1. Objetivo

La política de Seguridad de la Información de Coguasimales Service S.A.S., busca proveer las herramientas (procesos, políticas, personal y tecnología) necesarias para brindar apoyo y orientación a los colaboradores con respecto a la seguridad de los activos de información, alineadas con los requisitos del negocio y normativa aplicable.

2. Alcance

La Política de Seguridad de la Información es de cumplimiento obligatorio para todos los actores de Coguasimales Service S.A.S., sin excepción, independientemente de su relación contractual, el proceso en el que participen o el nivel de funciones que desempeñen.

Esta política aplica a la asamblea de accionistas, colaboradores, contratistas, proveedores y aliados que, en el ejercicio de sus actividades dentro de la organización, accedan a información o activos relacionados, ya sea por medios lógicos o físicos.

Todos los actores mencionados deben conocer, comprender y aplicar los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI), conforme a lo definido en el "Manual de Lineamientos y Controles de Seguridad de la Información".

3. Normativa aplicable

NTC ISO/IEC 27001:2022: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos.

Ley 1581 de 2012: **Ley de Protección de Datos Personales**: Establece disposiciones para la protección de datos personales y la privacidad de los individuos. Esta ley regula cómo se deben manejar, almacenar y proteger los datos personales.

Decreto 1377 de 2013: **Reglamento de la Ley 1581 de 2012**. Establece las disposiciones para la implementación de la Ley de Protección de Datos Personales y proporciona directrices adicionales sobre la protección de datos.

Ley 1266 de 2008: **Ley de Habeas Data**. Regula el manejo de la información financiera, crediticia, comercial, de servicios y la información de datos personales en Colombia, asegurando la correcta administración y protección de estos datos.

Ley 1273 de 2009: **Ley de Delitos Informáticos**. Tipifica los delitos relacionados con el uso indebido de las tecnologías de la información y establece sanciones para quienes cometan estos delitos.

Y otras normativas aplicables que se encuentren descritas en la CA-GJ-PR1-F18 MATRIZ DE REQUISITOS LEGALES.

4. Desarrollo

Coguasimales Service S.A.S. reconoce la importancia de la información como un activo para la prestación de sus servicios asociados al alcance del sistema de gestión y la toma de decisiones eficientes, por lo cual la alta dirección genera un compromiso sobre la protección de la información más significativa como parte de una estrategia orientada a la continuidad del negocio, la administración de los riesgos y la consolidación de una cultura de seguridad que permita la mejora continua del sistema, garantizando el cumplimiento de requisitos legales, contractuales y del negocio a través del sistema de gestión de seguridad de la información, con el objetivo de proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de la información que se maneja en la organización.

El propósito de la seguridad de la información es asegurar la continuidad del negocio en la organización y reducir al mínimo el riesgo de daño mediante la prevención de incidentes de seguridad, así como reducir su impacto potencial cuando sea inevitable. Para garantizar la efectividad de esta política se han establecido una serie de objetivos que refuerzan nuestro compromiso con la protección de los activos de información, los cuales son:

- Asegurar que la información crítica para el negocio sea protegida contra accesos no autorizados, alteraciones indebidas y pérdidas, garantizando así su disponibilidad y exactitud en todo momento.
- Desarrollar y mantener una cultura organizacional que valore y promueva prácticas seguras de manejo de la información, mediante la capacitación continua, concientización y la comunicación efectiva de las políticas y procedimientos de seguridad.
- Asegurar que todos los aspectos de la gestión de la seguridad de la información cumplan con las leyes, regulaciones y estándares internacionales aplicables, como la ISO/IEC 27001, para evitar sanciones y mantener la integridad de la empresa frente a auditorías y revisiones externas.

4.1. Principios

Los principios fundamentales de nuestra política de Seguridad de la Información los cuales están alineados con la norma ISO/IEC 27001:2022 son los siguientes:

Confidencialidad: Nos comprometemos a garantizar que la información solo sea accesible a personas autorizadas, protegiendo así los datos sensibles contra accesos no autorizados y divulgaciones indebidas.

Integridad: Nos aseguramos de que la información y los métodos de procesamiento se mantengan exactos y completos. Esto implica proteger la información contra modificaciones no autorizadas y garantizar la precisión de los datos a lo largo de su ciclo de vida.

Disponibilidad: Nos esforzamos por asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran. Esto incluye la implementación de medidas para prevenir interrupciones en el acceso y garantizar la continuidad del negocio.

Al adherirnos a estos principios, buscamos proteger los activos de información de la organización, mitigar riesgos y asegurar la continuidad de nuestras operaciones.

