

**DECISION DIRECTIVA No. 005**  
(Agosto 30 de 2022)

**“POR MEDIO DE LA CUAL SE REVOCA LA RESOLUCION DIRECTIVA No. 09 DE 2016 POR MEDIO DE LA CUAL SE ADOPTA LA POLITICA DE SEGURIDAD DE LA INFORMACION DE LA CÁMARA DE COMERCIO DE FACATATIVÁ Y SE EXPIDE LA NUEVA POLITICAN DE SEGURIDAD DE LA INFORMACION”**

La Junta Directiva de la Cámara de Comercio de Facatativá, en uso de sus atribuciones estatutarias y,

**CONSIDERANDO**

Que conforme el artículo 12, de la Resolución No. 021 de junio siete (7) de dos mil dieciséis (2016) mediante la cual se reforman los estatutos de la Cámara de Comercio de Facatativá, en su numeral 1 se establece que es función de la Junta Directiva *“aprobar las políticas generales de la Cámara de Comercio y velar por su cumplimiento”*.

Que mediante Resolución Directiva No. 09 del 29 de marzo de 2016, la Cámara de Comercio de Facatativá adoptó la política de seguridad de la información, la cual se hace necesaria revocar, por cuanto no se incluyó y ajustó a la Norma NTC-ISO 27001 de 2013, la cual trata sobre el sistema de gestión de la seguridad de la información.

Que la Cámara de Comercio de Facatativá, consciente que la información es un activo estratégico, ha implementado un sistema de seguridad de la información (SSI), lineamientos definidos en el Manual de Seguridad de la Información.

Que, en mérito de lo expuesto,

**DECIDE**

**ARTÍCULO PRIMERO:** Adóptese la Política de seguridad de la información, plasmado en el documento que hace parte integral de la presente decisión en nueve (9) folios

**OBJETIVO GENERAL**

La seguridad de la información permite desde la evaluación de los riesgos, implementar controles para para la Gestión de activos, redes, plataformas tecnológicas, e información, que permita desarrollar sus procesos, prestar los servicios y gestionar los tramites, garantizando el cumplimiento de la legislación vigente y los pilares de confidencialidad, integridad y disponibilidad de la información.

**OBJETIVOS ESPECIFICOS**

- Protección de los activos y recursos informáticos

- > Protección de la información de pérdida, daños o ciberataques.
- > Gestión de los riesgos de seguridad de la información, aplicando controles en las personas, los procesos y la tecnología de acuerdo a la vulnerabilidad y el impacto.
- > Garantizar la disponibilidad, integridad y confidencialidad de la información creada, procesada, recolectada, transmitida y almacenada por su actividad, con el fin de minimizar impactos financieros, operativos o legales debido al uso incorrecto de la misma.
- > Alineación estratégica de la organización, Implementando proyectos de innovación tecnológica requeridos para la competitividad, cumplimiento legal y mejoramiento continuo.
- > Gestión y control de incidentes de seguridad en las redes, sistemas de información o seguridad de la información.
- > Cumplimiento de la normatividad vigente en cuanto a seguridad de la información y tratamiento de datos personales.
- > Fortalecimiento de la cultura de seguridad de la información y buenas prácticas de todas las partes interesadas (funcionarios, contratistas, usuarios, entes de control etc.)

### **ALCANCE**

El sistema de seguridad de la información es aplicable en todos los procesos de la "Cámara de Comercio de Facatativá", durante todo el ciclo de vida de la información, desde: la creación, distribución, almacenamiento, conservación, consulta y destrucción por todas las partes interesadas de los funcionarios, colaboradores, contratistas, entidades de control y usuarios.

