Contenido

CONTENIDO

INTRODUCCIÓN

Las dinámicas empresariales, tecnológicas y regulatorias actuales incrementan los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información. En este contexto, la Cámara de Comercio de Cali (CCC) consolida un marco de referencia para proteger la información institucional y la de sus empresarios, usuarios y grupos de interés.

El presente Manual recopila las políticas, lineamientos y normas de Seguridad de la Información definidos por la CCC, los cuales constituyen los pilares para el desarrollo, implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI), alineado con ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de la Información.

Toda implementación o uso de aplicaciones, servicios de información, hardware, software, conectividad, bases de datos, terceros y colaboradores que procesen o tengan acceso a información de la CCC, deberá cumplir lo establecido en este manual, dado que su razón de ser es la protección integral de la información y la continuidad de los servicios.

1. OBJETIVO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Proteger la información de la Cámara de Comercio de Cali mediante la aplicación de controles adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información, y que soporten el cumplimiento legal, contractual y regulatorio aplicable, así como la continuidad de los procesos del alcance del SGSI.

2. ALCANCES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El alcance del SGSI de la Cámara de Comercio de Cali cubre la seguridad de la información asociada a los procesos críticos de la entidad, por ser indispensables para gestionar registro mercantil, ofrecer servicios oportunos, emitir información certificada, mantener información disponible para consulta e informes estadísticos, desarrollar soluciones informáticas y soportar la infraestructura tecnológica.

El alcance incluye las siguientes sedes y modalidades de operación:

- Sede Principal
- Sede Obrero
- Sede Unicentro
- Sede Aguablanca
- Sede Yumbo
- Sede Jamundí
- Teletrabajo
- Datacenter

3. DEFINICIONES, CONCEPTOS, TÉRMINOS Y EQUIVALENCIAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Principios de la Seguridad de la Información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: Mantenimiento de la exactitud y completitud de la información.
- Disponibilidad: La información debe ser accesible y utilizable a demanda por una entidad autorizada.

Definiciones clave (resumen):

- Lineamientos de Seguridad de la Información: Conjunto de reglas y prácticas que regulan cómo se maneja, protege y distribuye la información.
- Normas de Seguridad de la Información: Enunciados detallados de obligatorio cumplimiento que desarrollan las políticas.

- Activo de información: Cualquier información o elemento asociado a su tratamiento (sistemas, soportes, edificios, personas) con valor para la entidad.
- Transferencia de información: Traspaso de información de un activo de soporte a otro.

Definiciones relacionadas con protección de datos personales (Ley 1581 de 2012):

- Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- Dato sensible: Dato que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación (incluye datos biométricos).
- Base de datos: Conjunto organizado de datos personales objeto de tratamiento.
- Titular: persona natural cuyos datos son objeto de tratamiento.
- Responsable del tratamiento: Quien decide sobre la base de datos y/o el tratamiento.
- Tratamiento: Operación o conjunto de operaciones sobre datos personales (recolección, almacenamiento, uso, circulación o supresión).

Indicadores:

- KPIs (Indicadores Clave de Rendimiento): miden el éxito pasado o presente hacia los objetivos.
- KRIs (Indicadores Clave de Riesgo): anticipan riesgos futuros que podrían impedir alcanzarlos.

4. CONTEXTO DE LA ORGANIZACIÓN

La CCC gestiona su estrategia y operación en un entorno dinámico donde convergen riesgos de continuidad, tecnológicos, informáticos, reputacionales y regulatorios. En consecuencia, el SGSI se integra al SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN para asegurar la protección sistemática de la información, habilitando la prestación confiable de los servicios del alcance.

4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO

El contexto institucional se documenta y mantiene actualizado en el documento D-DE-0001, disponible para consulta interna. El SGSI toma dicho contexto como entrada para la identificación y tratamiento de riesgos de seguridad de la información.

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Basado en las partes interesadas identificadas en D-DE-0001, la CCC determina aquellas pertinentes al SGSI y define requisitos de seguridad de la información considerando, entre otros: empresarios, usuarios, colaboradores, proveedores, entes de control y entidades delegantes. Estos requisitos se traducen en controles, responsabilidades y compromisos de cumplimiento.

4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El alcance del SGSI se define en el numeral 2 de este manual y se revisa cuando ocurren cambios relevantes en procesos, sedes, tecnologías, servicios, tercerizaciones o requisitos legales. La definición de alcance incluye límites, interfaces y dependencias, con el fin de asegurar consistencia operacional y control del riesgo.

