Tabla de Contenido

OBJETIVO 4
ALCANCE 4
DEFINICIONES 4
CONTENIDO5
GENERALIDADES....5
1.1 CONTEXTO DE LA ENTIDAD....5
1.1.1 INTERFACES Y DEPENDENCIAS....5
1.2 LIDERAZGO Y COMPROMISO....5
1.2.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN....6
1.2.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN....6
1.2.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN CCC. 6
1.3 SOPORTE....6
1.3.1 RECURSOS....6
1.3.2 COMPETENCIAS, TOMA DE CONSCIENCIA Y COMUNICACIÓN 6
1.3.3 INFORMACIÓN DOCUMENTADA 7
1.4 PLANIFICACIÓN Y OPERACIÓN....7
1.5 EVALUACIÓN DEL DESEMPEÑO....7
1.5.1 INDICADORES....7
1.5.2 AUDITORÍAS....7
1.5.3 REVISIÓN POR LA DIRECCIÓN....7
1.6 MEJORA 8
2. LINEAMIENTOS Y NORMAS DE SEGURIDAD DE LA INFORMACION....9
2.1 CUMPLIMIENTO Y SANCIONES....9
2.2 CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN....9
2.3 PROPIEDAD INTELECTUAL....11
2.4 CONTINUIDAD DEL NEGOCIO 12
2.5 SEGURIDAD FISICA 13
2.6 SEGURIDAD EN EL PERSONAL....16
2.7 CAPACITACION Y CREACION DE CULTURA....16
2.8 CONTRATOS CON TERCEROS....17
2.9 CONEXIÓN A REDES 18
2.10 USO DE LOS RECURSOS INFORMATICOS 19
2.11 CÓDIGO MALICIOSO....20
2.12 GESTIÓN DE ACTIVOS 21
2.13 TRABAJO EN ÁREAS SEGURAS....23
2.14 DOCUMENTACION DE LOS SISTEMAS DE INFORMACION 24
2.15 VIRTUALIZACION DE SERVICIOS....24
2.16 CUMPLIMIENTO DE REQUISITOS LEGALES 26

2.17 TRATAMIENTO DE DATOS PERSONALES....26
2.18 REDES SOCIALES....27
2.19 GESTION DOCUMENTAL....27
2.20 IDENTIFICACION BIOMETRICA....28
2.21 ENVÍO DE CORREOS DIRECTOS E-MAILING O FISICO....29
2.22 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN....30

1. INTRODUCCION

A través de este documento se pretende establecer un marco de referencia que reglamente la seguridad que debe darse a la información interna y de los empresarios tomando como base las políticas y normas definidas en este manual.

Este Manual recopila las políticas y normas de seguridad de la información definidas por la Cámara de Comercio de Cali, en adelante CCC; las cuales constituyen los pilares para el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI).

La implementación de nuevas aplicaciones, servicios de información, herramientas de hardware, software, seguridad de la información, bases de datos, conectividad y en general los empleados, terceros y la información de uso de la Cámara de Comercio de Cali, deben cumplir con las políticas y normas definidas en este documento, dado que su razón de ser es la protección de la información.

Adicionalmente se detallan las normas por las cuales ha de guiarse la función de Seguridad de la Información de la CCC, los propietarios de la información y en general todo el personal que labora en la Entidad.

Este manual se elaboró con base en los principios básicos de la Seguridad de la Información de acuerdo con la Norma ISO 27001-2013 y los consagrados en las leyes 1581 de 2012**" *Por la cual se dictan disposiciones generales para la protección de datos personales*"** y la 1712 del 2014 **"*Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*"**, que enmarcan las disposiciones sobre la seguridad que debe darse a la información manejada en las bases de datos y la protección de los datos personales de los Clientes y Grupos de Interés de la CCC.

OBJETIVO

Proteger la información de la Cámara de Comercio de Cali, a través de la aplicación de controles adecuados para brindar confidencialidad, integridad y disponibilidad de la información.

ALCANCE

El alcance del SGSI de la Cámara de Comercio de Cali, cubre la seguridad de la información del proceso de *Registros Públicos* y del proceso de *Tecnología y Procesos y Gestión Documental.* Estos procesos son indispensables para gestionar los registros públicos, ofrecer servicios oportunos, emitir información certificada, mantener la información disponible para consulta e informes estadísticos, desarrollar soluciones informáticas y soportar la gestión de la infraestructura tecnológica. Incluye las siguientes sedes en la ciudad de Cali (Valle del Cauca):

- Principal
- Obrero
- Unicentro
- Aguablanca
- Yumbo
- Jamundí

Y sus centros de datos principal y alterno. Lo anterior de acuerdo con lo establecido en la declaración de aplicabilidad vigente.

DEFINICIONES

- 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[1].
  Integridad: mantenimiento de la exactitud y completitud de la información[2].
  Disponibilidad: La información debe ser accesible y utilizable a demanda por una entidad autorizada. [3].

- Lineamientos de Seguridad de la Información: Conjunto de reglas y prácticas que regulan cómo en la CCC se maneja, protege, y distribuye su información, la de los empresarios y grupos de Interés.

- Normas de Seguridad de la Información: Enunciados detallados que establecen que es lo que se puede y no se puede hacer en términos de seguridad de la información (son de obligatorio cumplimiento, duran en el mediano plazo, desarrollan y detallan las políticas de seguridad de la información)

- Activo de información: Cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la entidad. Ejemplos: Bases de datos, información física y digital, software, hardware, servicios de información, personas, servicios de telecomunicaciones, servicios de almacenamiento, imagen y reputación de la entidad[4].

- Transferencia de información: Traspaso de información de un activo de soporte a otro.

- Definiciones relacionadas con la protección de datos personales

[1] Tomado de NTC ISO/IEC 2700:2014.
[2] Ídem.
[3] Ídem.
[4] Ídem.

- Protección de datos de carácter personal: Es un derecho fundamental que tienen todas las personas naturales. Busca la protección de su intimidad y privacidad frente a una posible vulneración por el tratamiento indebido de datos personales capturados por un tercero.

  Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables[5].

  Datos Sensibles: Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.[6]

  Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento[7].

  Titular: Persona natural cuyos datos personales sean objeto de Tratamiento[8].

  Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos[9].

  Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

CONTENIDO

GENERALIDADES

Todas las políticas, procedimientos, lineamientos, directrices, etc., definidas en la CCC para la seguridad de la información, hacen parte de su Sistema de Gestión de Seguridad de la Información (SGSI), alineado con el estándar internacional ISO 27001:2013.

La implementación de los lineamientos y normas consagrados en este manual, será progresiva de acuerdo a la prioridad que se establezca una vez realizado el análisis de riesgo de los activos de información. Esta prioridad será definida por el Comité de Seguridad de la Información.

En este manual para efectos de fácil identificación, las normas No Implementadas se encuentran marcadas con (NI) y las que están en Proceso de Implementación con (PI).

1.1 CONTEXTO DE LA ENTIDAD

En el documento D-DE-0001, se detalla el contexto de la organización.

1.1.1 INTERFACES Y DEPENDENCIAS.

Basado en las partes interesadas identificadas por la CCC y descritas en el documento **D-DE-0001,** se identificaron las partes interesadas que son pertinentes al SGSI y definieron los requisitos en cuanto a seguridad de la información, lo cual queda establecido en el **D-AC-0002**

1.2 LIDERAZGO Y COMPROMISO

[5] Ley 1581 de 2012.
[6] Ídem
[7] Ídem.
[8] Ídem.
[9] Ídem.

1.2.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para la Cámara de Comercio de Cali, la información es un activo fundamental y estratégico para la Entidad, por tal motivo la seguridad de la información es un proceso integral, transversal y que genera valor a la entidad. Por lo anterior sus colaboradores internos y externos que en el ejercicio de sus labores tengan acceso, procesen o generen información deben seguir la normativa definida para la gestión segura de la información.

Al definir esta política, la Cámara de Comercio de Cali reafirma su compromiso por implementar y mejorar continuamente el SGSI, articulando sus procesos de manera eficaz y efectiva, a través de planes y programas que permitan mantener una adecuada gestión de riesgos, el cumplimiento de los requisitos legales y la vigencia de la normativa interna definida para Seguridad de la Información.

1.2.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información materializan y concretan la Política de Seguridad de la Información con propósitos alcanzables y tangibles para los procesos incluidos dentro del alcance del SGSI.

Para definir los objetivos de Seguridad de la Información se tiene en cuenta el entendimiento de la estrategia de la CCC.