4.2. Responsabilidades y Roles:

Para garantizar la eficacia de nuestra política de seguridad de la información, es fundamental que cada miembro de Coguasimales Service S.A.S entienda y cumpla con sus responsabilidades específicas. A continuación, se detallan los roles clave, con el fin de asegurar una gestión integral y coordinada de la seguridad de la información:

Líder TIC:

- Diseña y ejecuta estrategias tecnológicas que alineen los recursos tecnológicos con los objetivos empresariales y los requisitos de seguridad.
- Administra y mantiene las infraestructuras tecnológicas, incluyendo servidores, redes y sistemas de almacenamiento, asegurando que estén configurados y actualizados de acuerdo con las mejores prácticas de seguridad.
- Evalúa y recomienda tecnologías y soluciones que refuercen la seguridad de la información, realizando análisis de riesgo para la implementación de nuevas herramientas y sistemas.
- Supervisa el rendimiento y la seguridad de los sistemas tecnológicos, implementa medidas para la detección y respuesta ante incidentes de seguridad y gestiona las actividades de soporte técnico relacionadas con la seguridad.

Responsable de Seguridad de la Información:

- Elabora, revisa y actualiza las políticas y procedimientos de seguridad de la información para asegurar su alineación con las normativas internacionales y locales.
- Supervisa las actividades de seguridad, realiza revisiones internas para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y coordina las actividades para remediar las no conformidades.
- Identifica, evalúa y gestiona los riesgos asociados a la seguridad de la información, registrándolos en la “CE-GC-PR3-F1 Matriz de Riesgos” e implementando los controles establecidos para su mitigación.
- Desarrolla e implementa programas de formación y sensibilización sobre seguridad de la información para el personal, promoviendo una cultura de seguridad y asegurando que todos los colaboradores comprendan y cumplan con las políticas de seguridad.

Coordinadores, conciliadores de cuenta, Aliados y Otros:

- Siguen las políticas y procedimientos establecidos para la seguridad de la información, asegurando que todas las prácticas y actividades relacionadas con el manejo de información sean seguras y conformes a las normativas.
- Utilizan los recursos de información de manera adecuada, protegen la confidencialidad, integridad y disponibilidad de los datos, y reportan al área de TIC y/o al coordinador de seguridad de la información cualquier incidente o vulnerabilidad que detecten.
- Participan en las actividades de formación y concienciación sobre seguridad de la información, aplicando el conocimiento adquirido para proteger los activos de información de la organización.

4.3. Gestión de Riesgos

En Coguasimales Service S.A.S la gestión de riesgos es un componente fundamental para garantizar la protección de la información y los sistemas. Para ello, llevamos a cabo una evaluación de los riesgos en la “CE-GC-PR3-F1 Matriz de Riesgos”. Una vez identificados, implementamos medidas de tratamiento de riesgos diseñadas para mitigar los riesgos a un nivel aceptable. Este proceso incluye la implementación de controles con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información crítica de la organización.

4.4 Controles de Seguridad

En nuestro compromiso con la protección de la información, implementamos una serie de controles de seguridad para salvaguardar la integridad, confidencialidad y disponibilidad de nuestros activos.

Esto incluye la aplicación de medidas de control de acceso, garantizando que solo las personas autorizadas, conforme al Lineamiento de Gestión de Identidad, accedan a la información y sistemas pertinentes. Asimismo, nos comprometemos a establecer controles de seguridad física y ambiental para proteger los activos y las instalaciones contra accesos no autorizados, daños o pérdidas. Estos controles son fundamentales para mantener un entorno seguro, fortaleciendo la confianza en nuestros sistemas y datos.

4.5 Educación y Concientización

Todos los empleados deben participar en programas de formación y concienciación sobre seguridad de la información, para asegurar que entiendan sus responsabilidades y los riesgos asociados con la información.

4.6 Cumplimiento y Auditoría

v para evaluar el cumplimiento de esta política y la efectividad de los controles implementados. Los resultados de las auditorías se reportan a la alta dirección y se utilizan para mejorar continuamente el SGSI.

Este enfoque proactivo y de mejora continua garantiza que nuestro SGSI se mantenga robusto y eficaz frente a las amenazas cambiantes del entorno de seguridad de la información.

4.6 Revisión y Mejora Continua

En aras de mantener un nivel óptimo de seguridad de la información, Coguasimales Service S.A.S se compromete a realizar revisiones periódicas de esta política. Estas evaluaciones regulares nos permiten analizar la efectividad de las medidas implementadas y realizar ajustes según sea necesario para abordar nuevas amenazas o vulnerabilidades.

Además, nos comprometemos a implementar un proceso de mejora continua, que se basa en los resultados de estas revisiones y auditorías. Este enfoque nos permite adaptarnos dinámicamente a los cambios en el panorama de seguridad de la información y garantizar que nuestras prácticas de seguridad estén siempre actualizadas y sean efectivas.

La gerencia general aprueba esta política y es responsable de la autorización de sus modificaciones. Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la política de Seguridad de la Información vigente. En caso de ir en contravía de esta política se considerará como una falta grave establecida en el reglamento interno de trabajo y consagrada en el artículo 60 del Código Sustantivo del Trabajo.

Se firma en San José de Cúcuta, el 14 de marzo de 2025.

David Gámez
Líder TIC

Laura Yamile Buendía Ramírez
Gerente