ARTICULO 1º. INTRODUCCIÓN:

La Cámara de Comercio de San José reconoce que la información constituye uno de sus activos más valiosos, pues soporta la toma de decisiones, respalda el cumplimiento de las funciones registrales, administrativas y de apoyo, y garantiza la confianza de empresarios, usuarios, entidades públicas y demás grupos de interés.

En un entorno dinámico y altamente digitalizado, la información se ve expuesta a riesgos derivados de factores internos y externos, tales como incidentes tecnológicos, accesos no autorizados, ciberataques, errores humanos, desastres naturales o fallas operativas, los cuales pueden comprometer la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos institucionales.

En este marco, la presente Política de Seguridad de la Información establece los principios, lineamientos y responsabilidades que orientan la protección de la información bajo un enfoque preventivo y de mejora continua, y el marco normativo nacional aplicable.

De igual manera, busca asegurar la continuidad operativa, fortalecer la cultura de seguridad en todos los niveles de la organización y garantizar el cumplimiento de los requerimientos legales, regulatorios y contractuales, promoviendo la transparencia y la confianza de los diferentes actores que interactúan con la Cámara.

La Cámara de Comercio de San José se compromete, en el desarrollo de sus actividades, a controlar todos aquellos riesgos que puedan afectar el cumplimiento de los objetivos institucionales y misionales, adoptando mecanismos y acciones para gestionar los riesgos relacionados con la seguridad de la información, los cuales permitan identificar, valorar, evidenciar y administrar los riesgos propios de cada proceso; siendo responsabilidad de los directivos y funcionarios dueños de procesos definir y aplicar los controles necesarios para mitigar su materialización y garantizar la adecuada protección de la información.

En consecuencia, esta política constituye un instrumento estratégico y transversal que orienta las acciones institucionales en materia de seguridad de la información, asegurando que los riesgos asociados sean gestionados de manera oportuna, eficiente y responsable.

ARTICULO 2º. OBJETIVOS:

Establecer los lineamientos y controles necesarios para proteger la confidencialidad, integridad y disponibilidad de la información institucional, garantizando su uso adecuado, la continuidad operativa, el cumplimiento de la normatividad vigente y la prevención de riesgos relacionados con el acceso no autorizado, la pérdida, alteración o divulgación indebida de la información.

Esta política busca:

- Prevenir incidentes de seguridad y minimizar sus impactos.
- Cumplir con la normatividad nacional e internacional aplicable.
- Fortalecer la cultura institucional en materia de ciberseguridad.
- Asegurar la continuidad de las operaciones ante eventos que comprometan la información.
- Establecer roles claros de responsabilidad y buenas prácticas en el tratamiento de la información.

ARTICULO 3°. ALCANCE:

Aplica a todos los procesos, personas, sistemas, equipos y servicios que gestionen, almacenen o procesen información institucional, incluyendo entornos físicos, digitales, servicios en la nube y sistemas biométricos.

ARTICULO 4°. INCORPORACIÓN DE NUEVAS TECNOLOGÍAS:

En concordancia con la disponibilidad de recursos y el avance tecnológico, la Cámara de Comercio de San José incorporará progresivamente herramientas y soluciones tecnológicas que permitan la gestión digital de documentos, facilitando su acceso, garantizando su seguridad, confidencialidad e integridad, y optimizando la eficiencia operativa de los procesos institucionales.

La implementación de estas herramientas deberá cumplir con los lineamientos establecidos en esta Política de Seguridad de la Información, así como con la normatividad colombiana vigente en materia de protección de datos y gestión documental.

ARTICULO 5°. MARCO NORMATIVO:

La Cámara de Comercio de San José adopta los siguientes conceptos como base para su política:

- **Circular Externa 100-000002 del 25 de abril de 2022:** Superintendencia de Sociedades: Lineamientos para implementar el programa de gestión de riesgos de ciberseguridad y protección de datos personales.
- **Ley 1581 de 2012:** Protección de datos personales.
- **Decreto 1377 de 2013:** Regulación de la Ley 1581.
- **Ley 1273 de 2009:** Delitos informáticos.
- **Ley 1712 de 2014** – Transparencia y Derecho de Acceso a la Información Pública Nacional.
- **ISO/IEC 27001:2022:** Sistema de Gestión de Seguridad de la Información.
- **ISO/IEC 27005:2022:** Gestión de riesgos de seguridad de la información, entre otras normas específicas aplicables al sector.