Considerando lo anterior los objetivos de seguridad de la información están alineados con la política de seguridad de la información y el direccionameinto estrategico de la CCC, los cuales son:

- Proteger la información de las empresas, empresarios y profesionales independientes.
- Mantener la confidencialidad e integridad de la información creada, procesada o resguardada por los procesos de negocio.
- Tener disponible la información y los servicios que soportan los procesos de negocio de acuerdo con sus necesidades.
- Cumplir las disposiciones legales, regulatorias y contractuales relacionadas con la 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 de los procesos de negocio.
- Capacitar y concientizar a los colaboradores de la CCC en temas relacionados con la seguridad de la información.

1.2.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN CCC.

En el siguiente documento se describe la estructura organizacional de la seguridad de la información en cuanto a los roles y funciones de los diferentes actores del sistema

D-AC-0003- Estructura Organizacional de Seguridad de la Información

1.3 SOPORTE

1.3.1 RECURSOS

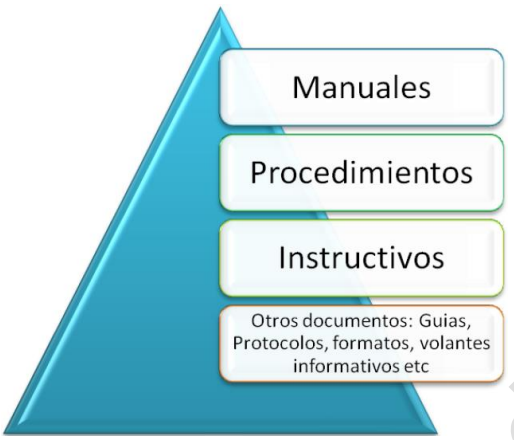
La CCC, a través del presupuesto aprobado por la Alta Dirección, asegura la provisión de recursos esenciales para implementar, operar, revisar, mantener y mejorar el SGSI. Los recursos asignados son personas, infraestructura y recursos financieros.

1.3.2 COMPETENCIAS, TOMA DE CONSCIENCIA Y COMUNICACIÓN

La CCC, con el objeto de contar con el personal competente, de acuerdo con los requerimientos de Seguridad de la Información, realiza charlas frecuentes y actualizadas con el objetivo de concientizar y capacitar a sus colaboradores.

1.3.3 INFORMACIÓN DOCUMENTADA

La documentación del Sistema de Gestión de la Seguridad de la Información se integra con el Sistema de Gestión de Calidad y se gestiona de acuerdo con los procedimientos ya establecidos; la documentación incluye los elementos que se detallan en la siguiente pirámide:



1.4 PLANIFICACIÓN Y OPERACIÓN

Como parte de la implementación del Sistema de Gestión de la Seguridad de la Información en la CCC, se utiliza el Procedimiento de Gestión de Riesgos Empresarial M-AC-0004, que permite:

- Definir las responsabilidades de la gestión de riesgos.
- Identificar y actualizar el contexto de la entidad.
- Identificar riesgos.
- Analizar riesgos.
- Valorar riesgos.
- Monitorear y revisar la gestión de riesgos.
- Comunicar y consultar sobre la gestión de riesgos.

1.5 EVALUACIÓN DEL DESEMPEÑO

1.5.1 INDICADORES

Para medir el desempeño del SGSI se definieron indicadores, los cuales se detallan en el documento **D-AC-0004 Indicadores del SGSI**

1.5.2 AUDITORÍAS

La CCC, realiza diferentes auditorías a sus sistemas de Gestión, estableciendo para ello un programa anual de auditorías, cumpliendo con los parámetros establecidos en las Normas ISO de cada uno de los Sistemas de Gestión de la CCC y/o estándares de la CCC.

La CCC cuenta con el procedimiento de **P-GC-0012 Auditorías Internas** en el cual se muestran los pasos a seguir en la planeación, ejecución y seguimiento de las auditorías internas de calidad.

1.5.3 REVISIÓN POR LA DIRECCIÓN.

La CCC realiza revisiones de seguimiento al SGSI a través de los comités de seguridad de la información.

Adicionalmente, se realiza una revisión general anual en el comité de mejoramiento en la revisión gerencial del Sistema de Gestión Empresarial, para determinar la idoneidad, suficiencia y eficacia continua del SGSI.

1.6 MEJORA

La CCC, ha establecido su SGSI como un modelo que le permita mejorarlo continuamente, para ello cuenta con el P-GC-0008 Acciones correctivas y de mejora, que permite tomar las acciones necesarias para eliminar las causas de las no conformidades reales o potenciales identificadas en el SGSI.

2. LINEAMIENTOS Y NORMAS DE SEGURIDAD DE LA INFORMACION

2.1 CUMPLIMIENTO Y SANCIONES

LINEAMIENTO

Todos los colaboradores de la CCC, terceros y demás usuarios de los servicios deben cumplir y acatar el manual de políticas en materia de protección y seguridad de la información.

NORMAS DE SEGURIDAD DE LA INFORMACION

Todo incumplimiento de algún lineamiento de seguridad de la información por un colaborador, proveedor o contratista es causal para iniciar acciones disciplinarias o contractuales, las cuales de acuerdo con su gravedad puede derivar la terminación de la vinculación laboral del empleado y los contratistas y/o proveedores la terminación del contrato suscrito con la CCC.

2.2 CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

LINEAMIENTO

Todos los colaboradores y terceros de la Cámara de Comercio de Cali que accedan a las bases de datos del negocio, de los empresarios y grupos de Interés de la entidad, deben disponer de un medio de identificación y su acceso estar controlado a través de una identificación personal.

NORMAS DE SEGURIDAD DE LA INFORMACION

Códigos de Usuario únicos (PI)

Cada usuario tendrá asignado un único código de identificación para tener acceso a todas las plataformas y aplicaciones que utilice.

Uso personalizado de la identificación de Usuario (PI)

Los usuarios de los recursos de tecnología de la información no deberán compartir ni revelar su código de usuario, contraseña o cualquier otro mecanismo otorgado para su identificación o autenticación.

Identificación y autenticación de usuarios (PI)

Para el acceso a cualquier de los recursos de tecnología informática de la CCC mediante la red pública o privada se requerirá de un proceso de autenticación del usuario.

Creación, eliminación e inhabilitación de códigos de identificación de usuarios (PI)

Los responsables de las unidades de negocio deberán asegurar la correcta administración de los códigos de usuario y son los únicos autorizados para crear, eliminar o inhabilitar los mismos. Cuando un usuario se ausente por más de una semana de la entidad o no haya accedido a los sistemas por un periodo de tiempo de 30 días se deberá inhabilitar al igual cuando tenga más de 5 intentos fallidos de acceso por contraseña no válida.

Revisión de los derechos de acceso de usuarios (PI)

Los dueños de los activos de información deben realizar una revisión periódica a las cuentas de usuario existentes en los sistemas de información, de tal forma que únicamente permanezcan vigentes las que se encuentren asignadas a colaboradores que formen parte del proceso y correspondan con las funciones asignadas para su cargo.

Creación de las contraseñas (PI)

Todas las contraseñas deberán ser creadas de acuerdo con un estándar definido por la CCC. Deberá considerarse el uso de herramientas automáticas que aseguren el cumplimiento de este estándar de contraseñas.

Vigencia de las contraseñas (PI)

Las contraseñas usadas deberán ser cambiadas cada 30 días, el usuario deberá ser informado para que la cambie y se deberá llevar un registro histórico de los cambios para evitar su repetición en los últimos 6 meses.

Confidencialidad de las contraseñas (PI)

Las contraseñas o cualquier otro medio de autenticación son totalmente confidenciales y restringidos para el uso del usuario, deberán ser entregados garantizando su confidencialidad con la notificación respectiva que comprometa al usuario a protegerla.

Asignación de contraseñas (PI)

La entrega de las contraseñas a los colaboradores, proveedores y/o terceros deberá estar controlada por un proceso formal que tenga en cuenta los siguientes aspectos:

- Compromiso por escrito de los usuarios para mantener su confidencialidad.
- Asegurar que los usuarios acaten los estándares y políticas para la creación y el cambio de las contraseñas.
- Notificar de una manera segura las contraseñas iniciales a los usuarios, las cuales deberían ser cambiadas en su primer uso de forma obligatoria.
- Confirmar el recibo de las contraseñas por parte de los usuarios.

Cifrado de las contraseñas (PI)

Las contraseñas, sin importar el sistema, aplicación o dispositivo deberán ser almacenadas utilizando un algoritmo de cifrado y no se podrán almacenar en texto claro.

Bloqueo de contraseñas (PI)

Las contraseñas deberán ser deshabilitadas después de 5 (cinco) intentos fallidos. Este evento deberá ser tratado como un evento de seguridad.

Usuarios por defecto y/o privilegiados (PI)

A todos los usuarios que vienen por defecto con los sistemas operativos, bases de datos, productos y programas relacionados con las diferentes plataformas instaladas en la CCC se les deberá restringir su uso o deshabilitar en caso de no requerirlos.

