POLÍTICA DE RELACIÓN CON PROVEEDORES.

Versión 3 – Fecha 08 de octubre de 2026

1. ANTECEDENTES

La Confederación Colombiana de Cámaras de Comercio - Confecámaras (en adelante la Confederación, o la Entidad) establece relaciones contractuales con terceros que prestan diferentes servicios y que puedan acceder, procesar, almacenar o administrar activos de información de Confecámaras.
Algunas relaciones con proveedores pueden ser consideradas críticas dentro del Sistema de Gestión de Seguridad de la Información (SGSI), según el nivel de acceso a la información y el impacto en procesos clave de la Entidad. Adicionalmente, los proveedores cuentan con sus propios equipos de cómputo para la prestación del servicio, lo que requiere establecer lineamientos específicos de seguridad aplicables a sus dispositivos.

2. PROPÓSITO

Establecer 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, 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 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, así como al uso de equipos de cómputo de propiedad de terceros para la prestación del servicio, 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 Entidad.

. 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 contractual, asegurando su uso exclusivo para los fines establecidos y previniendo accesos no autorizados, conforme a los requisitos legales y de seguridad de la Entidad.

. DISPOSITIVO DE PUNTO FINAL DE USUARIO: Equipos físicos o virtuales utilizados por proveedores, contratistas o terceros para acceder, procesar, almacenar o transmitir información de la organización o conectarse a sus sistemas, aplicaciones, redes o servicios tecnológicos. Incluyen, entre otros, computadores de escritorio, computadores portátiles, dispositivos móviles (teléfonos inteligentes y tabletas), servidores, estaciones de trabajo, equipos virtuales, dispositivos IoT y cualquier otro equipo con capacidad de conexión a la infraestructura tecnológica de la organización.

. EQUIPO DE CÓMPUTO DE PROPIEDAD DEL TERCERO: Dispositivo informático (computador portátil, computador de escritorio, dispositivo móvil o tableta) cuya propiedad pertenece al proveedor o tercero, no a Confecámaras, y que es utilizado por este para acceder, procesar, almacenar o transmitir información de la Confederación durante la prestación del servicio contratado por Confecámaras.

. MECANISMOS DE SEPARACIÓN DE INFORMACIÓN CORPORATIVA: Conjunto de controles técnicos definidos por Confecámaras, tales como perfiles de navegador de trabajo, políticas de protección de aplicaciones (MAM), control de sesión en aplicaciones en la nube, escritorios virtuales o cuentas de invitado con permisos restringidos orientados a separar y proteger la información de la Confederación cuando esta es accedida desde equipos de cómputo de propiedad del tercero.

. PROVEEDOR O CONTRATISTA: Tercero que suministra bienes o servicios a Confecámaras, 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
VICEPRESIDENTES, GERENTES, DIRECTORES Y JEFES	• Identificar y gestionar los proveedores bajo su responsabilidad. • Solicitar, justificar y aprobar los accesos requeridos por los terceros para la prestación de los servicios. • Gestionar los riesgos de seguridad de la información asociados a los proveedores que apoyan sus procesos. • Garantizar que los proveedores a su cargo cumplan los lineamientos establecidos en la presente Política. • Informar oportunamente la finalización de contratos, servicios o cambios de personal de los proveedores para la actualización o revocación de accesos.
SEGURIDAD DE LA INFORMACIÓN	• Velar por el cumplimiento de la presente Política. • Definir y mantener los lineamientos de seguridad aplicables a terceros y proveedores. • Participar en la evaluación y reevaluación de proveedores en los aspectos relacionados con seguridad de la información. • Asesorar a las áreas responsables en la gestión de riesgos de seguridad de la información asociados a proveedores. • Realizar seguimiento al cumplimiento de los controles de seguridad definidos para terceros. • Verificar el cumplimiento de los lineamientos de seguridad aplicables a los equipos utilizados por proveedores para la prestación de servicios. • Gestionar el seguimiento de los incidentes de seguridad reportados por terceros. • Incluir en los programas de concienciación los lineamientos relacionados con la gestión segura de proveedores.
GERENCIA LEGAL	• Elaborar y formalizar los contratos y acuerdos con proveedores. • Incluir las cláusulas de confidencialidad, propiedad intelectual, transferencia de información y demás requisitos legales y de seguridad definidos por Confecámaras. • Gestionar la selección, evaluación y reevaluación de proveedores conforme al Manual de Contratación. • Coordinar el seguimiento al cumplimiento de los requisitos establecidos para los proveedores. • Mantener los registros asociados al proceso de gestión de proveedores.
PROVEEDORES Y CONTRATISTAS	• Cumplir los requisitos de seguridad de la información definidos por Confecámaras y los establecidos contractualmente. • Garantizar que su personal cumpla las obligaciones de seguridad aplicables durante la prestación del servicio. • Reportar oportunamente incidentes de seguridad que puedan afectar los activos de información de Confecámaras. • Permitir las actividades de seguimiento y verificación de cumplimiento realizadas por Confecámaras.