4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y SUS PROCESOS

El SGSI establece, implementa, mantiene y mejora procesos para: (i) gobernar la seguridad de la información; (ii) gestionar riesgos; (iii) operar controles; (iv) gestionar incidentes; (v) asegurar continuidad; (vi) medir desempeño y (vii) ejecutar mejoras. La interacción con los procesos del Sistema de Gestión de Seguridad de la Información se asegura mediante roles, comités y la gestión de información documentada.

5. LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

La Alta Dirección demuestra liderazgo y compromiso con el SGSI asegurando: la asignación de recursos; la integración de requisitos de seguridad en los procesos; el enfoque basado en riesgos; el cumplimiento legal y contractual; la comunicación de la importancia de la seguridad de la información; y el respaldo a los responsables para implementar controles y gestionar incidentes.

5.1.2 ENFOQUE AL CLIENTE

La CCC asegura el cumplimiento de requisitos legales y reglamentarios aplicables y considera las necesidades de empresarios y usuarios para proteger la información que soporta los servicios del alcance. Los riesgos y oportunidades que puedan afectar la conformidad del servicio y la protección de la información deben ser comunicados oportunamente a los responsables de proceso y a la función de Seguridad de la Información.

5.2 PILARES (Política de Seguridad de la Información)

Para la Cámara de Comercio de Cali, la información es un activo fundamental y estratégico. Por tal motivo, la seguridad de la información es un proceso integral, transversal y generador de valor. Los colaboradores internos y externos que, en ejercicio de sus funciones, tengan acceso, procesen o generen información, deberán cumplir la normativa definida para su gestión segura.

La CCC reafirma su compromiso de implementar y mejorar continuamente el SGSI, manteniendo una adecuada gestión de riesgos, el cumplimiento de requisitos legales, regulatorios y contractuales, y la vigencia de la normativa interna de Seguridad de la Información.

5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

La estructura organizacional, roles y funciones relevantes para el SGSI se describen en el documento D-GH-0031 Macroestructura Organizacional y en los perfiles de cargo. En general, los dueños de proceso son responsables de proteger los activos bajo su gestión, Tecnología, procesos y el oficial de Ciberseguridad lideran la definición, acompañamiento y seguimiento de controles, y administran y operan la plataforma tecnológica y los mecanismos de monitoreo y respuesta.

6. PLANIFICACIÓN

6.1 ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES

La CCC gestiona los riesgos de seguridad de la información mediante el Procedimiento de Gestión de Riesgos Empresarial M-AC-0004, que permite definir responsabilidades, identificar y actualizar el contexto, identificar y analizar riesgos, valorar, tratar, monitorear y comunicar. Los riesgos se consolidan en los mapas de riesgos por proceso y su gestión se soporta en el aplicativo institucional de gestión.

6.2 OBJETIVOS ESTRATEGICOS, CORPORATIVOS Y PLANIFICACIÓN PARA LOGRARLOS

Objetivos de Seguridad de la Información (alineados con la política y la estrategia institucional):

- Proteger la información de empresas, empresarios y profesionales independientes.
- Mantener la confidencialidad e integridad de la información creada, procesada o resguardada por los procesos del negocio.
- Asegurar la disponibilidad de la información y de los servicios que soportan los procesos de negocio según necesidades.
- Cumplir disposiciones legales, regulatorias y contractuales relacionadas con seguridad de la información.
- Identificar y tratar los riesgos de seguridad de la información más relevantes para los procesos de negocio.
- Gestionar eventos e incidentes de seguridad de la información.
- Capacitar y concientizar a colaboradores y terceros en seguridad de la información.

La planificación para lograr estos objetivos se integra con los planes de acción de los procesos del alcance, incluyendo actividades, responsables, cronogramas, indicadores y recursos.

6.3 PLANIFICACIÓN DE LOS CAMBIOS

Los cambios que impacten el SGSI (tecnologías, servicios, tercerizaciones, controles, alcance) deben planificarse y ejecutarse de manera controlada. Los cambios tecnológicos se gestionan bajo el procedimiento P-GT-0042 Gestión de cambios tecnológicos, considerando pruebas, planes de reversa (rollback) y el impacto sobre continuidad del negocio y recuperación de desastres.

7. APOYO

7.1 RECURSOS

La CCC, a través del presupuesto aprobado por la Alta Dirección, asegura la provisión de recursos esenciales para implementar, operar, revisar, mantener y mejorar el SGSI. Los recursos incluyen personas, infraestructura, herramientas tecnológicas y recursos financieros.