ARTICULO 6°. FORMULACIÓN DE LA POLÍTICA:

La formulación de esta política fue liderada por el Área de Tecnología – como dependencia responsable de la seguridad de la información institucional. Su elaboración se basó en el marco

legal colombiano, estándares internacionales de ciberseguridad y el análisis de las necesidades propias de la Cámara de Comercio de San José.

Esta política fue revisada por el Comité de Calidad, aprobada por el Comité de Seguridad de la Información, y posteriormente ratificada por la Junta Directiva, según lo establecido en los estatutos de la entidad, garantizando su adopción formal, aplicación efectiva y socialización institucional.

ARTICULO 7º. FUNDAMENTOS:

La Cámara de Comercio de San José fundamenta su Política de Seguridad de la Información en las siguientes premisas:

- **Proteger los activos de información institucional** frente a amenazas internas o externas, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- **Cumplir con el marco normativo colombiano** e internacional en materia de protección de datos, ciberseguridad y gestión del riesgo de la información.
- **Fortalecer la cultura organizacional en torno a la seguridad digital**, promoviendo la corresponsabilidad y el uso ético y seguro de los recursos tecnológicos.
- **Establecer controles técnicos, administrativos y legales** para la prevención, detección, respuesta y recuperación ante incidentes de seguridad de la información.
- **Fomentar la formación, sensibilización y capacitación** continua del talento humano sobre buenas prácticas, amenazas y manejo seguro de la información.

ARTICULO 8º. PRINCIPIOS

- **Confidencialidad:** Acceso solo por personal autorizado.
- **Integridad:** Información libre de modificaciones no autorizadas.
- **Disponibilidad:** Acceso oportuno y garantizado.
- **Autenticidad:** Veracidad de los usuarios y fuentes.
- **Trazabilidad:** Registro verificable de actividades.

ARTICULO 9º. ROLES Y RESPONSABILIDADES:

La **Política de Seguridad de la Información** se estructura en **cuatro ejes fundamentales**, sobre los cuales se distribuyen los roles y responsabilidades de las distintas áreas y trabajadores de la entidad, así:

Gobernanza de la seguridad de la información: La Junta Directiva aprueba y respalda la presente política, mientras que la Presidencia Ejecutiva define las instancias responsables de liderar, aprobar

y supervisar las políticas, procedimientos y mecanismos de control relacionados con la gestión de la seguridad de la información.

Gestión del riesgo de seguridad de la información: Establece las responsabilidades en la identificación, análisis, tratamiento, monitoreo y control de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información. En este eje participan:

- El guardián de la información: Responsable de liderar el cumplimiento y la actualización de la política.
- Área de sistemas o responsable técnico: Implementa los controles técnicos, monitorea los accesos y gestiona los incidentes de seguridad.

Cumplimiento normativo y legal:

Designa las responsabilidades relacionadas con el cumplimiento de la legislación vigente en materia de seguridad de la información, especialmente lo establecido en la Ley 1581 de 2012 (protección de datos personales), la Ley 1712 de 2014 (transparencia y acceso a la información pública), y demás normas que resulten aplicables.

Capacitación y concientización: Asigna la responsabilidad de diseñar, ejecutar y participar en programas de formación y sensibilización en seguridad de la información. Esta obligación recae sobre todas las áreas, garantizando que el personal:

- Conozca sus responsabilidades en el manejo seguro de la información.
- Cumpla con los lineamientos establecidos.
- Reporte oportunamente cualquier vulnerabilidad o evento sospechoso.

ARTICULO 10°. POLITICAS ESPECIFICAS:

Control de Acceso

- Todo acceso a sistemas debe estar autenticado y autorizado.
- Cada usuario contará con un **ID único**, personal e intransferible.
- Las contraseñas deben ser robustas, confidenciales, renovadas periódicamente y no reutilizadas.

Gestión de Equipos y Recursos

- Prohibido instalar software o hardware sin autorización del área de TI.
- Toda entrega o retiro de equipos debe ser documentada.
- Todos los equipos de TI y dispositivos móviles deben contar con cifrado y antivirus actualizado.

- Bloqueo de acceso a dispositivos externos como USB – Unidades de almacenamiento externar que puedan alterar con ingreso de software maliciosos o virus que puedan vulnerar información sensible.

Clasificación de la Información

- Se define la información como Pública o Privada, Uso Interno, Confidencial o Reservada.
- Toda información confidencial debe ser cifrada y protegida en su almacenamiento y transmisión.

