POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

El presente documento tiene como finalidad establecer las directrices y lineamientos necesarios para proteger la información y los sistemas de información en los que SERCONTHA S.A.S. («Nosotros», «La Empresa», o «La Compañía») administra, produce, procesa, almacena o transforma datos propios y de sus clientes, ante cualquier amenaza que pueda comprometer la confidencialidad, integridad, disponibilidad y trazabilidad de dicha información.

1.1. OBJETIVOS ESPECÍFICOS

1.1.1. Gestión de activos de información

Orientar a los colaboradores de La Empresa en la identificación, clasificación y manejo de los activos de información que producen, almacenan o custodian, atendiendo los requisitos legales y contractuales aplicables.

1.1.2. Gestión de riesgos de seguridad de la información

Gestionar de forma oportuna los riesgos de seguridad de la información mediante controles proporcionales, reduciendo los impactos negativos en caso de materialización.

1.1.3. Gestión de incidentes de seguridad de la información

Atender y resolver los incidentes de seguridad que afecten la confidencialidad, integridad, disponibilidad o trazabilidad de los activos de información de La Empresa, conservando la evidencia y los registros que permitan su reconstrucción posterior.

1.1.4. Fomento de la cultura y la apropiación

Promover una cultura de seguridad y privacidad de la información entre los colaboradores, contratistas y proveedores, generando conciencia sobre sus deberes y responsabilidades en la protección de los activos de información.

2. ALCANCE

La presente política aplica a todos los procesos, sedes, colaboradores, contratistas, proveedores y aliados estratégicos que accedan o gestionen información de La Empresa y de sus clientes, incluyendo servicios tercerizados, uso de plataformas tecnológicas, trabajo remoto y dispositivos móviles.

En desarrollo de su objeto social, La Empresa administra información contable, tributaria, financiera, laboral y de nómina que pertenece a sus clientes. Respecto de los datos personales contenidos en dicha información, La Empresa actúa en calidad de Encargado del Tratamiento por cuenta de sus clientes, quienes conservan la condición de Responsables del Tratamiento, en los términos previstos en la Política de Tratamiento de Datos Personales de La Empresa. En consecuencia, los activos de información recibidos, generados o custodiados en esa calidad quedan cubiertos por la presente política y por los acuerdos de confidencialidad y las cláusulas de tratamiento de datos pactadas con cada cliente, sin perjuicio de las instrucciones que el Responsable imparta sobre dicha información.

Es responsabilidad de todas las partes involucradas cumplir con los lineamientos aquí establecidos y con los procedimientos específicos que se deriven de esta política.

3. DEFINICIONES

Para efectos del entendimiento y ejecución de la presente política, se tendrán las siguientes definiciones.

a. Activo de Información: Todo dato, documento, registro, base de datos, sistema, aplicación, equipo, medio de almacenamiento o conocimiento que tenga valor para La Empresa o para sus clientes y que, por lo tanto, requiere protección.

b. Confidencialidad: Propiedad según la cual la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

c. Integridad: Propiedad de exactitud y completitud de la información, de manera que esta no sea alterada o destruida de forma no autorizada.

d. Disponibilidad: Propiedad de la información de ser accesible y utilizable, cuando se requiera, por parte de quien está autorizado para ello.

e. Trazabilidad: Propiedad que permite registrar, conservar y reconstruir quién accedió, creó, modificó, transmitió o eliminó información, en qué momento y desde qué medio, de modo que las actuaciones puedan atribuirse de manera inequívoca.

f. Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de políticas, procedimientos, roles, controles y recursos que La Empresa establece, implementa, mantiene y mejora continuamente para preservar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

g. Control de Seguridad: Medida de carácter organizacional, técnico, físico o legal que modifica o mitiga un riesgo de seguridad de la información.

h. Riesgo de Seguridad de la Información: Posibilidad de que una amenaza aproveche una vulnerabilidad de un activo de información y cause un impacto adverso a La Empresa, a sus clientes o a los titulares de los datos.

i. Incidente de Seguridad de la Información: Evento o serie de eventos, únicos o inesperados, que tienen una probabilidad significativa de comprometer la confidencialidad, integridad, disponibilidad o trazabilidad de la información, incluyendo el acceso, uso, pérdida, alteración, consulta o divulgación no autorizada o fraudulenta de datos.

j. Colaborador: Toda persona natural vinculada laboralmente con La Empresa, así como los aprendices y practicantes que desempeñen funciones en ella.

k. Contratista o Proveedor: Persona natural o jurídica que tiene un vínculo contractual, de naturaleza civil o comercial, con La Empresa, ya sea para prestar o suministrar un servicio, o para hacer entrega de productos.

l. Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

m. Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

4. POLÍTICA

La Empresa se compromete a establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja la confidencialidad, integridad, disponibilidad y trazabilidad de

la información, mediante controles organizacionales y de gobierno, técnicos y tecnológicos, físicos y ambientales, y legales y contractuales, asegurando un enfoque de cultura y apropiación en la gestión de activos, la identificación de riesgos y la atención de incidentes, en cumplimiento con los requisitos legales, regulatorios y contractuales aplicables.