7.2 COMPETENCIA
La CCC define competencias requeridas para roles relacionados con seguridad de la información, asegura formación y/o experiencia apropiada y mantiene evidencia. La selección, inducción y capacitación se gestionan a través de Gestión Humana conforme al Manual de Personal y perfiles de cargo.

7.3 TOMA DE CONCIENCIA
La CCC promueve la toma de conciencia sobre seguridad de la información mediante campañas, sensibilizaciones, inducciones y comunicaciones periódicas. Los colaboradores y terceros deben comprender su contribución al SGSI, las implicaciones de no cumplir y sus responsabilidades frente a la protección de información.

7.4 COMUNICACIÓN
La CCC establece comunicaciones internas y externas pertinentes al SGSI, incluyendo qué comunicar, cuándo, a quién, cómo y quién comunica. Las comunicaciones se alinean con las políticas y protocolos institucionales (Comunicaciones y Gestión Humana) y con requerimientos de reporte de incidentes.

7.5 INFORMACIÓN DOCUMENTADA
La documentación del SGSI se integra con el SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y se gestiona según los procedimientos institucionales de control documental. Incluye políticas, manuales, procedimientos, instructivos, formatos, registros y evidencias.

7.5.1 Creación y actualización
La creación, modificación o eliminación de documentos del SGSI se realiza conforme al procedimiento de estructura y control de la información documentada. Los dueños de proceso revisan periódicamente su documentación y el proceso de Mejoramiento asegura disponibilidad de versiones vigentes en el repositorio institucional.

7.5.2 Control de la información documentada
Se definen parámetros de almacenamiento, acceso, conservación, protección, control de cambios y disposición. Los registros se conservan según TRD y lineamientos de Gestión Documental, garantizando trazabilidad y evidencia para auditoría.

8. OPERACIÓN

8.1 PLANIFICACIÓN Y CONTROL OPERATIVO
La CCC planifica, implementa y controla los procesos necesarios para cumplir los requisitos del SGSI e implementar las acciones determinadas en el capítulo 6, mediante:

- Establecer criterios para los procesos del SGSI (p. ej., entradas/salidas, responsables, controles, indicadores, criterios de aceptación).
- Implementar el control de los procesos de acuerdo con los criterios definidos (p. ej., verificaciones, aprobaciones, segregación de funciones, monitoreo y registros).

La información documentada se mantiene disponible en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

La CCC controla los cambios planificados y revisa las consecuencias de cambios no deseados, tomando medidas para mitigar cualquier efecto adverso cuando sea necesario.

La CCC garantiza que los procesos, productos o servicios proporcionados externamente que sean relevantes para el SGSI estén controlados, incluyendo requisitos de seguridad en contratos, evaluación de proveedores, seguimiento al desempeño y gestión de cambios del servicio.

8.2 EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
La CCC realiza evaluaciones de riesgos de seguridad de la información a intervalos planificados y cuando se propongan u ocurran cambios significativos (p. ej., nuevas aplicaciones/servicios, cambios de infraestructura, tercerización, incidentes mayores o cambios regulatorios), teniendo en cuenta los criterios establecidos en el numeral 6.1.2 a) (criterios de aceptación del riesgo y criterios para realizar evaluaciones).

Como evidencia, la CCC conserva información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información (p. ej., informe de evaluación, matriz/mapa de riesgos, propietarios del riesgo, niveles de riesgo, y decisiones de priorización).

8.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La CCC implementa el plan de tratamiento de riesgos de seguridad de la información, asegurando que los controles seleccionados se implementen, operen y sean monitoreados según lo planificado.

La CCC conserva información documentada de los resultados del tratamiento de riesgos de seguridad de la información (p. ej., plan de tratamiento, estado de implementación, evidencias de ejecución, aceptación de riesgo residual, y Declaración de Aplicabilidad cuando corresponda).

9. EVALUACIÓN DEL DESEMPEÑO

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Se establecen métricas e indicadores (KPIs y KRIs) para evaluar la eficacia de los controles implementados, alineados con los objetivos del negocio. Los responsables reportan periódicamente el estado de indicadores y la Dirección revisa resultados para decisiones basadas en datos y asignación de recursos.

9.2 AUDITORIA INTERNA

La CCC no cuenta con la certificación en la norma ISO 27001; en consecuencia, el capítulo de auditorías internas para Seguridad de la Información aún no está formalmente establecido. Sin embargo, como iniciativa para la adopción de buenas prácticas, se ha realizado un diagnóstico inicial (Gap) orientado a la futura implementación de dicha norma.

