INTRODUCCION

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.

Contenido

INTRODUCCION 1
1. PROPOSITO DEL MANUAL 7
1.1. OBJETIVO 7
1.2. ALCANCE 7
2. DEFINICIONES 7
2.1. Principios de la Seguridad de la Información 7
2.2. Lineamientos de Seguridad de la Información 7
2.3. Normas de Seguridad de la Información 8
2.4. Archivo de datos o Base de Datos 8
2.5. Datos Confidenciales Restringidos 8
2.6. Datos Confidenciales 8
2.7. Datos de Uso Interno 8
2.8. Datos Públicos 8
2.9. Dueño de la Información 8
2.10. Custodio del activo de información 8
2.11. Activo de información 9
2.12. Definiciones relacionadas con la protección de datos personales 9
3. POLITICA INTEGRAL DE SEGURIDAD DE LA INFORMACION 10
4. LINEAMIENTOS Y NORMAS DE SEGURIDAD DE LA INFORMACION 10
4.1. CUMPLIMIENTO Y SANCIONES 10
4.1.1. LINEAMIENTO 10
4.1.2. NORMAS DE SEGURIDAD DE LA INFORMACION 10
4.2. CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN 11
4.2.1. LINEAMIENTO 11
4.2.2. NORMAS DE SEGURIDAD DE LA INFORMACION 11
4.2.2.1. Códigos de Usuario únicos 11
4.2.2.2. Uso personalizado de la identificación de Usuario 11
4.2.2.3. Identificación y autenticación de usuarios 11
4.2.2.4. Creación, eliminación e inhabilitación de códigos de identificación de usuarios 11
4.2.2.5. Creación de las contraseñas 11
4.2.2.6. Vigencia de las contraseñas 11
4.2.2.7. Confidencialidad de las contraseñas 12
4.2.2.8. Asignación de contraseñas 12
4.2.2.9. Cifrado de las contraseñas 12
4.2.2.10. Bloqueo de contraseñas 12
4.2.2.11. Usuarios por defecto y/o privilegiados 12
4.2.2.12. Definición de Perfiles de Usuarios 12
4.2.2.13. Perfiles de Auditoría 12
4.2.2.14. Usuarios Administradores 12
4.2.2.15. Acceso a bases de datos de producción. 13
4.2.2.16. Acceso a diferentes ambientes informáticos de la entidad. 13
4.2.2.17. Bloqueo de las estaciones de trabajo 13
4.3. PROPIEDAD INTELECTUAL 13
4.3.1. LINEAMIENTO 13
4.3.2. NORMAS DE SEGURIDAD DE LA INFORMACION 13

4.3.2.1. Asignación de Derechos de Propiedad Intelectual a la Cámara de Comercio de Cali 13
4.3.2.2. Avisos de Propiedad Intelectual 13
4.4. CONTINUIDAD DEL NEGOCIO 14
4.4.1. LINEAMIENTO 14
4.4.2. NORMAS DE SEGURIDAD DE LA INFORMACION 14
4.4.2.1. Plan de recuperación de los servicios de tecnología informática 14
4.4.2.2. Plan de continuidad de proveedores críticos y/o terceros 14
4.4.2.3. Respaldo de la información crítica 14
4.4.2.4. Respaldo al software 14
4.4.2.5. Custodia de los medios de Respaldo de la información crítica 14
4.4.2.6. Pruebas de restauración de información crítica 14
4.5. SEGURIDAD FISICA 15
4.5.1. LINEAMIENTO 15
4.5.2. NORMAS DE SEGURIDAD DE LA INFORMACION 15
4.5.2.1. Seguridad Física de áreas de Acceso Restringido 15
4.5.2.2. Uso de los equipos de seguridad ambiental 15
4.5.2.3. Respaldo para el suministro de energía 15
4.5.2.4. Acceso de visitantes a áreas de acceso restringido 15
4.5.2.5. Obras Civiles en áreas de acceso restringido 15
4.5.2.6. Consumo de alimentos y cigarrillos en áreas que contienen recursos informáticos 16
4.5.2.7. Borrado seguro de información 16
4.5.2.8. Seguridad física de los equipos Portátiles 16
4.6. SEGURIDAD EN EL PERSONAL 16
4.6.1. LINEAMIENTO 16
4.6.2. NORMAS DE SEGURIDAD DE LA INFORMACION 16
4.6.2.1. Cumplimiento de los lineamientos y normas de seguridad de la información 16
4.6.2.2. Acuerdo de Confidencialidad con los Colaboradores 16
4.6.2.3. Reporte de incidentes de seguridad 17
4.6.2.4. Notificación de terminación de contrato. 17
4.6.2.5. Devolución de activos de información 17
4.6.2.6. Revisión de equipos 17
4.7. CAPACITACION Y CREACION DE CULTURA 17
4.7.1. LINEAMIENTOS 17
4.7.2. NORMAS DE SEGURIDAD DE LA INFORMACION 17
4.7.2.1. Programa de concientización 17
4.7.2.2. Divulgación de los lineamientos y normas de seguridad de la información y sus modificaciones 17
4.7.2.3. Certificación de los Usuarios 18
4.7.2.4. Medición de la efectividad del Programa de Concientización. 18
4.8. CONTRATOS CON TERCEROS 18
4.8.1. LINEAMIENTO 18
4.8.2. NORMAS DE SEGURIDAD DE LA INFORMACION 18
4.8.2.1. Inclusión de cláusulas de seguridad en los contratos con entidades externas 18
4.8.2.2. Inclusión de cláusulas de “derecho a auditar” en los contratos con entidades externas 18
4.8.2.3. Propiedad del software desarrollado por terceros 18
4.9. CONEXIÓN A REDES 18

