TABLA DE CONTENIDO

1 OBJETIVO

Implementar, mantener y mejorar continuamente la gestión de la Seguridad de la Información en Corredor Empresarial S.A., con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, alineados con la misión, visión, objetivos estratégicos del negocio, disposiciones legales, regulatorias, normativas y contractuales, asegurando que los objetivos de seguridad de la información se encuentren constantemente monitoreados y documentados para garantizar su actualización y pertinencia en relación con la seguridad de la información.

1.1 OBJETIVOS ESPECÍFICOS

- Estandarizar el proceso de seguridad de la información que deben cumplir las diferentes áreas de Corredor Empresarial S.A. (CE), según los requerimientos de cada una de ellas.
- Gestionar los riesgos de seguridad de la información sobre los procesos y sus interacciones, alineados a la política de riesgos de la compañía.
- Gestionar los incidentes de Seguridad de la Información.
- Fomentar en los empleados y terceros de Corredor Empresarial S.A., un nivel apropiado de concienciación, competencia y cultura en Seguridad de la Información.
- Velar por que los procesos y usuarios de los sistemas de información de Corredor Empresarial S.A, cumplan con su responsabilidad y obligaciones indicadas en las políticas, normas, documentos, procedimientos y buenas prácticas de seguridad de la información.
- Cumplir con las obligaciones aplicables y vigentes de tipo legal, regulatorio y contractual relacionadas con la Seguridad de la Información.

2 ALCANCE

Esta política aplica a la Alta Dirección, líderes de procesos, empleados, contratistas, y todas las partes interesadas que acceden a información o a los sistemas que la contengan (hardware, software, bases de datos, aplicaciones, entre otros.) de Corredor Empresarial S.A. para el cumplimiento de los propósitos generales de la compañía.

Esta Política puede compartirse a medida que sea requerida con proveedores, socios externos, e incorporarse a cualquier relación contractual.

3 DEFINICIONES

Con el fin de asegurar la adecuada interpretación y aplicación de los términos utilizados en la presente política, se establece el documento "Terminología Documentación SIGO" como fuente oficial de referencia. Todo término que requiera aclaración deberá ser consultado en dicho documento, el cual es de obligatorio uso para los colaboradores y terceros que se encuentren dentro del alcance de esta política.

4 CONTEXTO

La gestión de la Seguridad de la Información en Corredor Empresarial S.A. es fundamental para el manejo adecuado y protección de la información, de sus clientes y partes interesadas, alineada con su misión, objetivos estratégicos y valores corporativos.

Consciente del valor crítico que representa esta información, la empresa se compromete a implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los requisitos de la norma ISO 27001 vigente, abordando de manera efectiva los procesos y sus interacciones para garantizar niveles adecuados de:

- **Confidencialidad**, garantizando el acceso sólo para los usuarios autorizados.
- **Integridad**, evitando modificaciones no autorizadas.
- **Disponibilidad**, garantizando que la información esté disponible cuando se necesite.

Razón por la cual la información debe ser protegida de acuerdo con su criticidad en cualquier estado mientras se recolecte, almacene, procese o transmita; implementando controles de acuerdo con el impacto que se pueda generar por la divulgación o modificación no autorizada de la misma.

Por lo anterior, se debe implementar, mantener y mejorar el sistema de gestión de Seguridad de la Información en la compañía para proteger la confidencialidad, integridad y disponibilidad de la información propia, de sus partes interesadas y de sus clientes ante una serie de riesgos que atenten contra estos principios.

5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- Todas las políticas de seguridad de la información de Corredor Empresarial S.A. complementan y se alinean con la Política General de Seguridad de la Información, y deben ser interpretadas dentro del marco del Sistema de Gestión de Seguridad de la Información (SGSI). Esta relación asegura la coherencia entre los principios estratégicos establecidos por la alta dirección y los controles técnicos, operativos y organizacionales definidos en cada política específica, promoviendo una gestión integral y armónica de la seguridad de la información en toda la organización.
- Se debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI (Sistema de gestión de seguridad de la información) con base a la norma ISO 27001 vigente, según su requisitos y controles de referencia al ANEXO A.
- Corredor Empresarial S.A. implementa un programa de ciberseguridad basado en mejores prácticas, mejorando continuamente su seguridad y resiliencia y promoviendo una cultura integral de ciberseguridad entre empleados y partes interesadas, asegurando que todos comprendan sus responsabilidades en la protección de la información, salvaguardando la confidencialidad, integridad y disponibilidad de la información.
- Se debe aplicar un sistema documentado para la gestión de los riesgos de seguridad de la información, de acuerdo con los requisitos definidos en la política de riesgos la compañía. Los criterios para la evaluación y aceptación de los riesgos deben ser establecidos, formalizados y aprobados por la alta dirección de Corredor Empresarial S.A.
- Se pondrá en conocimiento de todos los empleados o partes interesadas de Corredor Empresarial S.A., las políticas de seguridad de la información y ciberseguridad, sus responsabilidades y deberes pertinentes al rol desempeñado.
- Se debe verificar que se revisen, actualicen y aprueben las políticas de seguridad de la información y ciberseguridad por parte de la alta dirección de Corredor Empresarial S.A. de manera anual.
- El Área de Seguridad de la Información debe establecer un programa que permita el fomento continuo y de creación de cultura y conciencia de seguridad en los empleados, contratistas, proveedores, personas y usuarios de la información de Corredor Empresarial S.A.
- Todo empleado antes de ingresar a trabajar con Corredor Empresarial S.A., debe contar con un proceso adecuado de selección de personal, para garantizar su idoneidad en el cargo que va a desempeñar.
- El área de Gestión Humana debe incluir en el proceso de selección y contratación de personal, procedimientos de seguridad antes, durante y después de la contratación.