9.3 REVISION POR LA DIRECCIÓN

La CCC realiza seguimiento y revisión del SGSI a través de los comités de seguridad y privacidad de la información y una revisión general anual en el comité de mejoramiento (revisión gerencial del sistema de gestión de Seguridad de la Información). La revisión considera, por ejemplo: Desempeño, resultados de auditoría, incidentes, riesgos, estado de acciones, cambios y oportunidades de mejora.

10. MEJORA

10.1 Generalidades

La Cámara de Comercio de Cali promueve la mejora continua para fortalecer la Seguridad de la Información. Aunque no tiene certificación ISO/IEC 27001, ya comenzó acciones alineadas con buenas prácticas internacionales para implementar un SGSI en el futuro. Esta mejora se basa en el diagnóstico inicial, la gestión de riesgos, análisis de incidentes y revisiones internas, lo que facilita identificar oportunidades para optimizar controles, políticas y procesos de protección de los activos de información.

10.2 No conformidad y Acción Correctiva

La CCC aún no cuenta con un SGSI certificado ISO/IEC 27001, por lo que la gestión de no conformidades se basa en diagnósticos, evaluaciones internas y eventos de seguridad. Las brechas detectadas se consideran oportunidades de mejora. Cuando surge una desviación, se establecen acciones para eliminar su causa, reducir riesgos y fortalecer controles, priorizando según impacto y riesgo, y haciendo seguimiento a su implementación.

ANEXO A. LINEAMIENTOS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN

2.1 CUMPLIMIENTO Y SANCIONES

- Lineamiento: Los lineamientos y normas de seguridad de la información definidos por la CCC. Son de obligatorio cumplimiento para colaboradores, contratistas, proveedores y terceros con acceso a información o recursos tecnológicos.
- Norma: El incumplimiento puede derivar en acciones disciplinarias o contractuales, según gravedad, incluyendo terminación de vínculo o contrato.

2.2 CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

- Lineamiento: El acceso a bases de datos y sistemas debe estar controlado por identificación personal.

- Norma: Cada usuario tendrá códigos únicos y accesos basados en el procedimiento P-GT-0002 seguridad de la información y uso de la plataforma tecnológica de los equipos de usuarios de la CCC

2.3 PROPIEDAD INTELECTUAL

- Lineamiento: La propiedad intelectual de desarrollos de software, productos y servicios debe protegerse.
- Normas: Asignación de derechos a la CCC y avisos de propiedad intelectual en productos/servicios.

2.4 CONTINUIDAD DEL NEGOCIO

- Lineamiento: La información crítica debe contar con respaldo para recuperación ante imprevistos o ataques.
- Normas: Plan de Recuperación de TI, planes de continuidad de proveedores críticos, respaldos, custodia externa, copias de respaldo y restauración P-GT-0001 y articulación con D-AC-0005 Plan de continuidad del negocio.

2.5 SEGURIDAD FÍSICA

- Lineamiento: Las áreas físicas deben tener seguridad acorde al valor de la información; la información confidencial/restringida debe mantenerse con acceso restringido.
- Normas: Controles de ingreso a áreas restringidas, seguridad de centros de datos/cableado, mantenimiento, visitantes, borrado seguro P-GT-0070 procedimiento borrado seguro de información, seguridad de portátiles.

2.6 SEGURIDAD EN EL PERSONAL

- Lineamiento: Proveer mecanismos para asegurar responsabilidades de seguridad desde ingreso hasta retiro.
- Normas: Cumplimiento obligatorio, acuerdos de confidencialidad, notificación de terminación/cambios, devolución de activos y paz y salvo.

2.7 CAPACITACIÓN Y CREACIÓN DE CULTURA

- Lineamiento: Programas periódicos de capacitación y concientización.
- Normas: Inducción, esquema anual de sensibilización y asistencia obligatoria.

2.8 CONTRATOS CON TERCEROS

- Lineamiento: Terceros deben cumplir políticas de seguridad y las establecidas en el contrato.
- Normas: Cláusulas de seguridad, derecho a auditar cuando aplique, acuerdos de confidencialidad y exigencia de niveles equivalentes de protección.

2.9 CONEXIÓN A REDES

- Lineamiento: Conexiones por redes públicas o acceso remoto deben autenticarse.
- Normas: Aprobación de nube, prohibición de nubes no corporativas para info confidencial, MFA y cifrado por defecto, segregación de redes, firewall como único punto de acceso, controles de enrutamiento, redes inalámbricas, transferencia de información con cifrado y acuerdos.