4.9.1. LINEAMIENTOS 18
4.9.2. NORMAS DE SEGURIDAD DE LA INFORMACION 19
4.9.2.1. Segregación de redes 19
4.9.2.2. Uso de los Firewalls de la entidad como únicos puntos de acceso a redes externas 19
4.9.2.3. Controles de enrutamiento 19
4.9.2.4. Acceso a redes inalámbricas de la entidad 19
4.9.2.5. Acceso de tabletas y teléfonos móviles a la red de la entidad 19
4.9.2.6. Acceso restringido a servicios de internet 19
4.9.2.7. Acuerdos de servicio vía Internet 19
4.10. USO DE LOS RECURSOS INFORMATICOS 20
4.10.1. LINEAMIENTO 20
4.10.2. NORMAS DE SEGURIDAD DE LA INFORMACION 20
4.10.2.1. Uso y cuidado de los recursos de Tecnología de la Información 20
4.10.2.2. Restricción en el uso de privilegios 20
4.10.2.3. Uso del correo electrónico Corporativo 21
4.10.2.4. Apagado de Equipos de Cómputo. 21
4.10.2.5. Uso de Internet 22
4.10.2.6. Prohibición a la explotación de vulnerabilidades de los recursos de informática. 22
4.10.2.7. Configuración del sistema operativo de las estaciones de trabajo. 22
4.10.2.8. Entrega de Bases de Datos a Terceros. 22
4.11. CÓDIGO MALICIOSO 22
4.11.1. LINEAMIENTO 22
4.11.2. NORMAS DE SEGURIDAD DE LA INFORMACION 22
4.11.2.1. Análisis de archivos 22
4.11.2.2. Software Antivirus. 22
4.12. GESTIÓN DE ACTIVOS 23
4.12.1. LINEAMIENTO 23
4.12.2. NORMAS DE SEGURIDAD DE LA INFORMACION 23
4.12.2.1. Clasificación del activo de información 23
4.12.2.2. Protección de la información 23
4.12.2.3. Rotulación de la información 23
4.12.2.4. Eliminación segura 23
4.12.2.5. Dos usuarios requeridos para todos los administradores 23
4.12.2.6. Revisión regular de los registros del sistema 24
4.12.2.7. Software de identificación de vulnerabilidades 24
4.12.2.8. 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. 24
4.12.2.9. Habilitación de Logs en sistemas y aplicaciones 24
4.12.2.10. Monitoreo de sistemas 24
4.12.2.11. Mantenimiento de los sistemas 24
4.12.2.12. Verificación física de los equipos críticos. 24
4.12.2.13. Revisión de acceso de usuarios. 24
4.12.2.14. Inventario de conexiones externas. 24
4.12.2.15. Reporte de pérdida o robo de identificación 25
4.13. TRABAJO EN ÁREAS SEGURAS 25
4.13.1. LINEAMIENTOS 25
4.13.2. NORMAS DE SEGURIDAD DE LA INFORMACION 25
4.13.2.1. Acceso a áreas seguras 25