La Gerencia de La Empresa respalda esta política y proveerá los recursos necesarios para su implementación y mejora continua.

4.1. ESTRUCTURA

La Política de Seguridad de la Información de La Empresa está alineada con los requisitos de la norma ISO/IEC 27001:2022 y las mejores prácticas del mercado. Este documento establece el «QUÉ» debe protegerse y los dominios de control principales. Los procedimientos específicos desarrollarán el «CÓMO» se implementan los controles en cada área.

4.2. DECLARACIONES GENERALES DE GESTIÓN

La Empresa:

a) Asume la responsabilidad formal sobre el SGSI, en coherencia con su compromiso con la excelencia y la confianza de sus clientes.

b) Designa al Representante Legal o a quien este delegue como responsable de la supervisión del SGSI, con facultades para reportar directamente a la alta dirección.

c) Realiza evaluaciones sobre la eficacia de los controles establecidos, internas o externas, con una frecuencia mínima de una (1) vez al año, y de manera extraordinaria cuando se materialice un incidente de alto impacto o se produzcan cambios significativos en la operación, la tecnología o la normatividad aplicable.

d) Se compromete con la mejora continua, gestionando los resultados de auditorías, riesgos, vulnerabilidades y cambios normativos o tecnológicos.

e) Implementa programas de sensibilización y capacitación en seguridad de la información para todo el personal, con una frecuencia mínima de una (1) vez al año, y como parte del proceso de inducción de todo nuevo colaborador o contratista.

f) Incluye cláusulas de confidencialidad y de seguridad de la información en los contratos con colaboradores, proveedores y aliados estratégicos.

g) Administra de manera centralizada las herramientas tecnológicas, el control de accesos y la seguridad en entornos de nube, trabajo remoto y dispositivos móviles.

4.3. ENFOQUE DE CONTROLES DE SEGURIDAD

Para garantizar la protección de la información, La Empresa implementa y mantiene un conjunto de controles de seguridad, los cuales se seleccionan y priorizan con base en el análisis de riesgos, los recursos tecnológicos disponibles, el tamaño de la operación y los requisitos contractuales exigidos por sus clientes.

Estos controles se agrupan en las siguientes categorías generales, sin perjuicio de que puedan documentarse controles adicionales en procedimientos internos específicos cuando el negocio lo requiera:

a) Controles organizacionales y de gobierno: Incluyen la definición de roles y responsabilidades en seguridad, la gestión de riesgos, los planes de capacitación y concientización para el personal, la gestión de incidentes y la continuidad de la operación ante eventos disruptivos.

b) Controles técnicos y tecnológicos: Abarcan las medidas aplicadas sobre la infraestructura de TI, como la gestión de accesos a sistemas y datos, el registro y conservación de trazas de auditoría, la protección contra software malicioso, el cifrado de información sensible, las copias de seguridad (backups), la seguridad en las comunicaciones, redes y correo electrónico, y el uso seguro de dispositivos móviles y trabajo remoto.

c) Controles físicos y ambientales: Comprenden la protección de las instalaciones físicas, el acceso restringido a áreas donde se procesa o almacena información crítica, y la disposición segura de equipos y documentos físicos que contengan datos sensibles.

d) Controles legales y contractuales: Garantizan el cumplimiento de la normatividad colombiana aplicable, especialmente la Ley 1581 de 2012 de protección de datos personales y sus decretos reglamentarios, la Ley 1273 de 2009 de delitos informáticos y la Ley 43 de 1990 en materia de reserva profesional, así como la inclusión de cláusulas de confidencialidad y seguridad en los contratos con clientes, proveedores y aliados estratégicos.

La documentación detallada de cada control específico, es decir el «CÓMO» se ejecutan, será desarrollada progresivamente en manuales, guías o procedimientos operativos internos, los cuales serán actualizados de acuerdo con la evolución de los riesgos, la tecnología y las necesidades del negocio. La ausencia de un control específico en esta política no exime a La Empresa de implementarlo si así lo determina una evaluación de riesgos posterior.