Definición de Perfiles de Usuarios (PI)

Los permisos de acceso a los sistemas y bases de datos de los Empresarios y Grupos de Interés deberán ser creados en un grupo de usuarios (Roles y los permisos serán otorgados de acuerdo con estos grupos o roles). Los roles o grupos deberán estar conformados por individuos cuyas responsabilidades y actividades son equivalentes.

Perfiles de Auditoría (PI)

Se deberá contar con perfiles especiales para la función de auditoría. Los Auditores deberán tener perfiles de consulta de información y no podrán realizar modificaciones.

Usuarios Administradores (PI)

Los usuarios privilegiados como Administradores del Sistema o de las Bases de Datos de la Entidad, deberán estar autorizados por el Director de la unidad a la que corresponda.

Para la creación de usuarios con privilegios especiales se deben seguir los siguientes lineamientos:

a) Los privilegios especiales del sistema se otorgarán únicamente a los administradores del mismo o a los responsables de la seguridad de la información.
b) Las contraseñas de usuarios con privilegios deben ser actualizadas periódicamente por el administrador del sistema o el Gerente de Tecnología y Proceso inmediatamente después del retiro de un colaborador con dicho conocimiento.
d) Se debe definir un procedimiento de tratamiento y custodia unificado de las contraseñas de administración de toda la plataforma tecnológica de la CCC.

Acceso a bases de datos de producción (PI)

Los aplicativos deberán ser el único medio para acceder a los datos de la entidad. Esto incluye las interfaces autorizadas y que han sido construidas utilizando herramientas de integración.

Acceso a diferentes ambientes informáticos de la entidad (PI)

El personal que realiza funciones relacionadas con ambientes específicos (producción, desarrollo, pruebas) sus perfiles deberán limitarse al ambiente en que trabajen.

Acceso a código fuente de aplicaciones (PI)

El acceso al código fuente de la entidad debe ser restringido, se deben definir los tipos de perfiles de acceso de acuerdo con el rol que se desempeñe, con el fin de protegerlo de modificaciones no autorizadas.

Bloqueo de las estaciones de trabajo (PI)

Todas las estaciones de trabajo de los usuarios deberán tener activado el bloqueo automático de estación, el cual deberá activarse luego de un período de ausencia o inactividad de 3 minutos. Por otra parte, el escritorio del equipo de trabajo deberá estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea la suficiente y necesaria para la labor que se desempeña.

Gestión de medios removibles (PI)

Se deben establecer métodos de protección de los datos en dispositivos móviles Corporativos o al servicio de la entidad, con el fin de evitar el acceso no autorizado o divulgación de la información almacenada o procesada.

Conexiones Remotas (PI)

Los mecanismos de conexión remota y teletrabajo, serán otorgados al personal que debido a sus funciones y por cuestiones de movilidad propias de sus cargos, requiere acceder a los sistemas de información desde ubicaciones diferentes a su puesto de trabajo, esto incluye labores de soporte tecnológico, atención de requerimientos en horario fuera del laboral, etc.

Las conexiones que se realicen de forma remota a los sistemas de la entidad deben ser registradas en logs de auditoría que permitan su posterior revisión.

2.3 PROPIEDAD INTELECTUAL

LINEAMIENTO

La propiedad intelectual de los desarrollos de software, productos y servicios de la entidad deberán protegerse.

NORMAS DE SEGURIDAD DE LA INFORMACION

Asignación de Derechos de Propiedad Intelectual a la Cámara de Comercio de Cali (NI)

Todos los colaboradores y a los terceros que se les encargue el desarrollo de software, de patentes, invenciones u otra propiedad intelectual que ellos originen deberán conceder a la CCC los derechos exclusivos de sus productos y servicios como parte de sus actividades en el desarrollo normal del negocio.

Avisos de Propiedad Intelectual (PI)

Se deberán incluir avisos de derechos de propiedad intelectual en todos los productos, servicios y el software de propiedad de la entidad.

2.4 CONTINUIDAD DEL NEGOCIO

LINEAMIENTO

Todas los archivos de datos y las bases de datos criticas utilizadas por las Unidades de Negocio de la entidad, deberán contar con el respaldo necesario para recuperase en caso de imprevistos o ataques a la seguridad de la información.

NORMAS DE SEGURIDAD DE LA INFORMACION

Plan de recuperación de los servicios de tecnología informática (PI)

Todos los sistemas de información que soportan las funciones críticas de la entidad deberán tener un Plan de Recuperación de TI, que le permita a la entidad garantizar una respuesta efectiva y eficiente ante eventos de desastre o interrupciones mayores, deberán estar documentados, actualizados y deberán probarse por lo menos una vez al año y dejando evidencia del resultado de estas.

Plan de continuidad de proveedores críticos y/o terceros (NI)

Los proveedores y/o terceros que soportan funciones críticas del negocio deberán presentar a la entidad su plan de continuidad para garantizar que pueden prestar sus servicios, ante eventos de desastre o interrupciones mayores.

Respaldo de la información crítica

Toda la información contenida en los archivos y las bases de datos de la entidad, utilizadas por los colaboradores para el soporte de los procesos de negocio deberán estar debidamente respaldadas para garantizar su disponibilidad.

Se deben realizar ejercicios periódicos de restauración de copias de respaldo en ambientes controlados, de tal forma que permitan garantizar la disponibilidad de los medios de respaldo y de la información contenida en ellos, y minimizar la posibilidad de falla cuando se requiera realizar una restauración de dicha información.

Respaldo al software (PI)

Las copias de respaldo del software desarrollado por la entidad como el SIRP, deberán realizarse de forma completa de tal forma que se garantice su recuperación mediante comandos y procedimientos de restauración.

Custodia de los medios de respaldo de la información crítica

Los medios de respaldo que contienen la información crítica del negocio deberán ser almacenados en un lugar externo a la entidad que cumpla con los requerimientos de seguridad y conservación de los medios.

Pruebas de restauración de información crítica (NI)

Cada dos (2) meses se deberán realizar pruebas de restauración de la información crítica del negocio con base en los medios de respaldo existentes y su información debe ser verificada.

Continuidad de Seguridad de la Información (PI)

Se debe contar con un sistema de gestión de continuidad de negocio en el que se incluyan los aspectos relacionados con Seguridad de la Información, que permitan garantizar que se contará con niveles similares de protección para la información ante cualquier eventualidad. Con base en ello, se deben tener en cuenta los siguientes aspectos:

a) Planificación: dentro de la planificación de las estrategias de operación en escenarios de continuidad y/o contingencia, se deben incluir los requisitos de la política de seguridad de la información y sus respectivos procedimientos, con el objetivo de garantizar niveles similares de protección de la información en cualquier escenario.
b) Implementación: Contar con niveles similares de seguridad de la información definidos en operación normal, en escenario de operación adversos.
c) Verificación, revisión y evaluación: verificar como mínimo una vez al año, los controles de seguridad de la información, establecidos para la operación en escenarios de contingencia y/o continuidad, a fin de asegurar que son suficientes y eficaces ante cualquier escenario.

2.5 SEGURIDAD FISICA

LINEAMIENTO

Todas las áreas físicas del negocio deberán contar con el nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas. La información confidencial y restringida deberá mantenerse en lugares con acceso restringido cuando no es utilizada

NORMAS DE SEGURIDAD DE LA INFORMACION

Seguridad Física de áreas de Acceso Restringido

Deberán existir estrictos controles para el ingreso a: Archivo Central, Call center, Centros de datos, Centros de cableado y otras áreas que contienen activos críticos de información. Se deberá tener un registro del personal que ingresa.

Toda persona que ingresa a algún área restringida de la entidad se compromete a dar cumplimiento a los registros y procedimientos de control establecidos.