4.13.2.2. Acceso no autorizado 25
4.13.2.3. Protección de información 25
4.14. DOCUMENTACION DE LOS SISTEMAS DE INFORMACION 26
4.14.1. LINEAMIENTOS 26
4.14.2. NORMAS DE SEGURIDAD DE LA INFORMACION 26
4.14.2.1. Acceso no autorizado. 26
4.15. VIRTUALIZACION DE SERVICIOS 26
4.15.1. LINEAMIENTOS 26
4.15.2. NORMAS DE SEGURIDAD DE LA INFORMACION 26
4.15.2.1. Control de Acceso 26
4.15.2.2. Transmisión Segura de Información 26
4.15.2.3. Registro de Auditoria 26
4.15.2.4. Revelación de información 27
4.15.2.5. Revisión al código fuente 27
4.15.2.6. Testing de Seguridad 27
4.15.2.7. Testing de Stress 27
4.15.2.8. Topología de instalación de las aplicaciones 27
4.15.2.9. Pruebas de penetración 27
4.15.2.10. Plan de continuidad del servicio 28
4.16. TRATAMIENTO DE DATOS PERSONALES 28
4.16.1. LINEAMIENTOS 28
4.16.2. NORMAS DE SEGURIDAD DE LA INFORMACION 28
4.16.2.3. Tratamiento de datos personales 28
4.16.2.4. Cifrado de Mensajes 28
4.16.2.5. Buenas prácticas en el uso del correo electrónico Corporativo relacionado con la protección de datos personales 28
4.17. REDES SOCIALES 29
4.17.1. LINEAMIENTOS 29
4.17.2. NORMAS DE SEGURIDAD DE LA INFORMACION 29
4.17.2.1. Verificación de la URL del sitio WEB 29
4.17.2.2. Seguimiento a enlaces (links) 29
4.17.2.3. Revelación de Información 29
4.17.2.4. Control de acceso 29
4.17.2.5. Opiniones personales en las redes sociales 29
4.18. GESTION DOCUMENTAL 30
4.18.1. LINEAMIENTOS 30
4.18.2. NORMAS DE SEGURIDAD DE LA INFORMACION 30
4.18.2.1. Espacios e instalaciones físicas 30
4.18.2.2. Retiro y/o traslado del personal 30
4.18.2.3. Administración y control de la gestión documental y archivos 30
4.19. IDENTIFICACION BIOMETRICA 30
4.19.1. LINEAMIENTOS 30
4.19.2. NORMAS DE SEGURIDAD DE LA INFORMACION 30
4.19.2.1. Acuerdo de confidencialidad 30
4.19.2.2. Uso de los recursos informáticos 31
4.19.2.3. Uso personal de los recursos 31
4.19.2.4. Traslado de los equipos debe ser autorizado 31
4.19.2.5. Identificación única para cada usuario 31
4.19.2.6. Usuarios autorizados 31
4.19.2.7. Direcciones IP Autorizados 31
4.19.2.8. Certificado de Autenticidad de la Registraduría 31

4.20. ENVÍO DE CORREOS DIRECTOS E-MAILING O FISICO 32
4.20.1. LINEAMIENTOS 32
4.20.2. NORMAS DE SEGURIDAD DE LA INFORMACION 32
4.20.1.1. Derecho de los destinatarios de dar de baja a las comunicaciones. 32
4.20.1.2. Único destinatario 32
4.20.1.3. Plataforma tecnológica para los e-mailing. 32
4.20.1.4. Base de datos de destinatarios 32
4.21. COMITÉ DE SEGURIDAD DE LA INFORMACION 33
4.21.1. LINEAMIENTOS 33
4.21.2. FUNCIONES COMITÉ DE SEGURIDAD DE LA INFORMACION 33
4.22. COORDINADOR DE GESTION DE RIEGOS 33
4.22.1. LINEAMIENTOS 33
4.22.2. FUNCIONES DEL COORDINADOR DE GESTION DE RIESGOS 33
4.23. OFICIAL DE SEGURIDAD DE LA IFORMACION 35
4.23.1. LINEAMIENTO 35
4.23.2. FUNCIONES OFICIAL DE SEGURIDAD DE LA INFORMACION 35

1. PROPOSITO DEL MANUAL

Crear 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.

Dotar a la CCC, de una herramienta que le permita de manera clara y definida, dar cumplimiento a las políticas y normas relacionadas con la seguridad de la información.

1.1. OBJETIVO

Constituir los lineamientos y normas de seguridad de la información aprobados por el comité de seguridad de la información.

1.2. ALCANCE

Este manual se elaboró con base en los principios básicos de la Seguridad de la Información de acuerdo a la Norma ISO 27001-2013 y los consagrados en las leyes 1581 de 2012 y 1712 del 2014, 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.

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).

2. DEFINICIONES

2.1. Principios de la Seguridad de la Información

Confidencialidad: Velar por la privacidad de la información, haciéndola accesible únicamente a usuarios autorizados

Integridad: Garantizar que la información no ha sido alterada interna o externamente.

Disponibilidad: Garantizar que el sistema esté operativo y cuente con los mecanismos de respaldo necesarios para permitir la continuidad del negocio.

Auditabilidad: Garantizar que todas las transacciones incluidas las de seguridad de la información pueda ser auditada por los usuarios autorizados.

2.2. Lineamientos de Seguridad de la Información

Conjunto de reglas y prácticas que regulan como en la CCC se maneja, protege, y distribuye su información, la de los empresarios y grupos de Interés.

Sirven de guía general para los colaboradores en la toma de decisiones.

Establecen las directrices para el manejo seguro de la información, son de carácter general y por lo tanto están diseñadas para durar en el largo plazo.

2.3. Normas de Seguridad de la Información

Son enunciados más detallados que las políticas y establecen que es lo que se puede y no se puede hacer en términos de seguridad de la información.

- Son de obligatorio cumplimiento
- Diseñadas para durar en el mediano plazo
- Desarrollan y detallan las políticas de seguridad de la información

2.4. Archivo de datos o Base de Datos

Conjunto organizado de datos utilizados por los Sistemas de Información para el funcionamiento de sus aplicaciones y que son objeto de tratamiento por las diferentes Unidades de Negocio.