5.2 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

5.2.1 Obligaciones de Confecámaras frente a la relación con proveedores

Los siguientes son lineamientos generales para la gestión de la seguridad de la información en su relación con los proveedores:

. Identificar y gestionar los riesgos de seguridad de la información relacionados con el uso de productos y servicios proporcionados por terceros, incluyendo el uso de servicios en la nube y posibles fallos, mal funcionamiento o vulnerabilidades en productos o servicios, incluidos sus componentes y subcomponentes de software.

. La evaluación de proveedores se llevará a cabo conforme al formato de reevaluación de proveedores, en el cual se incluye la evaluación de seguridad de la información del proveedor.

. El personal de la Entidad que interactúe con proveedores debe recibir capacitación y concienciación sobre las medidas de seguridad de la información que la Confederación adopta para la gestión de proveedores y terceros, las cuales son de obligatorio cumplimiento.

. Cuando la prestación del servicio requiera la transferencia de información de Confecámaras hacia un tercero, dicha transferencia deberá estar previamente autorizada y formalizada mediante acuerdos, contratos o cláusulas que definan el alcance de la información compartida, la finalidad de su uso, las medidas de protección aplicables y las responsabilidades de las partes, en los términos de la Política de Tratamiento y Protección de Datos Personales de Confecámaras.

. El área de Seguridad de la Información realizará el monitoreo, revisión y evaluación anual de los cambios en las prácticas de seguridad de la información del proveedor, conforme a lo establecido en el manual de contratación.

5.2.2 Obligaciones de los proveedores

. Los terceros que participen en proyectos de desarrollo de software deberán suscribir, a través de su representante legal, los acuerdos de confidencialidad (NDA)

y las cláusulas de propiedad intelectual exigidas por Confecámaras para cada proyecto. Adicionalmente, la empresa contratista será responsable de garantizar que sus empleados, contratistas y demás personas asignadas al proyecto se encuentren vinculados mediante acuerdos de confidencialidad y disposiciones de propiedad intelectual que protejan adecuadamente la información, los desarrollos y los derechos de Confecámaras.

. Cuando el proveedor sustituya al personal asignado para la prestación del servicio a Confecámaras, deberá informarlo previamente a la Entidad para proceder con la revocación de accesos del recurso saliente y la habilitación del nuevo recurso.

. El tercero deberá notificar a Confecámaras, de manera inmediata o dentro de los tiempos establecidos contractualmente, cualquier incidente de seguridad de la información que afecte o pueda afectar la confidencialidad, integridad o disponibilidad de los activos de información de la organización, incluyendo accesos no autorizados, pérdida de información, compromiso de credenciales, infecciones de software malicioso, fuga de información o afectación de los servicios prestados. Cuando el incidente involucre datos personales, deberá activarse adicionalmente el procedimiento interno aplicable para la gestión de incidentes de seguridad que involucren datos personales.

5.3 LINEAMIENTOS DE CONTROL DE ACCESO PARA TERCEROS

Todo acceso a los activos de información de Confecámaras por parte de terceros deberá cumplir los siguientes lineamientos:

. Los accesos deberán ser solicitados por el director, líder o responsable del servicio, contrato o proyecto de Confecámaras, mediante los mecanismos oficiales definidos para la gestión de solicitudes de acceso.
. La creación, modificación y eliminación de accesos deberá gestionarse a través de la herramienta corporativa de gestión de tickets o del procedimiento establecido por la organización.

. Los terceros deberán utilizar cuentas corporativas asignadas por su organización para el acceso a los activos de información de Confecámaras. No se permitirá el uso de cuentas personales.
. Se prohíbe el uso de credenciales compartidas. Todo acceso deberá estar asociado

a un usuario individual e identificable.

. Los accesos deberán otorgarse bajo el principio de mínimo privilegio y limitarse exclusivamente a los recursos requeridos para la prestación del servicio.