Correo Electrónico e Internet

- El uso del correo electrónico e internet está limitado exclusivamente a fines institucionales.
- Está Prohibido enviar contenido ofensivo, ilegal, cadenas o mensajes personales.
- El tráfico de red será **monitoreado para prevenir riesgos de seguridad**.

Copias de Seguridad

- La Cámara de Comercio de San José implementará y mantendrá un sistema de copias de seguridad que garantice la integridad, disponibilidad y recuperación oportuna de la información institucional.
- Las copias de respaldo se realizarán con una periodicidad definida, y serán almacenadas en medios seguros que aseguren su conservación y acceso controlado. Se promoverá el uso de tecnologías modernas, automatizadas y con respaldo fuera de sitio (off-site o en la nube), que minimicen el riesgo de pérdida de datos y reduzcan la dependencia de dispositivos físicos vulnerables.
- Solo el personal debidamente autorizado podrá gestionar los respaldos. Así mismo, se establecerán pruebas periódicas de restauración para validar la confiabilidad de los respaldos y garantizar la continuidad operativa ante eventos críticos

Seguridad Física

- El acceso a áreas críticas (cuartos de servidores, archivos, switches) es restringido.
- Toda salida de equipos debe estar autorizada mediante formato formal.

Seguridad en Biometría y Firma Digital

- El sistema biométrico debe estar vinculado a la infraestructura de firma digital.
- Todo trabajador con acceso a biometría deberá firmar el Acuerdo de Confidencialidad.

Gestión de Incidentes

- Todo incidente relacionado con la seguridad de la información deberá ser reportado de manera inmediata al Comité de Seguridad, para su respectivo tratamiento.

- Cada caso será documentado, analizado y tratado, aplicando las medidas correctivas necesarias para prevenir su recurrencia.

Concientización

- Se implementarán campañas internas continuas de concientización, orientadas a promover buenas prácticas en seguridad de la información y el cumplimiento de las políticas institucionales.

ARTICULO 11°. PREVENCIÓN DEL FRAUDE – SIPREF:

La Cámara de Comercio de San José, en cumplimiento de la normatividad colombiana y en coherencia con su compromiso de proteger la información institucional, adopta los lineamientos del Sistema de Prevención del Fraude – SIPREF, estableciendo controles que permitan:

- Identificar y analizar riesgos de fraude en procesos físicos y digitales.
- Implementar medidas de seguridad que reduzcan la posibilidad de suplantación, alteración de datos, manipulación indebida o accesos no autorizados.
- Fortalecer los sistemas de monitoreo, trazabilidad y alertas tempranas.
- Capacitar a todos los colaboradores en la detección y reporte de posibles fraudes.
- Garantizar que los casos detectados sean gestionados bajo protocolos formales de investigación, sanción y mejora continua.

ARTICULO 12°. DECLARACIÓN DE LA POLÍTICA:

La Alta Dirección y todos los colaboradores de la Cámara de Comercio de San José se comprometen con la implementación, cumplimiento y mejora continua de la presente Política de Seguridad de la Información, cuyo propósito es garantizar la confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad de la información institucional, independientemente de su formato, medio o entorno.
Este compromiso se materializa mediante la aplicación sistemática de controles técnicos, procedimientos operativos, formación constante del personal y el cumplimiento del marco normativo vigente, asegurando así la protección de los activos de información, la continuidad del negocio y la confianza de los grupos de interés.

ARTICULO 13°. CUMPLIMIENTO DE LA POLÍTICA:

La Cámara de Comercio de San José garantizará el cumplimiento de esta política mediante la formulación, diseño, ejecución y seguimiento de un Programa de Seguridad de la Información, orientado a implementar los controles, procedimientos y buenas prácticas necesarios para proteger los activos de información en todos los niveles de la organización.

El incumplimiento de lo dispuesto en la presente Política de Seguridad de la Información se clasifica en dos formas principales:

1. **Por Acción**: Se configura cuando un trabajador, contratista o tercero ejecuta de manera intencional o negligente una conducta contraria a las disposiciones de esta política, ejemplo: (Divulgación no autorizada de información confidencial).

2. **Por Omisión**: Se presenta cuando un trabajador, contratista o tercero deja de cumplir con un deber u obligación establecida en esta política, generando riesgo o vulnerabilidad para la entidad, ejemplo: (No reportar incidentes de seguridad detectados)

En cualquiera de sus formas, el incumplimiento de esta política será considerado una falta disciplinaria o contractual, y dará lugar a la aplicación de medidas correctivas conforme al régimen interno de la entidad, la normatividad laboral y las disposiciones contractuales vigentes, sin perjuicio de las acciones legales a que haya lugar.