2.5. Datos Confidenciales Restringidos

Información sensible que puede ser conocida únicamente por cierto número de colaboradores de la CCC, los empresarios y grupos de interés.

2.6. Datos Confidenciales

Información sensible al interior de la CCC es para uso exclusivo de un grupo específico de colaboradores o área.

2.7. Datos de Uso Interno

Información disponible solo para colaboradores de la CCC, la cual en caso de ser revelada a terceros representa un bajo riesgo para el negocio.

2.8. Datos Públicos

Información no sensible que puede ser conocida tanto por el personal de la CCC como por terceros.

2.9. Dueño de la Información

Un individuo o Unidad Organizacional que maneja información del negocio de la Cámara de Comercio de Cali o de los empresarios y que, por tanto, tiene la responsabilidad de clasificar y tomar decisiones de control con respecto al uso de dicha información.

2.10. Custodio del activo de información

El custodio del activo es cualquier empleado, o tercero autorizado, que tiene la responsabilidad de salvaguardar, mantener, recuperar y soportar la información de la entidad.

2.11. Activo de información

Todo aquello que posea valor para la organización por lo tanto debe protegerse. 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.

2.12. Definiciones relacionadas con la protección de datos personales

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.

Datos de carácter personal: Se refiere a la información de las personas naturales (identificadas o identificables), relativa tanto a su identidad (nombre y apellidos, domicilio, filiación, etc.) como a su existencia y ocupaciones (estudios, trabajo, enfermedades, etc.)

Habeas Data: Es el derecho que todo titular de información tiene de conocer, actualizar, rectificar u oponerse a la información concerniente a sus datos personales.

Titular de los datos personales: Es la persona natural cuyos datos personales son objeto de tratamiento por parte de un tercero.

Responsable del tratamiento: Es quien decide sobre la finalidad, contenido y uso de los datos de carácter personal.

Encargado del tratamiento: Es quien manipula los datos de carácter personal, pero no decide cómo, ni con qué fin. Su trabajo es operativo y se hace con base a las indicaciones e instrucciones del responsable del tratamiento.

Consentimiento del titular: Es una manifestación de la voluntad, informada, libre e inequívoca, a través de la cual el titular de los datos de carácter personal acepta que un tercero utilice su información con fines comerciales.

Tratamiento de los datos: Como regla general se requiere el consentimiento por parte de titular de los datos personales para poder realizar cualquier tratamiento de sus datos.

Sistema de información: Conjunto de elementos orientados al tratamiento y administración de datos e información organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Tratamiento: Cualquier operación o procedimiento físicos o automatizados que permita captar, registrar, reproducir, conservar, organizar, modificar, transmitir los datos de carácter personal.

3. POLITICA INTEGRAL DE SEGURIDAD DE LA INFORMACION

Para la Cámara de Comercio de Cali, los activos de información que generan, procesan o resguardan los datos de los procesos de negocio, las bases de datos de los empresarios y grupos de Interés son de vital importancia para la entidad y como tal propenderá por su protección.

Es política de la CCC trabajar continuamente en proteger los activos de información contra todo tipo de amenazas tanto internas como externas, deliberadas o accidentales y procurará que se cumplan con los siguientes requisitos:

- Proteger la información de los empresarios.
- Mantener la integridad de la información creada, procesada o resguardada por los procesos de negocio
- Posibilitar la confidencialidad de la información.
- Tener disponible la información y los servicios que soportan los procesos de negocio de acuerdo a sus necesidades
- Cumplir las disposiciones legales, regulatorias y contractuales relacionadas con la seguridad de la información.

4. LINEAMIENTOS Y NORMAS DE SEGURIDAD DE LA INFORMACION

4.1. CUMPLIMIENTO Y SANCIONES

4.1.1. LINEAMIENTO

Todos los colaboradores de la CCC, los contratistas, proveedores y los usuarios de los servicios deben cumplir y acatar el manual de políticas en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento al comité de seguridad de la información.

4.1.2. 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 a su gravedad pueden derivar la terminación de la vinculación laboral del empleado y los contratistas y/o proveedores la terminación del contrato suscrito con la CCC.

4.2. CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

4.2.1. 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.

4.2.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.2.2.1. 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.

4.2.2.2. 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.

4.2.2.3. 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.

4.2.2.4. 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.

4.2.2.5. 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.

4.2.2.6. 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.

4.2.2.7. 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.

4.2.2.8. 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

4.2.2.9. Cifrado de las contraseñas (PI)

Las contraseñan deberán ser almacenadas utilizando un algoritmo de cifrado, no se podrán almacenar en texto claro.

4.2.2.10. Bloqueo de contraseñas (PI)

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

4.2.2.11. 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.

4.2.2.12. 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.

4.2.2.13. 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.