### **MARCO NORMATIVO**

La presente política se implementa alineada a los requisitos establecidos en:

- Norma NTC-ISO 27001. 2013 sistema de gestión de la seguridad de la información
- Ley 1341 de 2009. Tecnologías de la Información y aplicación de seguridad
- Ley 1273 de 2009, Delitos Informáticos protección de la información y los datos.
- Ley 23 de 1982 propiedad intelectual y derechos de autor
- Ley 1581 de 2012 Protección de datos personales
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data

### **PILARES**

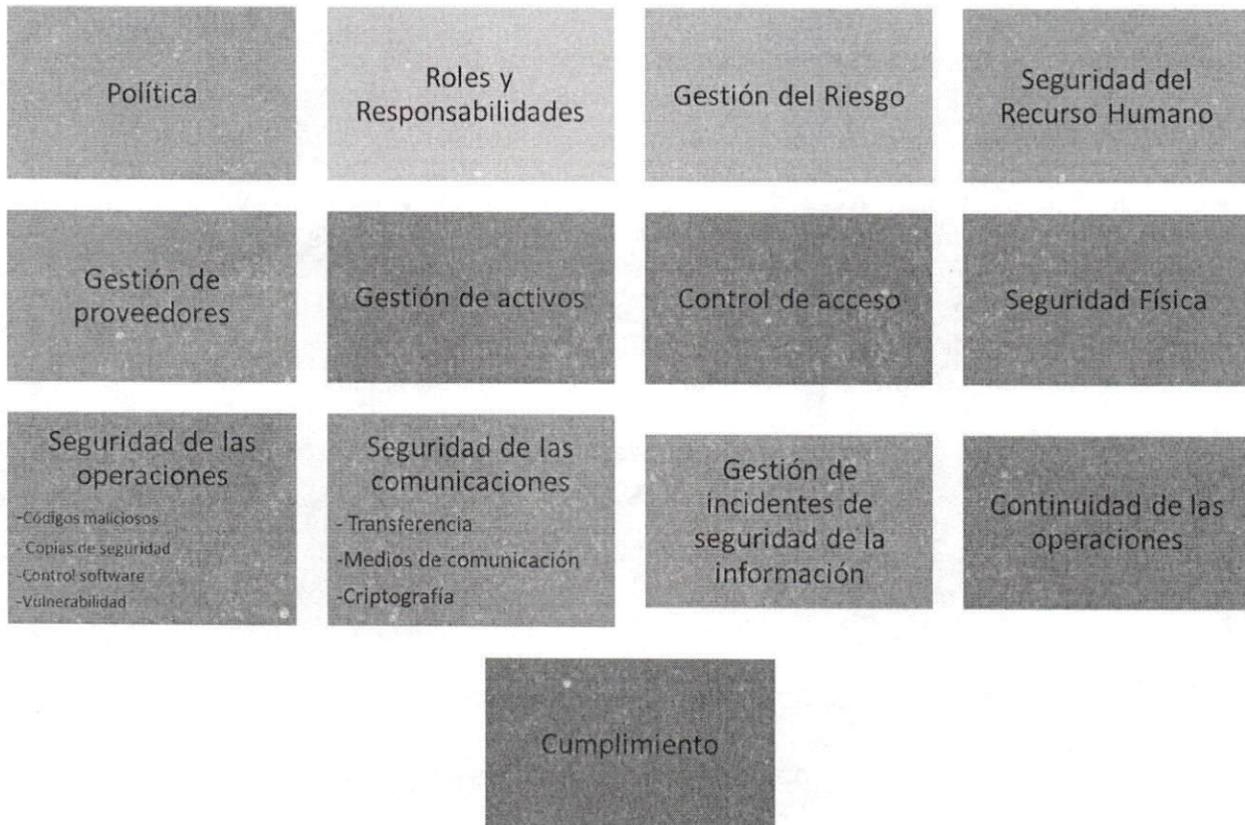
La Seguridad de la información dentro de la Cámara de Comercio de Facatativá está enmarcado bajo los siguientes pilares:

- **Confidencialidad:** Es la garantía de que la información será protegida y no será consultada, usada, divulgada o robada mediante ciberataques, acciones de espionaje o

cualquier otro delito informático; dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso controlado.

- **Integridad:** Garantiza la veracidad de la información, es importante que la información circule o se almacenen de la misma forma como se creó sin que exista intervención externa para dañarla, comprometerla o alterarla sin autorización previa.
- **Disponibilidad:** Se vincula al tiempo y a la accesibilidad de la información y de los sistemas corporativos, es decir, si pueden consultarse en el momento que amerite. La indisponibilidad de la información empresarial puede causar serios problemas en la continuidad del negocio por interrupción en las actividades.