- Todo empleado antes del ingreso a la compañía debe firmar un acuerdo de confidencialidad, el cual debe ser parte integral del contrato.
- Todo tercero debe firmar una cláusula o anexo de seguridad de la información, el cual debe ser parte integral del contrato.
- Los líderes de procesos deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de Corredor Empresarial. S.A.
- La alta dirección de Corredor Empresarial S.A. reconoce que un Gobierno de Seguridad de la Información forma parte de la cultura organizacional de la compañía, por lo cual se comprometen con el cumplimiento de los objetivos y alcance de dicho gobierno, asegurando que los recursos necesarios estén disponibles para ello.
- Corredor Empresarial S.A. llevará a cabo auditorías internas periódicas del Sistema de Gestión de Seguridad de la Información (SGSI), con el objetivo de verificar la conformidad con los requisitos establecidos en la norma ISO/IEC 27001, las políticas internas, y los controles implementados. Las auditorías serán planeadas, ejecutadas y documentadas conforme a un programa anual aprobado por la Alta Dirección. El Director del Sistema Integrado de Gestión será responsable de coordinar este programa de auditorías, asegurando la objetividad e imparcialidad de los auditores designados y garantizando que los resultados se utilicen para mejorar continuamente el SGSI.
- El proceso de compras y los gestores asignados de contratos por parte de Corredor Empresarial S.A., deben velar por la difusión y cumplimiento de las Políticas de Seguridad de la Información corporativas a sus proveedores y contratistas.
- Los empleados de Corredor Empresarial S.A, deben conocer sus roles y responsabilidades en seguridad de la información, asegurando así que entiendan cómo contribuir a la protección de los activos de la empresa y la prevención de incidentes, en conformidad con la norma ISO/IEC 27001 vigente.
- Las directrices de esta política se basan en los resultados del proceso de evaluación de riesgos de seguridad de la información, aplicado según la Metodología de Gestión Integral de Riesgos de Corredor Empresarial S.A. Este enfoque permite priorizar activos y amenazas, y definir controles adecuados que fortalezcan el SGSI bajo un principio de mejora continua
- La Alta Dirección de Corredor Empresarial S.A. realizará revisiones periódicas del Sistema de Gestión de Seguridad de la Información (SGSI), al menos una vez al año, con el fin de asegurar su continua adecuación, eficacia y alineación con los objetivos estratégicos del negocio.

- La organización reconoce el uso creciente de tecnologías emergentes como la Inteligencia Artificial (IA), la analítica avanzada y la automatización. Estas tecnologías pueden generar riesgos adicionales sobre la seguridad de la información. Por lo anterior, Corredor Empresarial S.A. establece que el uso, desarrollo e implementación de sistemas inteligentes o basados en IA, deberá gestionarse bajo principios de seguridad, privacidad, ética y cumplimiento normativo. estos deberán ser gestionados a través del SGSI, considerando su impacto sobre la confidencialidad, integridad y disponibilidad de la información.

6 CUMPLIMIENTO

Cualquier empleado o tercero, que incumpla esta política o las que se requieran para desarrollar el sistema de Seguridad de la Información, debe asumir las responsabilidades y sanciones a que haya lugar definidas o relacionadas con los reglamentos, la normatividad interna de Corredor Empresarial S.A. (**CE**). y la legislación vigente en materia de Seguridad de la Información o Protección de Datos Personales.

7 ÉTICA, SOSTENIBILIDAD Y DIRECTRICES QUE SE CUMPLEN

Todas las directrices de esta política cumplen con las leyes aplicables, las cuales incluyen regulaciones de derechos humanos, ambientales, laborales, de salud y seguridad, en contra de la evasión, corrupción y/o otras emitidas por nuestros stakeholders y COLJUEGOS.
Además de las reglas aplicables a Corredor Empresarial SA para el personal y el Código de Conducta y Ética, esta Política también compromete a todo el personal a respetar la conducta ética, la responsabilidad social, la transparencia, la auditabilidad, la rendición de cuentas y la sólida gestión de riesgos en el contexto de la misma. Las desviaciones de esto deben informarse para tomar las acciones correspondientes.

8 ACTUALIZACIÓN

Este documento será modificado por el Oficial de Seguridad de la Información en la medida que se requiera y permanecerá publicado en la herramienta de gestión documental corporativa.
La revisión de la vigencia de las directrices se realizará mínimo una vez cada año.