4.2.2.14. Usuarios Administradores (PI)

Los usuarios privilegiados como Administradores del Sistema o de las Bases de Datos de la compañía, de los empresarios y Grupos de Interés, deberán estar autorizados por el Director de la unidad de Negocio.

4.2.2.15. 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.

4.2.2.16. 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.

4.2.2.17. 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.

4.3. PROPIEDAD INTELECTUAL

4.3.1. LINEAMIENTO

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

4.3.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.3.2.1. 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.

4.3.2.2. 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.

4.4. CONTINUIDAD DEL NEGOCIO

4.4.1. 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.

4.4.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.4.2.1. 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 organización 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 las mismas.

4.4.2.2. 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

4.4.2.3. 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.

4.4.2.4. 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.

4.4.2.5. 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.

4.4.2.6. 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 ser verificada

4.5. SEGURIDAD FISICA

4.5.1. 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

4.5.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.5.2.1. Seguridad Física de áreas de Acceso Restringido

Deberán existir estrictos controles para el ingreso al Archivo Central, al 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.

4.5.2.2. 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.

4.5.2.3. 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.

4.5.2.4. 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 funcionario autorizado.

4.5.2.5. 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.

4.5.2.6. 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

4.5.2.7. Borrado seguro de información (PI)

Cualquier sistema de información o equipo de cómputo que sea dado de baja 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.

4.5.2.8. Seguridad física de los equipos Portátiles (PI)

- 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.
- 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.

4.6. SEGURIDAD EN EL PERSONAL

4.6.1. 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 institución

4.6.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.6.2.1. 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.

4.6.2.2. 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.

4.6.2.3. Reporte de incidentes de seguridad (NI)

Los empleados deberán reportar cualquier incidente, vulnerabilidad o riesgo potencial que afecte la seguridad de la información.

4.6.2.4. Notificación de terminación de contrato (PI)

La Gerencia de Gestión Humana deberá notificar de forma inmediata al Oficial de Seguridad de la Información sobre la terminación del contrato de algún colaborador. Se debe proveer paz y salvo posterior al bloqueo de los privilegios y accesos proveídos a su nombre y de la devolución de los activos de información.

4.6.2.5. 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.

4.6.2.6. 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.

4.7. CAPACITACION Y CREACION DE CULTURA

4.7.1. LINEAMIENTOS

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

4.7.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.7.2.1. 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

4.7.2.2. 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.

4.7.2.3. 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.

4.7.2.4. 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.

4.8. CONTRATOS CON TERCEROS

4.8.1. LINEAMIENTO

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

4.8.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.8.2.1. 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 a lo definido en el presente manual de forma mandatorio.

4.8.2.2. 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.

4.8.2.3. 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.

4.9. CONEXIÓN A REDES

4.9.1. 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

4.9.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.9.2.1. 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 a la criticidad de los activos de información. La unidad 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.

4.9.2.2. 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 institución con redes externas. Bajo ninguna circunstancia se deberán establecer conexiones directas a redes externas por los colaboradores de la entidad o contratistas.

4.9.2.3. 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.

4.9.2.4. 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.

4.9.2.5. 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.

4.9.2.6. 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 (URLs) permitidos de acuerdo a la naturaleza del cargo.

4.9.2.7. 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.

4.10. USO DE LOS RECURSOS INFORMATICOS

4.10.1. LINEAMIENTO

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

4.10.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.10.2.1. 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 los mismos.
- 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 oficial de seguridad y por ningún motivo deberá intentar probar o explotar dicha debilidad.
- Bajo 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 o 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.

4.10.2.2. 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.

4.10.2.3. Uso del correo electrónico Corporativo (PI)

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo diariamente. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos, personales, en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

En el caso de recibir un correo no deseado o no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al oficial de seguridad de la información.

No se podrá utilizar el correo electrónico facilitado por la CCC para actividades profesionales paralelas a las tareas encomendadas en el contrato de trabajo.
Las personas que lleguen a tener cuentas de correo electrónico innominadas no podrán en ningún momento ni por ningún motivo facilitar dichas direcciones para asuntos domésticos y/o personales.
No está permitido el uso de programas chat, acceso a redes sociales, uso mensajería instantánea u otras aplicaciones similares durante la jornada de trabajo, a menos que dichas redes o aplicaciones tengan relación con las funciones encomendadas. Los mensajes que formen parte de un procedimiento administrativo, u otros que se tengan que conservar, sólo se pueden eliminar de la cuenta de correo si previamente han sido debidamente archivados en la carpeta que corresponda para dicho fin.