Seguridad en los centros de cómputo (PI)

Para conservación de medios de almacenamiento, equipos de telecomunicaciones, computadores, servidores, y elementos tecnológicos en general, se requiere cumplir con estándares de seguridad y adecuación a centros de cómputo como:

a) Los recursos disponibles en el centro de cómputo principal y alterno deben ser los adecuados para soportar la operación de la CCC.
b) Suministro de materiales no combustibles y pisos falsos.
c) Contar con instrumentos capaces de registrar condiciones de humedad y temperatura, las cuales deben ser supervisadas diariamente por los Operadores de Centro de Cómputo o la persona que se designe para esta función.
d) Los detectores deben ser probados de acuerdo con las recomendaciones del fabricante o al menos una vez cada 6 meses. Estas pruebas deben estar previstas en los procedimientos de mantenimiento y control.
e) Se debe contar con un monitoreo permanente de los centros de datos y sus condiciones ambientales.
f) Sistema de refrigeración por aire acondicionado.
g) Contar con una planta de generación de energía, y UPS´s que proporcionen tiempos de respaldo adecuados, con el fin de garantizar el servicio de energía eléctrica en cualquier momento.
h) Evitar la permanencia de papelería, madera y materiales que representen riesgo de propagación de fuego.

i) Contar con extintores de incendios debidamente probados, con capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

Seguridad en el cableado (PI)

El cableado de energía y de las telecomunicaciones debe ser protegido contra la interceptación o daño. Se deben considerar los siguientes lineamientos para el cableado:

- Las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información, en lo posible deben ser subterráneas o deben estar sujetas a una alternativa de protección adecuada.
- El cableado de la red de comunicaciones debe estar protegido contra interceptaciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar la interferencia sobre las comunicaciones.
- Se deben utilizar estándares para la identificación y etiquetado de cables y equipos con el fin de minimizar errores en la manipulación, como un empalme accidental de los cables de red equivocados.
- Se debe mantener documentación actualizada de las conexiones de red.

Mantenimiento de los equipos(PI)

Los equipos deben recibir un mantenimiento adecuado de acuerdo con las directrices estipuladas por los fabricantes.

La CCC, hará uso de la garantía de los equipos, en caso de falla por parte de estos, asegurándose de obtener un servicio 7 x 24 por parte del fabricante o proveedor.

Se deben considerar los siguientes lineamientos para el mantenimiento de los equipos:

- Sólo el personal autorizado puede llevar a cabo las reparaciones y el mantenimiento de los equipos.
- Se deben mantener registros de todas las fallas y todo mantenimiento preventivo y correctivo.
- Se deben implementar los controles adecuados para el mantenimiento y protección de la información confidencial, teniendo en cuenta si dicho mantenimiento es realizado localmente o fuera de las instalaciones de la CCC.

Uso de los equipos de seguridad ambiental (PI)

La totalidad de los colaboradores que trabajen en el Call Center y Centros de Cómputo de la entidad deberán estar capacitados sobre el uso de los equipos de control ambiental. El conocimiento se deberá reforzar periódicamente.

Respaldo para el suministro de energía

Las áreas de atención al cliente, centro de cómputo, centros de cableado, de procesamiento de información crítica y en general las indispensables para la operación del negocio deberán contar con suministro de energía de respaldo con autonomía mínima de 8 horas.

Acceso de visitantes a áreas de acceso restringido

Para las áreas restringidas, únicamente el personal de la entidad formalmente autorizado podrá accederlas en función de las actividades que realiza. En el caso de que colaboradores de otras áreas y/o de entes externos a la entidad requieran ingresar, deberán obtener la autorización correspondiente y estar siempre acompañado de un colaborador autorizado.

se requiere cumplimiento de las siguientes disposiciones por parte de colaboradores y contratistas:

- Portar escarapela visible que los identifique. Adicionalmente cuando requieran ingresar a áreas restringidas deben hacerlo en compañía de un colaborador de dicha área.

- Tener acceso únicamente a las áreas necesarias para el desarrollo de sus actividades.
- Mantener por un período de seis (06) meses el registro de acceso del personal autorizado y de ingresos, con el objeto de facilitar procesos de seguimiento.
- El personal de recepción debe confirmar por teléfono las visitas, a menos que se haya dado aviso previo por parte del colaborador que va a ser visitado.
- Abstenerse de utilizar equipos de grabación y comunicaciones como teléfonos celulares, cámaras, grabadoras sin previa autorización. Para la toma de fotografías o grabaciones de cualquier tipo, contar con la previa autorización.
- El registro de control de las visitas debe estar protegido para evitar que los visitantes puedan ver detalles de otras personas y estar en custodia del personal de seguridad o de recepción.

Obras Civiles en áreas de acceso restringido (PI)

Todos los cambios estructurales dentro de los lugares destinados para servicio al cliente de la Cámara de Comercio de Cali como son los Centros de Atención Empresarial (CAE), los Centros de Conciliación y Arbitraje y el procesamiento de los datos y/o almacenamiento de recursos de Tecnología de la Información deberán estar soportados por un análisis de riesgo con el fin de evaluar, antes de la ejecución de los trabajos, las posibles consecuencias sobre la seguridad física y de la información.

Consumo de alimentos y cigarrillos en áreas que contienen recursos informáticos (PI)

Está prohibido fumar y consumir alimentos en las áreas de acceso restringido que contienen recursos de Tecnología de la Información críticos de la entidad como: Centros de Cómputo, Call Center. Centros de Cableado, Centros de potencia.

Borrado seguro de información (PI)

Cualquier sistema de información o equipo de cómputo que sea dado de baja, trasladado o reutilizado, deberá contar con un proceso de borrado seguro. El proceso de borrado seguro consistirá en la destrucción de la información que reside en el equipo; la validación del proceso y de la prueba del proceso, procurando que ningún dato se deja en el equipo.

En caso de dar de baja el equipo, se debe realizar la destrucción física del medio de almacenamiento.

Seguridad física de los equipos Portátiles (PI)

- Es obligatorio asegurar los computadores portátiles en los puestos de trabajo mediante guayas.
- Los colaboradores deberán garantizar la seguridad física de los equipos portátiles cuando se encuentre fuera de las instalaciones. Podrán utilizar cable de seguridad u otras técnicas aprobadas por la Entidad.
- El colaborador que viaja con su equipo portátil no deberá registrar la computadora portátil como equipaje de carga. La computadora portátil deberá siempre llevarla como equipaje de mano.
- El empleado que viaja con su equipo portátil u otro equipo o información de la entidad, deberá ser cauteloso y mantener los artículos siempre con él.
- Cuando el portátil vaya en el carro del empleado este deberá ir en el baúl.
- No está permitido prestar el equipo a ninguna persona.
- Cifrado de información residente en el disco duro, en los casos que se requiera por el nivel de confidencialidad de la información almacenada.
- Para el ingreso o traslado de equipos del centro de cómputo, se debe solicitar autorización debidamente justificada por parte del Gerente de Tecnología y Procesos.

Ingreso y retiro de activos de información de terceros. (PI)

Ningún equipo de cómputo, dispositivo de almacenamiento o procesamiento de información ni software de uso personal está autorizado para ingresar, ser conectado, explorado o ejecutado dentro de la red y recursos de la CCC, sin previa validación del área de Seguridad física y autorización del área responsable por el tercero.

El personal de vigilancia de recepción debe verificar y registrar siempre las características de identificación del activo en el sistema empleado para registro de visitantes.

2.6 SEGURIDAD EN EL PERSONAL

LINEAMIENTO

La Cámara de Comercio de Cali se esforzará por proveer los mecanismos necesarios para asegurar que los colaboradores cumplan sus responsabilidades en seguridad de la información desde su ingreso hasta su retiro de la entidad

NORMAS DE SEGURIDAD DE LA INFORMACION

Cumplimiento de los lineamientos y normas de seguridad de la información (PI)

Es obligación de los colaboradores de la entidad, conocer, respetar, cumplir y hacer cumplir las políticas y normas de seguridad de la información contenidas en este documento. Por lo tanto, deberán hacer parte de los contratos de trabajo o en su defecto del reglamento interno de trabajo. Esta norma aplicará de igual forma para los empleados suministrados por las empresas de servicios temporales y los terceros que prestan servicios a la entidad.

Acuerdo de Confidencialidad con los Colaboradores (PI)

Todos los empleados, independiente del tipo de contrato, deberán firmar un acuerdo de confidencialidad de la información que deberá ser parte integral de contrato de trabajo.

Notificación de terminación o cambio de contrato (PI)

Cuando se presente un cambio o terminación en la relación laboral con un colaborador, Gestión Humana debe comunicar y cumplir las actividades necesarias para garantizar la finalización de la relación en términos de seguridad de la información (generación de Paz y Salvo), incluyendo el reporte a las áreas correspondientes sobre retiro o ajuste de los privilegios de acceso a los activos de información y contenedores, de forma inmediata al retiro o cambio.

Devolución de activos de información (PI)

Todos los activos de información provistos a los colaboradores, tales como equipos portátiles, tarjetas de identificación, software, datos, documentación, manuales etc., deberán ser entregados apropiadamente y de forma inmediata en el momento de la terminación del contrato.

Revisión de equipos (PI)

Cualquier equipo de cómputo o de comunicaciones proveído o utilizado por el colaborador para realizar las labores del negocio deberá ser examinado y toda la información interna recuperada o destruida del dispositivo antes del retiro del empleado de la entidad por la Gerencia de tecnología y procesos.

