Norma ISO 27001:2022.

➤ Propósito

La política de seguridad de la información establece el compromiso de la organización con la protección de la información confidencial, la preservación de la integridad de los sistemas de información y la garantía de la disponibilidad de los recursos críticos. Esta política proporciona un marco para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con los requisitos de la norma ISO 27001.

➤ Alcance

Esta política se aplica a todos los activos de información, sistemas de información, procesos y personas dentro de la organización. Se extiende a todos los empleados, contratistas, consultores y terceros que interactúan con los sistemas de información de la organización.

➤ Compromiso de la Dirección

La alta dirección se compromete a proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI. La dirección promueve una cultura de seguridad de la información, estableciendo objetivos y metas medibles para mejorar constantemente la postura de seguridad de la organización.

➤ Cumplimiento Legal y Regulatorio

La organización se compromete a cumplir con todas las leyes, regulaciones y requisitos contractuales aplicables relacionados con la seguridad de la información. Se establecerán procesos para monitorear y garantizar el cumplimiento continuo de estos requisitos.

➤ Identificación y Evaluación de Riesgos

La organización realizará evaluaciones periódicas de riesgos para identificar y evaluar los riesgos de seguridad de la información. Se implementarán controles adecuados para mitigar los riesgos identificados a un nivel aceptable.

➤ Protección de Activos de Información

POLÍTICA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



Se implementarán controles físicos y lógicos para proteger los activos de información contra amenazas internas y externas. Se establecerán políticas y procedimientos para la gestión segura de datos, acceso a sistemas y servicios, y disposición segura de la información.

➤ **Gestión de Incidentes de Seguridad**

Se establecerán procedimientos para la detección, notificación, respuesta y recuperación de incidentes de seguridad de la información. La organización se compromete a minimizar el impacto de los incidentes y a restaurar la operatividad normal de los sistemas de información lo antes posible.

➤ **Formación y Concienciación**

Se proporcionará formación y concienciación en seguridad de la información a todos los empleados y partes interesadas relevantes. Se promoverá una cultura de seguridad de la información mediante la sensibilización sobre las responsabilidades individuales y la importancia de la seguridad de la información.

➤ **Revisión y Mejora Continua**

El SGSI será objeto de revisiones periódicas para garantizar su eficacia, adecuación y mejora continua. Se establecerán procesos para la revisión de la política de seguridad de la información y la identificación de áreas de mejora.

➤ **Responsabilidades Individuales**

Todos los empleados son responsables de cumplir con esta política, así como con los procedimientos y controles asociados. Se espera que todos contribuyan activamente a la protección de la información y al cumplimiento de los requisitos de seguridad de la organización.

➤ **Principios**

- o **Confidencialidad:** garantizar que la información sensible solo esté disponible para aquellos que tengan autorización para acceder a ella.
- o **Integridad:** asegurar que la información sea precisa, completa y no se haya modificado de manera no autorizada.
- o **Disponibilidad:** asegurar que la información esté disponible y accesible cuando sea necesario para usuarios autorizados.

POLÍTICA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



- o **Autenticación:** verificar la identidad de los usuarios y garantizar que solo las personas autorizadas puedan acceder a los recursos de información.
- o **Autorización:** controlar los derechos de acceso de los usuarios para garantizar que solo tengan acceso a la información y los recursos que necesitan para realizar sus funciones.
- o **Responsabilidad:** establecer la responsabilidad de los usuarios en el uso y manejo adecuado de la información y los recursos de la organización.
- o **Resiliencia:** garantizar la capacidad de la organización para recuperarse de incidentes de seguridad de manera oportuna y eficiente.
- o **Cumplimiento legal y normativo:** asegurar que la organización cumpla con todas las leyes, regulaciones y estándares relacionados con la seguridad de la información.
- o **Gestión de riesgos:** identificar, evaluar y mitigar los riesgos de seguridad de la información para proteger los activos de la organización.
- o **Cultura de seguridad:** fomentar una cultura organizacional que valore y priorice la seguridad de la información, involucrando a todos los empleados en la protección de los activos de la organización.

La dirección asegura que la presente Política de Seguridad de la Información será mantenida, entendida y revisada periódicamente, comunicada a todos los empleados y puesta a disposición de todas las partes interesadas.

Madrid, a 03 de febrero de 2025

Fdo.: La dirección