El colaborador al cual se le asigne una cuenta de correo electrónico corporativo de la entidad es responsable de:

- Conservar el usuario y contraseña de acceso a su correo electrónico de forma secreta y segura, además de no facilitar en ningún momento esta información a terceros.
- No utilizar una contraseña poco segura o fácilmente deducible.
- No hacer uso de la opción de “guardar contraseña” que ofrecen las distintas aplicaciones con el fin de evitar introducirla de nuevo en cada conexión.
- Bloquear el acceso a la cuenta de correo y a su equipo en caso de que no esté presente en su puesto de trabajo.
- No seguir cadenas de mensajes.
- No abrir mensajes sospechosos. Comunicarlo de forma inmediata y directa al oficial de seguridad de la CCC.
- Comunicar todo problema que detecte en su correo electrónico al personal encargado que dispone la CCC para estos fines

4.10.2.4. 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.

4.10.2.5. 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.

4.10.2.6. 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 la ha dado acceso. En caso de encontrar vulnerabilidades estas deberán ser reportadas al oficial de seguridad de la información.

4.10.2.7. 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.

4.10.2.8. 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.

4.11. CÓDIGO MALICIOSO

4.11.1. 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.

4.11.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.11.2.1. 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 (diskettes, CDs, DVDs, 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.

4.11.2.2. 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.

4.12. GESTIÓN DE ACTIVOS

4.12.1. LINEAMIENTO

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

4.12.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.12.2.1. 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)

4.12.2.2. 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 a su valor, según lo definido por su clasificación.

4.12.2.3. 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.

4.12.2.4. Eliminación segura (NI)

Cualquier información electrónica eliminada de sistemas informáticos y documentos impresos desechados deberán ser destruidos de forma tal que se proteja la confidencialidad.

4.12.2.5. 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.

4.12.2.6. 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.

4.12.2.7. Software de identificación de vulnerabilidades (NI)

La CCC deberá disponer de un firewall que proporcione un software de IDS (Intrusión Detection System), detección de virus y bloqueo de correo no deseado, para hacer una administración proactiva de los incidentes de seguridad de la información.

4.12.2.8. 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.

4.12.2.9. 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.

4.12.2.10. Monitoreo de sistemas (PI)

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

4.12.2.11. 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.

4.12.2.12. 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.

4.12.2.13. 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.

4.12.2.14. 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 organización.

4.12.2.15. 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.

4.13. TRABAJO EN ÁREAS SEGURAS

4.13.1. LINEAMIENTOS

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

4.13.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.13.2.1. 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.

4.13.2.2. 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.

4.13.2.3. 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.

4.14. DOCUMENTACION DE LOS SISTEMAS DE INFORMACION

4.14.1. LINEAMIENTOS

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

4.14.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.14.2.1. 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.

4.15. VIRTUALIZACION DE SERVICIOS

4.15.1. 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

4.15.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.15.2.1. Control de acceso (PI)

Los servicios virtuales deberán cumplir con los lineamientos y normas de seguridad de la información estipulada en el capítulo 4.1 del presente manual.

4.15.2.2. Transmisión segura de información (PI)

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

Todos los sitios web publicados deberán estar protegidos con un certificado de autenticación y privacidad de alto grado SSL (Secure Socket Layer).

4.15.2.3. 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.

4.15.2.4. 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.

4.15.2.5. 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.

4.15.2.6. 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.

4.15.2.7. 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

4.15.2.8. 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.

4.15.2.9. 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.

4.15.2.10. 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.

4.16. TRATAMIENTO DE DATOS PERSONALES

4.16.1. 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.

4.16.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.16.2.3. 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.

4.16.2.4. 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.

4.16.2.5. 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.

4.17. REDES SOCIALES

4.17.1. 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.

4.17.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.17.2.1. 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.

4.17.2.2. 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.

4.17.2.3. Revelación de Información (NI)

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

4.17.2.4. 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.

4.17.2.5. 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.”

4.18. GESTION DOCUMENTAL

4.18.1. LINEAMIENTOS

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

4.18.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.18.2.1. 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.

4.18.2.2. 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.

4.18.2.3. 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.

4.19. IDENTIFICACION BIOMETRICA

4.19.1. LINEAMIENTOS

Los activos de información relacionados con la integración de los servicios de la CCC, Confecámaras y la Registraduría 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.

4.19.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.19.2.1. 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.

4.19.2.2. 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.

4.19.2.3. 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.

4.19.2.4. 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.

4.19.2.5. 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.

4.19.2.6. 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 Registraduría Nacional.

4.19.2.7. 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.

4.19.2.8. 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.

4.20. ENVÍO DE CORREOS DIRECTOS E-MAILING O FISICO

4.20.1. 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 las mismas, con excepción de los datos contenidos en los registros públicos que no requieren autorización previa para su tratamiento

4.20.2. NORMAS DE SEGURIDAD DE LA INFORMACION

4.20.1.1. 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.

4.20.1.2. 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).

4.20.1.3. 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.

4.20.1.4. 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.