2.7 CAPACITACION Y CREACION DE CULTURA

LINEAMIENTOS

La CCC desarrollará periódicamente programas de capacitación y concientización para fortalecer la cultura de seguridad de la información en la entidad.

NORMAS DE SEGURIDAD DE LA INFORMACION

Programa de concientización (NI)

Se desarrollarán programas de concientización que enfaticen en la importancia del cumplimiento de los lineamientos de seguridad de la información y su contribución al logro de los objetivos del negocio, teniendo en cuenta los siguientes aspectos:

- En el proceso de inducción a nuevos colaboradores, se incluirá una charla de concienciación sobre los requisitos de seguridad de la información, responsabilidades legales, uso correcto de los servicios de procesamiento de información y procesos disciplinarios.
- Se adoptará un esquema para sensibilizar de forma continua a colaboradores y terceros para que conozcan los riesgos de seguridad de la información y sus obligaciones para proteger los activos de información.

Divulgación de los lineamientos y normas de seguridad de la información y sus modificaciones (NI)

Los lineamientos y normas de seguridad de la información se divulgarán cada tres (3) meses con el fin de reforzar en los colaboradores su conocimiento y cumplimiento.

Certificación de los Usuarios (NI)

Los colaboradores de la CCC, usuarios de los recursos de Tecnología de la Información, deberán certificar periódicamente su conocimiento con respecto a la seguridad de la información como parte del programa de concientización.

Medición de la efectividad del Programa de Concientización (NI)

Se deberán realizar evaluaciones anuales de los resultados del programa de toma de conciencia a fin de establecer su efectividad y obtener información que permita establecer ajustes y correctivos en su diseño y ejecución.

2.8 CONTRATOS CON TERCEROS

LINEAMIENTO

Los terceros que utilicen los servicios de información de la entidad deberán cumplir con las políticas de seguridad de la información establecidas.

NORMAS DE SEGURIDAD DE LA INFORMACION

Inclusión de cláusulas de seguridad en los contratos con entidades externas (NI)

Se deberán incluir las políticas y normas de seguridad de la información que apliquen a cada contrato de acuerdo ccon lo definido en el presente manual de forma mandatorio.

Inclusión de cláusulas de “derecho a auditar” en los contratos con entidades externas (NI)

Todos los contratos deberán incluir una cláusula de "derecho a auditar" asegurando que el personal de la CCC o representantes autorizados puedan evaluar física y lógicamente a los terceros.

Se deben realizar revisiones a los terceros críticos para la operación, por lo menos una vez al año o cada vez que presente un cambio considerado como crítico para la operación.

Propiedad del software desarrollado por terceros (NI)

La propiedad del software desarrollado por personal externo (ej., contratistas) deberá ser definido claramente en los acuerdos del contrato.

Gestión de seguridad de la información en la prestación de los servicios de proveedores PI)

Cuando se presente la adquisición de un producto o servicio, en el que el tercero tenga acceso a activos de información de la entidad, el líder del área contratante es responsable de que el tercero cumpla con las siguientes políticas:

a) Los terceros deben firmar un acuerdo de confidencialidad.

b) Los contratos en los cuales se transfiere la responsabilidad de la seguridad de la información a un tercero se deben especificar que el tercero asume la responsabilidad de brindar los mismos niveles de seguridad de la información que tiene la entidad.
c) Toda la información utilizada por los terceros, debe ser clasificada y administrada de acuerdo a los niveles confidencialidad establecidos por el SGSI de la CCC.

2.9 CONEXIÓN A REDES

LINEAMIENTOS

Todas las conexiones por medio de redes públicas (celular, Internet) o por acceso remoto deberán ser autenticadas para evitar que la información sea develada o alterada sin autorización.

NORMAS DE SEGURIDAD DE LA INFORMACION

Segregación de redes (PI)

Se deberán definir en la arquitectura de la red, zonas separadas que agrupen lógicamente los recursos de Tecnología de la Información de la CCC de acuerdo con la criticidad de los activos de información. El proceso de Registros Públicos deberá tener una red privada, al igual que deberá existir una red independiente para visitantes y usuarios de los puntos de autoservicio de la entidad. Así mismo se deberá:

a) Implementar mecanismos de control que permitan fortalecer la seguridad perimetral de la entidad.
b) Realizar un monitoreo preventivo y correctivo a los componentes de la infraestructura de red de la entidad.
c) Monitorear el cumplimiento de los niveles de servicio acordados en la gestión de los proveedores de servicios de redes.
d) Mantener actualizada en temas de seguridad la infraestructura tecnológica.
e) Llevar a cabo inspecciones a los sistemas de comunicación de aquellos terceros que administren activos de información, para verificar que la información se esté manejando con las normas de seguridad acordadas.

Uso de los Firewalls de la entidad como únicos puntos de acceso a redes externas (PI)

El Firewall será el único punto autorizado para el establecimiento de conexiones de cualquier recurso informático de la entidad con redes externas. En ninguna circunstancia se deberán establecer conexiones directas a redes externas por los colaboradores de la entidad o contratistas.

Controles de enrutamiento (PI)

Se deberá contar con mecanismos que controlen el enrutamiento en la red. El acceso a los recursos de Tecnología de la Información de la entidad desde redes externas o internas requerirá que se verifique y controle.

Acceso a redes inalámbricas de la entidad (PI)

El acceso a las redes inalámbricas de la entidad solo podrá ser autorizado por los Líderes de cada una de las Unidades de Negocio.

- Los terceros solo podrán tener acceso a la red inalámbrica de visitantes provista por la CCC

- Los colaboradores con permiso de acceder a los servicios internos de la entidad por la red inalámbrica solo lo podrán hacer desde equipo de propiedad de la entidad.

Acceso de tabletas y teléfonos móviles a la red de la entidad (NI)

El acceso a la red de la entidad por medio de tabletas y/o celulares personales deberá ser previamente autorizado por la dirección de cada unidad de negocio.

Acceso restringido a servicios de internet (PI)

El acceso de usuarios a los servicios de internet deberá ser autorizado por la dirección de cada unidad de negocio especificando los sitios (Irlos) permitidos de acuerdo con la naturaleza del cargo.

Acuerdos de servicio vía Internet (PI)

Solo con autorización expresa del representante Legal de la entidad, los usuarios podrán usar las conexiones de Internet para establecer nuevos o diferentes servicios en la nube.

Transferencia de información (PI)

Cualquier intercambio de información con terceros a través de algún medio de comunicación, debe cumplir los siguientes lineamientos:

a) Existencia de controles para la detección y protección contra códigos maliciosos.
b) Uso de técnicas de cifrado para la información que lo requiera de acuerdo con su nivel de confidencialidad.
c) Establecer acuerdos que regulen el intercambio de información.

2.10 USO DE LOS RECURSOS INFORMATICOS

LINEAMIENTO

Los recursos de Tecnología de la Información provistos por la CCC a sus colaboradores son para uso exclusivo del negocio

NORMAS DE SEGURIDAD DE LA INFORMACION

Uso y cuidado de los recursos de Tecnología de la Información (PI)

Es responsabilidad de los colaboradores de la CCC la conservación y uso correcto de los recursos de TI. Deberán ser utilizados únicamente para fines del negocio aprobados por la entidad y deberán someterse a todas las instrucciones técnicas que imparta el comité de seguridad. El producto del uso de dichos recursos de tecnología de la información será de propiedad de la entidad.

El uso adecuado de los recursos de tecnología de información deberá hacerse bajo las siguientes condiciones:

- La instalación de cualquier tipo de software en los equipos de cómputo de la CCC será responsabilidad de la Gerencia de tecnología y procesos y, por lo tanto, son los únicos que definirán el personal autorizado para realizar esta labor.

- Los usuarios no deberán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios podrán realizarlos únicamente por el área de tecnología y procesos o quien esta designe.

- La información de carácter confidencial no deberá ser divulgada por medio de los recursos de telefonía de la CCC y los colaboradores deberán tomar precauciones para discutir información propia del negocio en ambientes donde esta puede ser escuchada por una tercera persona no autorizada.
- El uso de recursos para impresión, fotocopia, transmisión y recepción de fax deberán contar con un responsable y asignación de claves por área, con el fin de controlar el uso de estos.

- Los equipos de impresión deberán ser protegidos y depurados periódicamente, para evitar que se generen copias no autorizadas de la información que queda guardada en estos, poniendo en riesgo la información de la entidad y de las personas.

- Está prohibido el almacenamiento en los equipos de la entidad de música, juegos, software sin licencia, fotos y/o material con contenido pornográfico u ofensivo.