### LINEAMIENTOS



### ROLES Y RESPONSABILIDADES

El Sistema de gestión de seguridad de la información, está en cabeza de la **Presidencia Ejecutiva** quien lidera el sistema a toda la organización. La **Dirección de Desarrollo Institucional**, vela por el cumplimiento de los controles y Gestión de las TIC's, garantiza el cumplimiento de los controles definidos en este documento.

La Cámara y Comercio de Facatativá, por medio de Talento Humano, define las responsabilidades de los diferentes roles en la organización, para gestionar, controlar, asegurar y garantizar la seguridad de la información.

> ***Dirección Administrativa y Financiera:***

- Realiza la compra y control de los activos adquiridos por la organización de acuerdo al procedimiento de activos fijos.
- Mantiene actualizado el inventario de activos fijos, respecto a equipos informáticos.
- Controlar el inventario del almacén de suministros.
- Proporciona los recursos físicos y financieros para garantizar la seguridad física de la infraestructura tecnológica y de comunicaciones de la CCF
- Vela por el cumplimiento de este procedimiento por parte del personal y de los proveedores.
- Asegurar el suministro de los recursos físicos y financieros para la ejecución del plan de continuidad
- Gestionar con el profesional de seguridad y salud en el trabajo, el plan de atención de emergencia, cuando se presente algún evento.

***Talento Humano:***

- Notifica a Gestión TIC's de la CCF, las vinculaciones y desvinculaciones del personal con la debida antelación para que sea factible realizar las actividades descritas en este procedimiento.
- Tomar las medidas disciplinarias por el incumplimiento de este procedimiento y las normas de uso, confidencialidad y seguridad de la información.
- Capacita al personal en protocolos para la seguridad física.

> ***Dirección de Desarrollo Institucional***

- Activar y liderar el proceso de continuidad de la seguridad de la Información.
- Evaluar y liderar la gestión del cambio en los procesos de tecnología.
- Controlar los proyectos a desarrollar por tecnología de acuerdo al plan estratégico y plan de trabajo definido.

***Gestión de la TIC's:***

(Coordinador de sistemas informáticos y Profesional de soporte tecnológico)

- Administrar el uso de los Sistemas y equipos de Información de la CCF
- Capacitar al personal en el uso de los activos e información relacionados con sistemas de la información
- Velar por el cumplimiento de las políticas y lineamientos definidos en este procedimiento.



- Configurar y asegurar el correcto funcionamiento de los equipos y servicios que el personal requiera para el desempeño de sus actividades.
- Gestionar las requisiciones de equipos, software y demás elementos informáticos, complementarios para la organización.
- Proporcionar la información que requiera la Dirección Administrativa y Financiera para mantener actualizado el inventario de activos fijos, respecto a equipos informáticos.
- Mantener actualizado los registros de inventario de los activos informáticos, incluyendo los asignados a usuarios y aquellos de reposición.
- Auditar los programas y licencias ofimática instaladas en los equipos.
- Gestionar permisos de acceso del personal de la CCF y usuarios a los programas y aplicativos, de acuerdo a los privilegios del cargo y la labor a desarrollar.
- Participar en reuniones, foros, capacitaciones en entidades de control o grupos de interés (Confecamaras, Superintendencia de Industria y comercio, Superintendencia financiera, etc.) en temas de ciberseguridad.
- Capacitar al personal en control de acceso a los sistemas, programas, redes y aplicativos relacionados con sistemas de información.
- Velar por el cumplimiento de las políticas y lineamientos definidos en este procedimiento, por los proveedores de sistemas de información y los usuarios.
- Mantener actualizados los directorios de los usuarios de la red.
- Garantizar la seguridad física en áreas y equipos, que manejan información crítica y activos informáticos.
- Realizar la inspección de locativas cada seis (6) meses para garantizar el buen estado de la infraestructura.
- Gestionar ante la Dirección administrativa y financiera los recursos necesarios para garantizar la seguridad física de las instalaciones que manejan información.
- Registrar, analizar, definir y desarrollar el plan de trabajo para la gestión del cambio en los sistemas de información.
- Identificar las amenazas en la seguridad de sistemas de información.
- Evaluar el impacto de los riesgos en cada uno de los servicios.
- Definir y actualizar las estrategias de respuesta.
- Establecer y actualizar el plan de recuperación.
- Planificar, realizar y evaluar los simulacros al plan de continuidad.
- Gestionar el proceso de continuidad en caso de presentarse eventos.