4.4. CONFIDENCIALIDAD Y RESERVA PROFESIONAL

La información contable, tributaria, financiera, laboral y de nómina que La Empresa conoce en razón de los servicios que presta está amparada por la reserva profesional que rige el ejercicio de la Contaduría Pública, conforme a la Ley 43 de 1990 y al Código de Ética profesional aplicable, sin perjuicio de la reserva legal que protege los libros y papeles del comerciante y de las obligaciones derivadas de la normatividad de protección de datos personales.

En consecuencia, los colaboradores, contratistas y proveedores de La Empresa deben abstenerse de divulgar, reproducir, comercializar o utilizar en provecho propio o de terceros la información de los clientes a la que accedan con ocasión de sus funciones, y solo podrán tratarla en la medida estrictamente necesaria para prestar el servicio contratado. La entrega de información a terceros procederá únicamente por autorización expresa del cliente o por requerimiento de autoridad competente formulado conforme a la ley, caso en el cual se atenderá con la debida diligencia y se dejará constancia documental de la entrega.

Todo colaborador, contratista y proveedor suscribirá un acuerdo de confidencialidad como condición previa al acceso a la información. El deber de reserva es indefinido y subsiste después de la terminación del vínculo laboral o contractual, por el tiempo en que la información conserve su carácter reservado.

5. CUMPLIMIENTO E INCUMPLIMIENTO

5.1. CUMPLIMIENTO

Los procedimientos, manuales y lineamientos derivados de esta política serán almacenados y actualizados en repositorios accesibles para las partes interesadas. La Empresa realizará revisiones para verificar la eficacia de los controles con una frecuencia mínima de una (1) vez al año, cuyos resultados serán presentados a la alta dirección y servirán de insumo para el plan de mejora del SGSI.

5.2. INCUMPLIMIENTO

El incumplimiento de cualquiera de las disposiciones de esta política o de los documentos que de ella se deriven podrá constituir una falta disciplinaria. La calificación de su gravedad y la sanción aplicable se determinarán conforme a las faltas y sanciones expresamente tipificadas en el Reglamento Interno de Trabajo de La Empresa y previo el agotamiento del procedimiento disciplinario allí previsto, garantizando en todo caso el derecho de defensa y contradicción del colaborador.

Lo anterior se entiende sin perjuicio de los siguientes regímenes de responsabilidad, que son independientes entre sí y que no son aplicados por La Empresa:

a) Responsabilidad penal: Las conductas que puedan configurar alguno de los delitos previstos en la Ley 1273 de 2009 u otras normas penales serán puestas en conocimiento de las autoridades competentes, a quienes corresponde su investigación y sanción.

b) Responsabilidad administrativa: La inobservancia del régimen de protección de datos personales puede dar lugar a las sanciones que la Superintendencia de Industria y Comercio imponga a La Empresa en su condición de Responsable o Encargado del Tratamiento, conforme a la Ley 1581 de 2012.

c) Responsabilidad civil: La reparación de los perjuicios que el incumplimiento cause a La Empresa, a sus clientes o a terceros se regirá por las normas generales de responsabilidad y por lo pactado contractualmente.

Los contratistas y proveedores que incumplan estarán sujetos a las consecuencias previstas en las cláusulas contractuales correspondientes, incluida la terminación del contrato cuando así se haya pactado.

5.3. EXCEPCIONES

Cualquier excepción a esta política deberá tramitarse por escrito ante el responsable de la supervisión del SGSI, indicando la disposición que se pretende exceptuar, la justificación de negocio, el análisis del riesgo asociado y los controles compensatorios propuestos. Su aprobación corresponde a la alta dirección de La Empresa.

Toda excepción aprobada se inscribirá en el Registro de Excepciones del SGSI, en el que se dejará constancia de su objeto, el solicitante, el responsable de los controles compensatorios, la fecha de aprobación y la fecha de vencimiento.

Las excepciones tendrán una vigencia máxima de doce (12) meses. Vencido este plazo quedarán sin efecto de pleno derecho, salvo que se renueven mediante una nueva evaluación de riesgo y una nueva aprobación. El Registro de Excepciones será revisado al menos cada seis (6) meses con el fin de verificar la vigencia de las excepciones otorgadas y la operación efectiva de los controles compensatorios.

6. INFORMACIÓN DE CONTACTO

Para consultas o reporte de incidentes relacionados con la seguridad de la información, los colaboradores, clientes y proveedores pueden comunicarse a través de los siguientes canales:

SERCONTHA S.A.S.

Calle 26 A # 13 – 97, Oficina 1702, Bogotá D.C.

Correo electrónico: administrativo@sercontha.com

Teléfonos: (601) 718 0825 – 312 491 0505 – 320 848 6218

Dada en Bogotá D.C., el treinta y uno (31) de agosto de 2026.