- En caso de que un usuario o cualquier tercero detecte o sospeche sobre la existencia de una posible debilidad de control de algún sistema de información o plataforma tecnológica, deberá reportarlo inmediatamente al coordinador de seguridad y por ningún motivo deberá intentar probar o explotar dicha debilidad.
- En ninguna circunstancia los equipos o dispositivos podrán ser dejados desatendidos en lugares públicos o a la vista en el caso que esté siendo transportado en un vehículo (propio transporte público).

- En caso de pérdida o robo de un equipo de La CCC, se deberá reportar como un incidente de seguridad de la información y se deberá poner la denuncia ante la autoridad competente.

Restricción en el uso de privilegios (PI)

Está prohibido intentar sobrepasar los controles de seguridad de los recursos de TI, buscar vulnerabilidades de seguridad y/o examinar los recursos de Tecnología de la Información en busca de información, sin autorización expresa. Los usuarios solo deberán ingresar a las funciones u opciones de lo aplicativos inherentes a su cargo.

Apagado de Equipos de Cómputo (PI)

Con fin de proteger la seguridad y distribuir bien los recursos de la entidad, el responsable del equipo de cómputo deberá asegurarse de apagarlo en las noches, fines de semana y festivos y en general cuando el equipo se encuentre fuera de uso.

Uso de Internet (PI)

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deberán ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas.

Prohibición a la explotación de vulnerabilidades de los recursos de informática (NI).

Los usuarios no deben explotar las deficiencias de seguridad para dañar los sistemas o la información contenida en ellos, obtener acceso a los recursos a los cuales no se le ha dado acceso. En caso de encontrar vulnerabilidades estas deberán ser reportadas al Coordinador de seguridad de la información.

Configuración del sistema operativo de las estaciones de trabajo (PI)

Solamente los colaboradores de la Gerencia de tecnología y procesos estarán autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

Entrega de bases de datos a terceros (NI)

Está prohibida la entrega de las bases de datos de la entidad a proveedores, contratistas y en general a terceras personas para efectos de revisión, pruebas o verificación de datos. En caso de ser necesario que terceras partes requieran las bases de datos, la Gerencia de Tecnología y Procesos de la CCC deberá proporcionar una forma segura mantenimiento los lineamientos de seguridad de la información establecidos en el presente manual.

2.11 CÓDIGO MALICIOSO

LINEAMIENTO

Todos los documentos electrónicos que ingresen a la entidad deberán ser revisados como medida preventiva de código malicioso por el funcionario de la entidad que recibe le documento.

NORMAS DE SEGURIDAD DE LA INFORMACION

Análisis de archivos (PI)

Los archivos adjuntos al correo electrónico y todos los archivos descargados de Internet deberán ser analizados antes de su ejecución. Medios de almacenamiento externos electrónicos y ópticos (Discos duros extraíbles, CD, DVD, memorias USB, etc.) que han estado fuera de control del usuario se deberán ser analizados antes de su uso por parte del funcionario de la entidad que está manipulando el archivo.

Software Antivirus

El software provisto para la revisión y protección de virus se deberá habilitar en todas las estaciones de trabajo y deberá actualizarse en línea desde el servidor de antivirus. Es responsabilidad del usuario garantizar que el proceso se lleve a cabo en sus estaciones de trabajo asignados. Si el usuario tiene alguna razón de creer que el proceso no está funcionando correctamente, deberá comunicarse con el área de tecnología y procesos inmediatamente.

2.12 GESTIÓN DE ACTIVOS

LINEAMIENTO

La entidad procurará proteger la información que produce y recibe de acuerdo con los lineamientos y normas establecidos en el presente documento y en instrumentos complementarios que regulen la materia.

NORMAS DE SEGURIDAD DE LA INFORMACION

Clasificación del activo de información (NI)

Las unidades de negocio responsables de la información son quienes deberán realizar la definición de la clasificación del activo de información (Eje. Confidencial, uso del negocio, pública), teniendo en cuenta criterios de evaluación relevantes para el negocio y posteriormente poder realizar una evaluación de riesgos e implementación de controles para los activos de información y contenedores respectivos.

La clasificación de la información se realizará con el objeto de establecer los niveles de protección adecuados y medidas de control procedentes, de acuerdo con su valoración.

La clasificación de la información se realiza considerando las tres propiedades de la información (Confidencialidad, Integridad y Disponibilidad) lo cual le da una clasificación a la información según el nivel de sensibilidad (Impacto de la perdida de la propiedad) de cada propiedad.

Protección de la información (PI)

La información de la entidad en cualquier formato (ej., impresa, disco, cinta) deberá ser protegida por todos los colaboradores, contratistas y proveedores de acuerdo con su valor, según lo definido por su clasificación.

Rotulación de la información (NI)

La información clasificada como confidencial o sensible deberá ser rotulada con la clasificación de la información definida para dicho documento.

Eliminación segura (PI)

Para la destrucción de documentación física sensible se deben utilizar máquinas destructoras de papel, teniendo en cuenta los tiempos de retención documental.

Medios físicos en tránsito (PI)

El transito físico de información debe realizarse con las medidas de protección que garanticen que no va a ser extraviada, duplicada o destruida.

La información que físicamente deba ser movilizada, debe estar debidamente identificada, marcada y clasificada.

Dos usuarios requeridos para todos los administradores (PI)

Los usuarios administradores de los sistemas deberán tener dos identificaciones de usuarios: Uno con privilegios de administración y otro con privilegios de usuarios normal.

Revisión regular de los registros del sistema (NI)

La Gerencia de Tecnología y Procesos deberá revisar mensualmente los registros y logs de cada uno de los sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad de la información. De igual forma los usuarios responsables de los procesos deberán revisar de forma mensual los registros y logs de sus aplicaciones.

Software de identificación de vulnerabilidades (NI)

Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información de la entidad. Una vez se obtenga dicha información, se deben tomar las medidas apropiadas para mitigarlas.

El análisis de vulnerabilidades debe ser planificado, a fin de reducir la posibilidad de interrupciones en la prestación del servicio.

Mantenimiento preventivo de equipos de cómputo, sistema de redes y telecomunicaciones, sistemas de control ambiental y sistemas de potencia, equipos de monitoreo, control de acceso (PI)

Se deberá realizar mantenimiento preventivo regularmente a todos los equipos, software y sistemas que usa la CCC como control para procurar que el riesgo de falla se mantenga en un nivel bajo. Esta norma aplicará de igual forma para los equipos ubicados en el centro alterno.

Habilitación de Logs en sistemas y aplicaciones (PI)

Se deberá habilitar la gestión de logs (registro de transacciones) en los sistemas y aplicaciones críticas de la CCC. Los registros de auditoría deben incluir:

- Autenticación en los sistemas identificando las cuentas de usuario utilizadas.
- Fechas, horas y detalles de eventos claves.
- Intentos de acceso fallidos y rechazados al sistema.
- Cambios en la configuración del sistema.

Monitoreo de sistemas (PI)

Se deberá realizar monitoreo a los sistemas críticos para identificar de manera proactiva el mal funcionamiento de los sistemas.

Sincronización de relojes (PI)

Los relojes de todos los sistemas de procesamiento de información dentro de la entidad se deben sincronizar con respecto a una única fuente de referencia. Esta sincronización se debe realizar, cuando menos, una vez al día.

Mantenimiento de los sistemas

Se deberá realizar periódicamente el mantenimiento a las bases de datos, antivirus, sistemas de correo y servicios informáticos en general de la entidad.

Gestión de cambios (PI)

Se deben controlar los cambios realizados a los sistemas de procesamiento de información, de forma que se garantice la integridad en la plataforma tecnológica:

- La documentación de los cambios, debe contemplar las actividades previas, durante el cambio, posteriores y las propuestas en caso de regreso del cambio (Rollback).

- Los cambios deberán considerar los impactos que generen al Plan de Recuperación de Desastres y/o de Continuidad de Negocio definido.

Gestión de capacidad (PI)

Tecnología y Procesos, área responsable de la administración de la plataforma tecnológica de la CCC, deberá implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación, conforme lo establecido en el procedimiento gestión de la capacidad.

Verificación física de los equipos críticos (PI)

Se deberá verificar periódicamente el estado físico de los equipos de cómputo críticos incluyendo los ubicados en el centro alterno.

Revisión de acceso de usuarios (PI)

La Unidad de Aseguramiento Corporativo deberá revisar los accesos de los usuarios a las aplicaciones críticas, por lo menos dos veces al año.

Inventario de conexiones externas (PI)

Se deberá mantener un registro de conexiones a las redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la entidad.

Reporte de pérdida o robo de identificación (PI)

Todo empleado deberá reportar a la mayor brevedad posible cualquier sospecha de pérdida o robo de carné de identificación o tarjeta de acceso físico a las instalaciones.