### ***Profesional II de soporte***

- Revisar los tickets recibidos, clasificarlos y priorizar su atención.
- Asignar el caso, al responsable de la solución.
- Solucionar la incidencia de soporte de Hardware y Software en los Nivel 1, nivel 2 y nivel 3.

### ***Coordinador de Sistemas de Información***



- Responsable de la implementación efectiva del proceso de gestión de incidentes en la CCF.

- Recibe los casos escalados para la solución de sistemas de Información y redes.
- Solucionar la incidencia de soporte a sistemas de Información en los Nivel 1, nivel 2 y nivel 3.
- Llevar el control del tiempo de respuesta
- Preparar los informes de gestión (No, de casos, tiempos y satisfacción del usuario).
- Alimentar la gestión del conocimiento

➤ ***Dirección de Asuntos jurídicos***

- Custodiar dentro de los contratos el licenciamiento de software.
- Gestionar los procesos judiciales interpuestos ante la Policía y Fiscalía por la violación de la seguridad de la información.

➤ ***Usuarios***

- Cumplir las políticas y lineamientos definidos en este procedimiento.
- Firmar y cumplir el acuerdo de uso, confidencialidad y seguridad de los sistemas de información
- Informar a Gestión de las TIC's incidentes, requerimientos y consultas que se puedan presentar durante la manipulación de los equipos y programas suministrados por la CCF.
- Informar a Gestión de las TIC's incidentes, bloqueos o pérdida de contraseñas de acceso que se puedan presentar durante el ingreso a red, programas o aplicativos suministrados por la CCF.
- Informar a Gestión de las TIC's incidentes, incumplimientos o riesgos en la seguridad física de las instalaciones e información.
- Observar y reportar cualquier debilidad de seguridad de la información
- Registrar en el Software Aplicativo (mesa de ayuda) las incidencias detectadas
- Dar el cierre a la incidencia solucionada y diligenciar la encuesta de satisfacción de usuarios.

➤ ***Empresa de Vigilancia***

Aplicar los controles de acceso del personal y permisos de salida de activos.

**VIGENCIA Y ACTUALIZACIÓN**

Esta política ha sido aprobada por la Junta Directiva de La Cámara De Comercio De Facatativá, entrará en vigor desde la firma y se aplicará durante el ciclo de vida de la información y hasta tanto no se emita alguna otra disposición corporativa o legal en cuanto a la materia de seguridad de la información.

La política de seguridad de la Información es revisada anualmente por la Dirección del SGC, evaluando su conveniencia, adecuación y eficacia.

Esta Política se publicará en la página web <https://www.ccfacatativa.org.co> de la CCF y debe ser conocida y adoptada por todos los colaboradores.

**ARTÍCULO SEGUNDO:** El presente plan puede ser objeto de revisión y ajuste, de acuerdo al seguimiento y evaluación que se realice del mismo.

**ARTÍCULO TERCERO:** El seguimiento, análisis y medición será responsabilidad de la Dirección de Desarrollo Institucional y la Coordinación de sistemas.

**ARTÍCULO CUARTO:** La presente decisión no se considera acto administrativo por ser proferida por la Cámara de Comercio de Facatativá, entidad de naturaleza privada, y rige a partir de la fecha de expedición y revoca todas las normas que le sean contrarias.

Comuníquese, al área o Dirección competente para su cumplimiento.

Dado en Facatativá, a los treinta (30) días del mes de agosto dos mil veintidós (2022).



**MANUEL ANTONIO VARGAS CAMELIO**  
Presidente Junta Directiva.



**GRATILIANO SUAREZ SUAREZ**  
Secretario Junta Directiva.

Revisó: JLVB/DAJ  EHPH/CS 