2.10 USO DE LOS RECURSOS INFORMÁTICOS

- Lineamiento: Recursos TI provistos por la CCC son para uso exclusivo del negocio.
- Normas: Condiciones de uso, prohibiciones (software sin licencia, material ofensivo), reporte de debilidades, instalación controlada, apagado de equipos, uso de internet, prohibición de explotación de vulnerabilidades, entrega de bases de datos a terceros prohibida.

2.11 CÓDIGO MALICIOSO

- Lineamiento: Documentos electrónicos entrantes deben revisarse preventivamente.
- Normas: Análisis de adjuntos/descargas/medios externos, gestión proactiva (EDR/XDR), escaneos periódicos de vulnerabilidades y mitigación según criticidad, antivirus actualizado.

2.12 GESTIÓN DE ACTIVOS

- Lineamiento: Proteger información producida/recibida según este manual y complementos.
- Normas: Eliminación segura, monitoreo (SOC), habilitación de logs, sincronización de relojes, mantenimiento, gestión de cambios P-GT-0042, gestión de capacidad, revisión periódica de accesos.

2.13 TRABAJO EN ÁREAS SEGURAS

- Lineamiento: Áreas seguras deben estar protegidas.

- Normas: Control y supervisión de acceso, registro de proveedores, protección de puntos de entrega de correo/impresoras y de información en tableros/documentos impresos.

2.14 DOCUMENTACIÓN DE LOS SISTEMAS DE INFORMACIÓN

- Lineamiento: La documentación de sistemas debe protegerse.
- Norma: Acceso controlado sólo a quienes lo requieran, bajo autorización del jefe inmediato.

2.15 VIRTUALIZACIÓN DE SERVICIOS

- Lineamiento: Exposición de servicios en internet con certificados electrónicos seguros.
- Normas: Certificados digitales, registros de auditoría, requisitos de desarrollo seguro, revisión de código, testing de seguridad, pruebas de stress, redes segmentadas, pruebas de penetración, plan de redundancia, desarrollo con terceros con requisitos de seguridad.

2.16 CUMPLIMIENTO DE REQUISITOS LEGALES

- Lineamiento: Cumplimiento de obligaciones legales, estatutarias, reglamentarias o contractuales.
- Normas: Identificación y monitoreo de legislación aplicable, protección de registros, revisión de cumplimiento por gerencia y líderes.

2.17 TRATAMIENTO DE DATOS PERSONALES

- Lineamiento: Proteger datos personales bajo la Ley 1581.
- Normas: Aplicación de M-AL-0015, cifrado de mensajes cuando aplique, para categorías sensibles.

2.18 REDES SOCIALES

- Lineamiento: Uso/publicación controlados para no comprometer seguridad.
- Buenas prácticas: Control de navegación, Capacitación a los usuarios de un uso responsable de internet.

2.19 GESTIÓN DOCUMENTAL

- Lineamiento: Protección de información documental mediante articulación con Gestión Documental y normatividad archivística.
- Norma: Gestión segura durante el ciclo de vida, trazabilidad, conservación y control por Comité de Gestión Documental.

2.20 IDENTIFICACIÓN BIOMÉTRICA

- Lineamiento: Proteger activos vinculados a integración con Confecámaras/Registraduría.
- Normas: Acuerdo de confidencialidad, uso de recursos, autorizaciones de traslado, identificación única, usuarios autorizados.

2.21 ENVÍO DE CORREOS DIRECTOS E-MAILING O FÍSICO

- Lineamiento: Envíos promocionales sólo por áreas autorizadas y con consentimiento cuando aplique.
- Normas: Dirección válida y baja, uso de CCO, límites de envíos masivos, plataforma autorizada, base de datos centralizada (PI).

2.22 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Lineamiento: Todos deben reportar incumplimientos, eventos y actividades anómalas.
- Normas: Procedimiento P-GT-0071 gestión de incidentes de seguridad y privacidad en datos personales.

NOTA: Este documento cambió de manera integral

	Revisó	Aprobó
Nombre	FERNANDO OLAYA OCAMPO/ MONICA GONZALEZ	MARÍA DEL MAR PALAU MADRIÑAN
Cargo	GERENTE DE TECNOLOGÍA/ JEFE DE INFRAESTRUCTURA TI	PRESIDENTA EJECUTIVA
Fecha	17 de abril de 2026	22 de abril de 2026