. Los desarrolladores de terceros tendrán acceso únicamente a los repositorios, ambientes, aplicaciones y componentes estrictamente necesarios para la ejecución de sus actividades. Siempre que sea técnica y operacionalmente viable, Confecámaras implementará mecanismos que restrinjan la descarga o almacenamiento local del código fuente y de la información de la organización en los dispositivos del tercero. Asimismo, podrán establecerse controles de monitoreo y prevención de fuga de información (DLP) u otras medidas de seguridad equivalentes para proteger los activos de información durante la prestación del servicio.

. Se prohíbe el acceso directo a ambientes de producción, salvo autorización expresa del responsable del activo de información y conforme a los procedimientos establecidos por Confecámaras.

. Los accesos deberán ser eliminados o ajustados cuando finalice la relación contractual, el proyecto, el servicio o cuando ya no exista una necesidad de negocio que los justifique.

. Los terceros deberán cumplir los requisitos adicionales de control de acceso definidos en la Política de Control de Acceso, el Procedimiento de Gestión de Accesos y demás lineamientos de seguridad aplicables al activo de información correspondiente.

. Confecámaras podrá revisar periódicamente los accesos asignados a terceros y solicitar los ajustes o revocaciones que considere necesarios para la gestión del riesgo de seguridad de la información.

5.4 LINEAMIENTOS DE SEGURIDAD PARA EQUIPOS DE CÓMPUTO DE PROPIEDAD DEL TERCERO

Todo tercero o proveedor que acceda, procese o almacene información de Confecámaras deberá garantizar que los dispositivos utilizados para la prestación del servicio cumplan como mínimo con los siguientes lineamientos:

. Los equipos utilizados para la prestación del servicio deberán estar formalmente asignados al colaborador o contratista del tercero y el equipo deberá estar registrado en el inventario de activos de la organización.

. Los dispositivos deberán contar con una solución de protección antimalware o EDR con licencia vigente, instalada, activa y actualizada.

. Los dispositivos deberán mantener sistemas operativos y aplicaciones soportados por el fabricante y con las actualizaciones de seguridad aplicables instaladas.

. Los dispositivos deberán contar con mecanismos de control de acceso activos y bloqueo automático de pantalla, conforme a la política de control de acceso definida por el tercero.

. La información de Confecámaras no deberá almacenarse localmente en los dispositivos del tercero, salvo que sea estrictamente necesario para la prestación del servicio.

. Cuando, por requerimientos de la relación contractual, sea necesario almacenar información de Confecámaras en el dispositivo, este deberá contar con mecanismos de cifrados activos que protejan la información almacenada.

. El tercero deberá contar con lineamientos o políticas vigentes para la protección de los dispositivos de punto final utilizados en la prestación del servicio, incluyendo restricciones sobre la instalación y uso de software no autorizado.

. Cuando un tercero opere mediante dispositivos personales, deberá disponer de una política BYOD vigente y verificable por parte de Confecámaras dentro de las actividades de seguimiento y monitoreo del proveedor.

. Cuando sea requerido por Confecámaras y acordado con el tercero, los dispositivos utilizados para la prestación del servicio deberán permitir la implementación de controles tecnológicos orientados al monitoreo de seguridad, trazabilidad de actividades y prevención de fuga de información (DLP), de acuerdo con la clasificación de la información y el nivel de riesgo asociado al servicio prestado.

. Confecámaras se reserva el derecho de verificar el cumplimiento de los presentes

lineamientos sobre los equipos del tercero asignados a la prestación de su servicio, mediante revisiones técnicas, requerimientos documentales o evaluaciones de cumplimiento, conforme a lo establecido contractualmente.

. Al finalizar la relación contractual, el servicio o la autorización de acceso, el proveedor deberá eliminar de manera segura la información de Confecámaras que se encuentre almacenada en sus equipos, salvo que exista un deber legal o contractual de conservación, y suministrar evidencia de dicha eliminación cuando le sea requerida.

6. CONSECUENCIAS DEL NO CUMPLIMIENTO

En caso de alguna inquietud, duda o requerimiento 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 de Seguridad de la Información.

El incumplimiento de la presente Política será gestionado de acuerdo con la naturaleza de la relación con Confecámaras. Para los colaboradores se aplicarán las disposiciones laborales y reglamentarias correspondientes y, para los proveedores y contratistas, las medidas y consecuencias previstas en el respectivo contrato o instrumento jurídico.