TABLA DE CONTENIDO

1. ANTECEDENTES

Confecámaras establece relaciones contractuales con terceros que prestan servicios tecnológicos, incluyendo desarrollo, mantenimiento, soporte y operación de sistemas de información, así como con proveedores de servicios en la nube.

Dichas relaciones son consideradas críticas dentro del Sistema de Gestión de Seguridad de la Información (SGSI), ya que los proveedores pueden tener acceso a activos de información sensibles o participar en procesos clave de la organización.

2. PROPÓSITO

Establecer los principios, directrices y controles necesarios para gestionar de forma segura las relaciones con proveedores que puedan acceder, procesar, almacenar o administrar activos de información de Confecámaras, o que provean servicios relevantes dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los requerimientos establecidos en la norma ISO/IEC 27001 y sus controles asociados.

3. ALCANCE

Esta política aplica a todos los colaboradores, contratistas y terceros autorizados que interactúan con la Confederación Colombiana de Cámaras de Comercio - Confecámaras, en el marco de la gestión de relaciones con proveedores.

Su aplicación se extiende a todos los procesos relacionados con la selección, contratación, evaluación, monitoreo y finalización de relaciones con proveedores que puedan afectar la seguridad de la información, conforme al alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

4. DEFINICIONES

. ACTIVO DE INFORMACIÓN: Cualquier pieza de información, sea esta en cualquier medio magnético, impreso o que sea transmitida electrónica, visual u oralmente y que tenga valor para la organización.

. ACUERDO DE CONFIDENCIALIDAD: Documento contractual mediante el cual una o ambas partes se comprometen a proteger y no divulgar información sensible o confidencial a la que tengan acceso durante la relación comercial o contractual, asegurando su uso exclusivo para los fines establecidos y previniendo accesos no autorizados, conforme a los requisitos legales, normativos y de seguridad de la organización.

. PROVEEDOR: Terceros que suministran bienes o servicios a una organización, incluyendo aquellos que ofrecen servicios especializados de ciberseguridad para proteger los activos de información frente a amenazas y riesgos.

. RIESGO: Efecto de la incertidumbre sobre los objetivos.

. TRANSFERENCIA DE INFORMACIÓN: Proceso mediante el cual la información es enviada, recibida o compartida entre personas, áreas, sistemas o terceros, utilizando medios electrónicos o físicos. Debe realizarse cumpliendo controles que aseguren la confidencialidad, integridad y disponibilidad de la información transferida, conforme a su clasificación y a las políticas organizacionales.

5. DIRECTRICES

5.1. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
LÍDERES Y DIRECTORES	• Identificar y documentar todos los proveedores en la matriz de proveedores • Gestionar los riesgos de seguridad de la información asociados a proveedores en el marco de sus procesos. • Participar en el proceso de evaluación de proveedores.
SEGURIDAD DE LA INFORMACIÓN	• Velar por el cumplimiento de esta política. • Liderar la gestión de riesgos de seguridad de la información relacionados con proveedores. • Definir los procedimientos para la gestión de cambios de proveedores. • Evaluar a los proveedores conforme el formato establecido. • Realizar el acompañamiento a las demás áreas en la reevaluación de proveedores. • Incluir en los programas de capacitación a colaboradores temas relacionados con la seguridad de la información en las relaciones con proveedores.
PROVEEDORES	• Cumplir con los requerimientos de seguridad de la información establecidos por Confecámaras • Firmar acuerdos de confidencialidad y no divulgación, con el objetivo de proteger la información a la que tengan acceso durante la prestación de servicios. • Notificar de manera inmediata cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad o disponibilidad de la información o los servicios bajo su responsabilidad. • Aceptar la realización de auditorías, revisiones o evaluaciones de cumplimiento, conforme a lo establecido contractualmente o según lo determine Confecámaras para verificar el cumplimiento de los controles de seguridad.

5.2. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

La Vicepresidencia de Tecnología establece la siguiente política para la gestión de la seguridad de la información en su relación con proveedores:

.Se deben identificar y gestionar los riesgos de seguridad de la información relacionados con el uso de productos y servicios proporcionados por terceros. Esto incluye:

. El uso de servicios en la nube.
. Posibles fallos, mal funcionamiento o vulnerabilidades en productos o servicios, incluyendo componentes y subcomponentes de software.

. Todos los proveedores deben ser identificados y registrados en la matriz de proveedores administrada por el área de Tecnología de la Información (TI).

. La evaluación de proveedores se llevará a cabo conforme al formato de reevaluación de proveedores, establecida por el área de Contratación y Compras.

. Todo proveedor o tercero con acceso a información de la organización deberá firmar un acuerdo de confidencialidad y no divulgación que garantice la protección de los activos de información.

. Se deben formalizar acuerdos contractuales con proveedores donde se especifiquen:

. Los servicios TIC, infraestructura y datos a los que pueden acceder, controlar o monitorear.
. Las medidas para el tratamiento de incidentes, fallos, incumplimientos y contingencias.
. Las obligaciones tanto del proveedor como de la organización.

. Los proveedores de servicios en la nube deben garantizar, mediante cláusulas contractuales, la eliminación total y segura de los datos una vez finalice la relación comercial o según el período de retención establecido en el contrato.

. Los acuerdos deberán contemplar medidas de recuperación y contingencia que garanticen la disponibilidad de la información crítica, tanto del proveedor como de la organización.

. El personal de la organización que interactúe con proveedores debe recibir capacitación y concienciación sobre:

. Esta política
. Procedimientos para la gestión de accesos del proveedor
. Uso aceptable de la información y sistemas compartidos.

. La transferencia de información hacia y desde proveedores se realizará de acuerdo con lo establecido en la Política de Transferencia de Información del SGSI.

. Se debe realizar el monitoreo, revisión y evaluación de los cambios en las prácticas de Seguridad de la información del proveedor conforme lo establecido en el manual de contratación.

6. CONSECUENCIAS DEL NO CUMPLIMIENTO

En caso de alguna inquietud, duda o requerimientos se debe contactar al Oficial de Seguridad de la Información de Confecámaras. Este considerará el requerimiento, y según su concepto de ser necesario lo escalará al Comité en Seguridad de la Información. En caso de no cumplimiento de la misma, se presentará el caso al jefe de área respectivo para la definición de sanciones o penalidades según lo estipulado en el reglamento de trabajo.

7. CONTROLES APLICABLES

ISO 27001:2022:

A.5.19 Seguridad de la información en las relaciones con proveedores

A.5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores

8. CONTROL DEL DOCUMENTO

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	19/Jul/2019	Creación de la política de relaciones con los proveedores.
2	16/Jul/2025	Se revisa y actualiza de manera general y se alinea a los controles relacionados de la ISO 27001:2022

ELABORÓ	REVISÓ	APROBÓ
Nombre: Pedro Alejandro Garnica Rueda **Cargo:** Oficial de Seguridad de la Información **Fecha:** 16/Jul/2025	**Nombre:** Pedro Johanni Duarte Cruz **Cargo:** Especialista de Seguridad Informática **Fecha:** 18/Jul/2025	**Nombre:** Jorge Hernán Vargas Orozco **Cargo:** Vicepresidente de TI **Fecha:** 18/Jul/2025