Parágrafo 1: La Oficina del Sistema de Control Interno (SCI) será responsable de coordinar y ejecutar las auditorías internas, actividades de verificación, seguimientos, mediciones de desempeño y demás mecanismos de control establecidos para el cumplimiento de la Política de Seguridad de la Información, así como de las demás políticas asociadas.

Parágrafo 2: Para efectos de cumplimiento, control, seguimiento y mejora continua, se tendrán en cuenta las actividades definidas en el Plan Estratégico 2023–2027 y en el plan de trabajo correspondiente a cada vigencia, garantizando la articulación con los objetivos institucionales.

Parágrafo 3: Las mediciones se realizarán mediante indicadores de gestión, los cuales permitirán evaluar los avances cuantitativos y cualitativos de manera semestral y al cierre de cada vigencia. Dichos indicadores facilitarán la identificación de posibles riesgos, la implementación de acciones correctivas y el fortalecimiento de la mejora continua en cumplimiento de los objetivos institucionales.

ARTICULO 14°. VIGENCIA:

La presente política de Seguridad de la Información rige a partir de la fecha adopción y firma.

ARTICULO 15°. DIVULGACIÓN:

Esta política dará a conocer a todos los colaboradores mediante los diferentes canales de comunicación de la entidad y estará disponible para todas las partes interesadas.

ARTICULO 16°. EVALUACIÓN Y ACTUALIZACIÓN:

Esta política fue revisada por el Comité de Calidad, aprobada por el Comité de Seguridad de la Información, y ratificada por la Junta Directiva, conforme a lo establecido en los estatutos de la Cámara de Comercio de San José.

La presente Política de Seguridad de la Información será revisada anualmente, o antes si ocurren cambios tecnológicos, normativos, estructurales o de riesgo que así lo ameriten. Toda actualización deberá ser aprobada por la Presidencia Ejecutiva y el Comité de Seguridad de la Información, garantizando su pertinencia, aplicabilidad y mejora continua.

La presente Política de Seguridad de la Información fue revisada por el Comité de Calidad, aprobada por el Comité de Seguridad de la Información y ratificada por la Junta Directiva, conforme a lo establecido en los estatutos de la Cámara de Comercio de San José.

La política será evaluada y revisada de manera anual, con el fin de garantizar su efectividad y alineación con los objetivos estratégicos de la Cámara de Comercio. Sin perjuicio de lo anterior, podrá actualizarse antes de dicho plazo en caso de presentarse cambios de carácter tecnológico, normativo, estructural o de riesgo que lo ameriten.

Toda actualización deberá contar con la aprobación de la Presidencia Ejecutiva y del Comité de Seguridad de la Información, asegurando su pertinencia, aplicabilidad y mejora continua.

ARTICULO 17°. APROBACIÓN:

La presente Política de Seguridad de la Información ha sido revisada y aprobada por la Alta Dirección de la Cámara de Comercio de San José, como expresión del compromiso institucional con la gestión eficiente, transparente y responsable de la seguridad de la información, salvaguardando los intereses de todas las partes involucradas y asegurando el cumplimiento de la misión, visión y objetivos estratégicos de la entidad.

Esta política entra en vigencia a partir de la fecha de su aprobación y será de obligatorio cumplimiento para todos los colaboradores, contratistas, proveedores, usuarios y demás partes interesadas vinculadas a los procesos institucionales de la Cámara.

Aprobada por la Junta Directiva en reunión ordinaria realizada el día 27 del mes de septiembre del año 2025, mediante el Acta No. 445, y será de obligatorio cumplimiento para todos.

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**MOTIVO**
01	15/12/2015	Creación de la Política.
02	27/08/2025	Esta actualización se realiza con el fin de dar cumplimiento a la normatividad vigente en materia de seguridad de la información y atender las necesidades institucionales identificadas en el marco del Programa de Seguridad de la Información. Su propósito es fortalecer la gestión de riesgos, prevenir el fraude y los actos de corrupción, proteger los activos de información y garantizar la continuidad operativa de la Cámara de Comercio de San José.

Oscar Mauricio Quevedo Padilla	**Kelly Johanna Mendoza Coronado**	**Jorge Alberto Gordillo Vacca**	**Franf Helver Garzón Lozano**
Técnico en Sistemas	Directora Registro Publico	Presidente Junta Directiva	Presidente Ejecutivo
ELABORÓ	**REVISÓ**	**REVISÓ y APROBÓ**	**REVISÓ y APROBÓ**