2.13 TRABAJO EN ÁREAS SEGURAS

LINEAMIENTOS

Las áreas de la entidad clasificadas como seguras deberán estar protegidas.

NORMAS DE SEGURIDAD DE LA INFORMACION

Acceso a áreas seguras (PI)

Cualquier acceso autorizado a terceros a un área segura deberá ser controlado y supervisado. Todos los proveedores con acceso al área segura deberán ser autorizados y registrados; esto incluye servicios de ayuda como limpieza o eliminación de desechos. Equipos de grabación como cámaras fotográficas, vídeo y audio no se permitirán dentro de un área segura a menos que sea autorizado específicamente por el Director de una unidad de negocio.

Acceso no autorizado (PI)

Todos los puntos de entrega de correo físico (entrante y saliente), las fotocopiadoras y las máquinas de fax deberán ser protegidas frente al acceso no autorizado. Se deberá prestar especial cuidado durante horas no laborales, para protegerlas contra el uso incorrecto de estos recursos.

Protección de información (PI)

Los colaboradores deberán recoger todos los documentos impresos (impresoras, faxes, fotocopias) de forma oportuna. Las impresoras, faxes y fotocopiadoras en áreas de trabajo seguras deberán monitorearse regularmente (todos los días en horas no laborales) para saber si hay impresiones que no se recogieron. Los artículos deberán ser asegurados hasta que los dueños de los documentos están disponibles. Toda la información de negocio escrita en tableros deberá borrarse posterior a su uso.

2.14 DOCUMENTACION DE LOS SISTEMAS DE INFORMACION

LINEAMIENTOS

La documentación de los sistemas de información desarrollados en la entidad deberá ser protegida.

NORMAS DE SEGURIDAD DE LA INFORMACION

Acceso no autorizado (PI)

La documentación del sistema deberá ser controlada y protegida contra el acceso no autorizado. Se procurará minimizar el acceso a la documentación. La autorización deberá proveerse únicamente a los empleados o terceros que requieren el acceso para realizar sus funciones de trabajo.

2.15 VIRTUALIZACION DE SERVICIOS

LINEAMIENTOS

Se propenderá porque la exposición de servicios en internet sea segura, manteniendo el principio de confidencialidad, disponibilidad e integridad para la entidad, los empresarios y grupos de interés.

NORMAS DE SEGURIDAD DE LA INFORMACION

Control de acceso (PI)

Los servicios virtuales deberán cumplir con los lineamientos y normas de seguridad de la información estipulada en el capítulo 2.2 del presente manual.

Transmisión segura de información (PI)

La información que se transmite entre el usuario de la aplicación y los servidores de la entidad deberá viajar cifrada.

Todos los sitios web publicados deberán estar protegidos con un certificado digital para comunicación y autenticación segura a través de internet.

Registro de auditoria (PI)

Todas las transacciones que realicen los usuarios por los servicios virtuales deberán dejar registro de auditoría en las bases de datos de la entidad de tal forma que permita realizar la trazabilidad de las operaciones.

Requisitos básicos para desarrollo seguro

Para el desarrollo y mantenimiento de software, la entidad deberá cumplir con los siguientes requerimientos:

a) Mantener tres ambientes independientes: uno para el desarrollo, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción.
b) Contar con procedimientos y controles para el paso de programas a producción.
c) Manejar control de versiones de todas las aplicaciones.

Revelación de información (PI)

Toda la documentación producida en el desarrollo de las aplicaciones de los servicios virtuales como puede ser: La arquitectura, el diseño, configuración, rutas de acceso, nombres de servidores etc., deberá ser considerada altamente confidencial y por lo tanto deberá ser protegida.

Revisión al código fuente (PI)

Todo el código fuente de las aplicaciones de los servicios virtuales deberá ser revisado antes de su despliegue, especialmente para garantizar que no contenga código malicioso (malware), ni prácticas de desarrollo inseguras.

Testing de seguridad (PI)

Todo el código fuente de las aplicaciones de los servicios virtuales deberá pasar por un proceso de pruebas de seguridad antes de su despliegue, con el propósito de minimizar que la aplicación pueda ser forzada a realizar acciones que excedan la funcionalidad especificada.

Testing de stress (PI)

Las aplicaciones deberán someterse a un proceso de pruebas de stress simulando una carga alta de peticiones y manteniéndola durante un tiempo prolongado, así mismo se deberá simular tráfico en ráfagas

Topología de instalación de las aplicaciones (PI)

Todas las aplicaciones deberán instalarse en una red segmentada y/o una zona DMZ y en servidores con funciones separadas (Base de datos, Aplicaciones, Servidor Web), para los casos en que la tecnología de esas aplicaciones lo permitan.

Pruebas de penetración (PI)

Todos los activos de información involucrados en la prestación de los servicios virtuales se deberán someter a pruebas de penetración en lo posible cada seis (6) meses.

Datos de prueba

Cuando se necesite tomar copias de la información de las bases de datos de producción, para la realización de pruebas, se deberán establecer los controles necesarios para garantizar el acceso solamente a usuarios autorizados durante la ejecución de las pruebas.

Plan de continuidad del servicio (PI)

Todos los activos de información que soportan los servicios virtuales de la entidad deberán disponer de un plan de continuidad que garantice la prestación del servicio ante una falla temporal o definitiva.

El plan de continuidad deberá estar documentado, probado, contemplar el regreso a la normalidad de las operaciones y no deberá perder los controles de seguridad de la información requerida por el servicio.

Desarrollo contratado con terceros

Cuando se realice la contratación de desarrollo de software con terceros, es necesario contar los siguientes controles:

a) Los terceros deben cumplir con la metodología de desarrollo de software definida por la entidad.
b) Definir acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
c) Auditar la calidad del trabajo realizado.
d) Definir requisitos de seguridad del código.

2.16 CUMPLIMIENTO DE REQUISITOS LEGALES

LINEAMIENTOS

Se debe dar cumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad que aplique para la CCC.

NORMAS DE SEGURIDAD DE LA INFORMACION

Identificación de la legislación aplicable

Se deben definir mecanismos para identificar y realizar un monitoreo del cumplimiento de todas las regulaciones, requisitos, resoluciones y contratos que se encuentren vigentes y sean aplicables a la operación de la entidad, con el objetivo de dar cumplimiento de estas y evitar multas y/o sanciones respecto de un incumplimiento.

Derechos de propiedad intelectual

Se deben implementar medidas para garantizar que la entidad y sus colaboradores cumplan con derechos de propiedad intelectual, con el fin de proteger los productos que se desarrollan para la entidad.

Protección de los registros de la entidad

Los registros de información clasificados como confidencial, no pueden ser extraídos fuera de las instalaciones de la CCC, a no ser que exista una autorización escrita por parte del dueño del activo de información. Así mismo debe permanecer en custodia de acuerdo con lo estipulado por la normativa interna, las regulaciones y/o leyes vigentes que apliquen.

Cumplimiento de la política de seguridad de la información

Es responsabilidad de la Gerencia, así como de los líderes de las áreas y procesos, revisar con regularidad el cumplimiento de las políticas y procedimientos de información, así como de cualquier otro requisito de seguridad, dentro de la entidad y/o su área de responsabilidad.

2.17 TRATAMIENTO DE DATOS PERSONALES

LINEAMIENTOS

Los datos personales de los colaboradores, empresarios, usuarios, grupos de interés que no esté catalogada como pública deberá ser protegida, manteniendo el principio de confidencialidad, disponibilidad e integridad, dando cumplimiento a lo expresado en la ley estatutaria 1581 de 2012.

NORMAS DE SEGURIDAD DE LA INFORMACION

Tratamiento de datos personales (PI)

El tratamiento de los datos personales se regirá de acuerdo con los lineamientos del manual de políticas y procedimientos para el manejo de los datos personales y atención de consultas de la entidad.

Cifrado de Mensajes (NI)

Los mensajes de correo electrónico se deberán cifrar cuando su contenido incluya: Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

Buenas prácticas en el uso del correo electrónico corporativo relacionado con la protección de datos personales (PI)

- Revisar las direcciones electrónicas de los destinatarios, antes de enviar el mensaje.
- Cuando el colaborador reenvíe un correo electrónico, deberá eliminar las direcciones de los anteriores destinatarios para no difundir, de forma injustificada, direcciones de correo de terceros las cuales son consideradas datos de carácter personal.
- No incluir datos personales en el asunto.
- Utilizar el pie de firma un disclaimer de los mensajes de correo electrónico, de acuerdo con el modelo corporativo establecido, que incluye la cláusula de confidencialidad.

2.18 REDES SOCIALES

LINEAMIENTOS

El uso y publicación de información en las redes sociales deberá ser controlado de tal forma que no comprometa la seguridad de la información de la entidad.