4.21. COMITÉ DE SEGURIDAD DE LA INFORMACION

4.21.1. LINEAMIENTOS

La CCC constituye el Comité de Seguridad de la información, con el objeto de:

a) Apoyar y aprobar la definición de lineamientos de seguridad de la información definiendo estrategias claras que permitan su implementación
b)) Evaluar el plan de contingencia y redefinir su alcance en función del riesgo presentando propuestas integrales a la alta gerencia que permitan una mitigación en función de los recursos en el corto, mediano y largo plazo
c) Apoyar y liderar los proyectos de seguridad de la información

4.21.2. FUNCIONES COMITÉ DE SEGURIDAD DE LA INFORMACION

- Definir y monitorear la estrategia de seguridad de la información
- Definir los lineamientos en materia de seguridad de la información
- Apoyar y acompañar los proyectos orientados al fortalecimiento de la seguridad de la información
- Proponer las normas y procedimientos de seguridad de la información
- Evaluar las solicitudes de excepciones a las normas y procedimientos de seguridad de la información
- Evaluar y promover las inversiones en seguridad de la información
- Servir de escenario para la discusión y el consenso con respecto a los lineamientos de seguridad de la información
- Contribuir al cumplimiento de los lineamientos y demás normas que regulen el tratamiento de los datos personales
- Apoyar el cumplimiento de las recomendaciones relacionas con la seguridad de la información
- Velar por la difusión y conocimiento de los lineamientos, normas y procedimientos relacionados con la seguridad de la información dentro de la entidad
- Monitorear el plan de mitigación de riesgos de seguridad de la información
- Las demás que sean acordes con el objeto del comité

El comité de seguridad de la información se reunirá ordinariamente por los menos tres (3) veces al año y extraordinariamente cuando se requiera.

4.22. COORDINADOR DE GESTION DE RIEGOS (PI)

4.22.1. LINEAMIENTOS

La CCC designará un Coordinar de Gestión de Riegos para gestionar de forma integral los riesgos de la Entidad.

4.22.2. FUNCIONES DEL COORDINADOR DE GESTION DE RIESGOS

- Gestionar el Sistema de Seguridad de la Información (SGSI)
- Velar por el cumplimiento de los procesos de gestión de riesgo operativo, riesgo de continuidad y riesgo de seguridad de la información

- Establecer e implementar un plan de seguridad que permita controlar el entorno lógico y físico de la información estratégica de la entidad, teniendo en cuenta los criterios de confidencialidad, integridad, auditabilidad y disponibilidad.
- Asegurar la implantación, mejoras, mantenimiento, verificación y cumplimiento de las políticas de Seguridad de la información y los medios requeridos para lograrlo. Uno de estos medios es la realización de un Manual de Seguridad, del cual debe velar por su correcto desarrollo, mantenimiento e implantación. Adicionalmente, representará a la Cámara de Comercio de Cali interna y externamente en todo lo referente al tema de Seguridad de la Información.
- Participar en la definición de las normas y estándares de seguridad, capacitar a los colaboradores, y hacer seguimiento a su cumplimiento.
- Definir e implementar un procedimiento para clasificación de los activos de información y velar porque se realice una adecuada clasificación de la Información en la entidad, mediante la concientización de los dueños de información de la entidad y la actualización del programa de clasificación de la Información.
- Definir las normas y procedimientos para el uso de equipos de seguridad, conjuntamente con Seguridad Física, y realizar su capacitación al interior de la empresa.
- Establecer y apoyar a las áreas encargadas en la ejecución de un plan de Capacitación continuo que permita actualizar a los colaboradores en aspectos de seguridad de la información fortaleciendo la cultura sobre el tema (Toma de Conciencia).
- Efectuar estudios de análisis de riesgos en Seguridad de la Información para identificar oportunamente los eventos o situaciones de fallos en los accesos o en el manejo de la información presentados en la CCC, estableciendo planes de acción que incluyan controles para contrarrestarlos y reducir el riesgo a un nivel aceptable.
- Apoyar a la Gerencia de Aseguramiento Corporativo a liderar el Comité de Seguridad de la Información.
- Participar activamente en los proyectos informáticos de la entidad para proveerlos de las seguridades adecuadas, liderando los de Seguridad de la Información. (Coordinador y/o Analista).
- Coordinar con las áreas de TI y del negocio en general la elaboración, y mantenimiento de los planes de continuidad, de emergencia, contingencia, de respaldo y recuperación para las diferentes plataformas tecnológicas de la organización.
- Liderar el proceso de pruebas que se debe ejecutar periódicamente a los Planes de Continuidad, Emergencia, Contingencia y de Recuperación.
- Definir las directrices básicas de Seguridad de la Información para la descripción de los diferentes requerimientos en la adquisición y desarrollo de tecnología y software en la Cámara de Comercio de Cali
- Velar porque se realicen las pruebas de seguridad a los Sistemas de Información y participar en su ejecución.
- Responsable General del programa de manejo de incidentes de seguridad de la entidad. Investigar, documentar e informar a los propietarios de la información los incidentes de seguridad
- Planificar y coordinar las actividades de respuesta y tratamiento del incidente, notificando los eventos relevantes a los dueños de los Procesos y/o Información
- Aprobar la implantación de los controles establecidos, así como la estrategia de concientización asociada y sugerir los comentarios que se consideren pertinentes
- Coordinar el plan de pruebas de penetración y tomar las acciones necesarias cuando se presenten desvíos durante la ejecución de las pruebas, apoyar la evaluación del resultado de las pruebas y sugerir las modificaciones al Manual de Seguridad de la Información
- Realizar evaluación de los perfiles de acceso
- Responsable por aprobar el plan de revisión de uso de utilitarios de uso de comandos y utilitarios sensibles
- Elaborar, conjuntamente con el área de procesos, el procedimiento de generación y revocación de claves de encripción de datos y velar por su aplicación
- Apoyar al líder de Seguridad Física en el análisis de las áreas para su clasificación de acuerdo a la información que contienen