NORMAS DE SEGURIDAD DE LA INFORMACION

Verificación de la URL del sitio WEB (PI)

Los usuarios de las redes sociales de la entidad deberán verificar que están ingresando al sitio correcto y que adicionalmente el sitio disponga de un certificado de autenticación seguro SLL (https://) lo que garantiza que la información se transmite de forma segura.

Seguimiento a enlaces (links) (PI)

No se permitirá que los colaboradores de la entidad ingresen a enlaces ajenos a las redes sociales autorizadas (seguimiento de enlaces) al igual que no podrán ejecutar ni descargar archivos enviados.

Revelación de Información (NI)

No se podrá publicar información en las redes sociales clasificada como confidencial.

Control de acceso (PI)

Solo los usuarios autorizados por la entidad podrán hacer uso de las redes sociales y deberán emplear contraseñas “fuertes” para su uso. Se procurará controlar el acceso restringido de forma automática a través de filtrado de contenido.

Opiniones personales en las redes sociales (PI)

Los colaboradores de la CCC que expresen sus opiniones personales en las redes sociales deberán especificar que: “la opinión es personal y en ningún caso representan los intereses de la Cámara de Comercio de Cali.”

2.19 GESTION DOCUMENTAL

LINEAMIENTOS

Cumplir con la normatividad archivística nacional y asegurar la adecuada producción, recepción, distribución, entidad, conservación, recuperación y consulta oportuna de los documentos de archivo independientemente del soporte en que se encuentren

NORMAS DE SEGURIDAD DE LA INFORMACION

Espacios e instalaciones físicas (PI)

La entidad deberá garantizar los espacios y las instalaciones físicas necesarias para la conservación de la información teniendo en cuenta las normas vigentes sobre la materia.

Retiro y/o traslado del personal (PI)

Los empleados de la entidad al retirarse de sus cargos y/o trasladarse, deberán entregar los documentos y archivos a su cargo debidamente organizados e inventariados.

Administración y control de la gestión documental y archivos (PI)

El control de la documentación y archivos de la CCC se regirá de acuerdo con los lineamientos del manual de gestión documental, el cual estará a cargo del comité de gestión documental de la entidad.

2.20 IDENTIFICACION BIOMETRICA

LINEAMIENTOS

Los activos de información relacionados con la integración de los servicios de la CCC, Confecamaras y la Registradora Nacional del estado civil deberán ser protegidos. Por lo tanto, los usuarios de la entidad del sistema de autenticación biométrica en línea deberán cumplir con los lineamientos de seguridad descritos en este manual.

NORMAS DE SEGURIDAD DE LA INFORMACION

Acuerdo de confidencialidad (NI)

Para el uso de los recursos tecnológicos la CCC, todo colaborador deberá firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación de las soluciones de autenticación biométrica en línea con su respectivo kit de hardware.

Uso de los recursos informáticos (PI)

El uso del computador personal y demás recursos informáticos por parte del colaborador o usuarios del sistema de autenticación biométrica en línea, deberá someterse a todas las instrucciones técnicas, que imparta el comité de seguridad.

Uso personal de los recursos (PI)

Los recursos informáticos de la CCC, dispuestos para la operación registral, solo deberán ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica en línea a los usuarios de la CCC. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la CCC. Cualquier otro uso estará sujeto a previa autorización de la Presidencia.

Traslado de los equipos debe ser autorizado (NI)

Ningún equipo de cómputo debe será reubicado o trasladado dentro o fuera de las instalaciones de la CCC sin previa autorización. Así mismo, ningún equipo de cómputo asignado en el kit de identificación biométrica podrá ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado. El traslado de los equipos deberá hacerse con las medidas de seguridad necesarias, por el personal de la Gerencia de Tecnología y Procesos asignado.

Identificación única para cada usuario

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (Usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y

confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. En caso del sistema de autenticación biométrica en línea, el acceso al sistema se realizará mediante un cotejo inicial entre el sistema biométrico y el sistema de la entidad, los colaboradores contarán con una identificación única personal y su respectiva contraseña asignada el área de tecnología y procesos de la CCC.

Usuarios autorizados (NI)

Solo podrán hacer uso del sistema de autenticación biométrica en línea aquellos usuarios autorizados por la Unidad de Registros Públicos y redes empresariales de la CCC, las direcciones IP asignadas deberá ser fijas y únicas y deben corresponder a las direcciones IP reportadas como autorizadas en la Registradora Nacional.

Direcciones IP Autorizadas (NI)

Solo se podrá hacer uso del sistema de autenticación biométrica en línea en la CCC desde las direcciones IP autorizadas y reportadas a la Registraduría Nacional, para la cual la Gerencia de Tecnología y procesos de la entidad realizará el control automatizado.

Certificado de Autenticidad de la Registraduría

El certificado de autenticidad emitido por la Registraduría se almacenará en forma electrónica en el expediente del empresario en el sistema de gestión documental de la CCC.

2.21 ENVÍO DE CORREOS DIRECTOS E-MAILING O FISICO

LINEAMIENTOS

El envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación solo podrán realizarlo personas o áreas autorizadas para tal efecto y sí previamente estas comunicaciones fueron solicitadas o expresamente autorizadas por los destinatarios de estas, con excepción de los datos contenidos en los registros públicos que no requieren autorización previa para su tratamiento

La información que se envíe o reciba por medio de mensajes electrónicos debe estar protegida:

a) Los mensajes de correo electrónico no deben utilizarse para crear, almacenar ni transmitir información de carácter hostil.
b) No está permitido el envío o transmisión de mensajes con archivos adjuntos o imágenes que atenten contra los derechos de autor o derechos de propiedad intelectual de terceros.
c) Cada colaborador es responsable por los mensajes que son enviados con su cuenta de correo electrónico corporativa.
d) No suscribirse con la cuenta de correo corporativa a listas de redes de ocio a menos que se requiera para el desarrollo de sus funciones.

NORMAS DE SEGURIDAD DE LA INFORMACION

Derecho de los destinatarios de dar de baja a las comunicaciones (PI)

Todos los e-mailing deberán enviarse de una dirección de correo electrónica de la CCC válida. En el correo se deberá indicar la dirección de correo electrónico en donde los destinatarios puedan ejercitar el derecho de dar de baja a estas comunicaciones.

Único destinatario

Los correos electrónicos que se envíen a más de un destinatario tendrán que enviarse individualmente, o con los destinatarios en la opción de CCO (Con Copia Oculta).

Plataforma tecnológica para los e-mailing.

El envío de comunicaciones por e-mailing solo se podrá realizar empleando la plataforma tecnológica o servicio autorizado por la Gerencia de Tecnología y Procesos de la CCC. Lo anterior

para proteger a la Entidad del riesgo de inclusión en listas negras de direcciones IP consideradas como generadoras de SPAM.

Base de datos de destinatarios (NI)

Las bases de datos que contiene la información de los destinatarios para el envío de los e- mailing deberán estar centralizadas manteniendo las políticas de seguridad de la información contenidas en este manual.

2.22 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

LINEAMIENTOS

Todos los colaboradores de la CCC, son responsables de reportar faltas, incumplimientos a las políticas de seguridad de la información como incidentes de seguridad de la información, así como eventos, actividades anómalas que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información.

NORMAS DE SEGURIDAD DE LA INFORMACION

Gestión de incidentes

Se debe implementar un procedimiento que permita gestionar adecuadamente los incidentes, eventos y debilidades de seguridad de la información, iniciando desde la identificación de estos, el reporte a los responsables y sus acciones a realizar, la solución, generación de lecciones aprendidas y el cierre del mismo.

Se deben tener en cuenta cuando menos las siguientes políticas y controles:

a. Todos los colaboradores, proveedores, terceros y en general, todos los terceros con relación contractual vigente y que en alguna medida tengan acceso a información de la entidad o de sus clientes, están en la obligación de reportar incidentes de seguridad de la información, que se identifiquen en la operación de la entidad y que puedan afectar la prestación de servicios.
b. Los incidentes descubiertos durante actividades de monitoreo deberán ser comunicados al dueño del activo de información y/o el administrador de recursos y registrado a través del proceso.
c. El Coordinador de Seguridad de la Información será la persona que recibirá y hará seguimiento a cualquier incidente de seguridad de la información.
d. De acuerdo con el tipo de incidente, en caso de requerirse levantamientos forenses, se debe contratar con terceros especializados en el tema.

	Revisó	Aprobó
Nombre	Diego Alejandro Romero / Andrés Messa	Luis Fernando Pérez
Cargo	Gerente de Aseguramiento Corporativo / Gerente de Tecnología y Procesos	Presidente
Fecha	Junio 1 de 2022	Junio 1 de 2022