- Coordinar las actividades de identificación definición y diseño de alertas en el uso de los recursos de información
- Definir el plan de monitoreo del manual de seguridad la entidad considerando el cubrimiento a los recursos críticos y la adecuada revisión de los elementos incluidos en el Manual.
- Revisar los informes de Auditoría y asegurar la ejecución de todas las actividades relacionadas con la implantación de las recomendaciones generadas en el informe relacionadas con Seguridad.
- Responsable del análisis de riesgo del acceso remoto a los recursos informáticos de la entidad y definir en conjunto con el dueño de la información, la necesidad de mecanismos de Seguridad para proteger la Información, revisar y aprobar solución final
- Difundir y mantener actualizado el mecanismo para el uso de analizadores de protocolos y traces de información confidencial
- Aprobar la implantación del estándar de Seguridad establecido, así como de la estrategia de concientización asociada y de sugerir los comentarios que se consideren pertinentes
- Diseñar, Desarrollar, Implantar, Mantener y controlar el Modelo de Seguridad de la información de la Entidad

4.23. OFICIAL DE SEGURIDAD DE LA IFORMACION (PI)

4.23.1. LINEAMIENTO

La CCC designa un Oficial de Seguridad de la Información para implementar, controlar y mantener las políticas, normas, estándares, procedimientos, necesarios para preservar y proteger la confidencialidad, disponibilidad e integridad de la información. Este rol podrá ser desempeñado por una firma especializada en modalidad de outsourcing,

4.23.2. FUNCIONES OFICIAL DE SEGURIDAD DE LA INFORMACION

- Responsable por la correcta ejecución de los procedimientos relacionados con el manejo de Incidentes, en todas sus etapas.
- Liderar al grupo de investigación de incidentes aportando sus conocimientos específicos en el área de Seguridad y realizar el proceso de documentación general del proceso de investigación y de la evidencia recopilada. Responsable por la ejecución del procedimiento de tratamiento de evidencia y su adecuado manejo durante la investigación del incidente correspondiente (Cadena de Custodia).
- Evaluar la definición de perfiles de usuarios en las diferentes plataformas y sistemas de acuerdo con las necesidades de recursos establecidas y las funciones de los diferentes cargos.
- Contar con mecanismos de monitoreo con el fin de detectar oportunamente procedimientos inseguros para los Sistemas Operacionales, Aplicativos, Datos y Redes.
- Evaluar la definición de los requerimientos de respaldo y backup de la información almacenada en servidores y medios magnéticos requerida para garantizar la continuidad del negocio.
- Definir, configurar y mantener la base de datos de conocimiento de Seguridad de la Información y el archivo Físico de Seguridad de la Información
- Identificar el detalle de los requerimientos de encripción de la información y definir la solución
- Realizar las evaluaciones de riesgo de seguridad de la información con el apoyo del Coordinador

- Apoyar al dueño de la Información y al área de tecnología en la determinación de los requerimientos técnicos de protección, definición de la solución para su implementación y el plan de ejecución para las actividades relacionadas con la clasificación de la información
- Definir la solución de manejo de antivirus, mantenerse permanentemente actualizado en temas relacionados y liderar las acciones para la detección y erradicación de virus Informáticos en la entidad
- Definir los requerimientos de Seguridad para el manejo de los respaldos y recuperación de información crítica y confidencial.
- Apoyar al dueño de la Información en el análisis de riesgos y durante del proceso de elaboración del plan de Contingencia en cuanto a la validación e inclusión de los controles de Seguridad apropiados para la operación de la entidad ante un evento de Contingencia
- Coordinar el plan de pruebas de los planes de continuidad y contingencias
- Apoyar a los administradores del Sistema en la definición de eventos a registrar en lo relacionado con la seguridad y en la realización de revisión de logs y análisis de Riesgo. Solicitar la restauración de información de logs y eventos de los recursos informáticos para la realización de revisiones internas de su área
- Apoyar el dueño de la información en las definiciones de los requerimientos, identificar los eventos, fuentes y estrategia de filtrado de información y herramientas necesarias para la incorporación de los mecanismos de registro y control.
- Apoyar al Coordinador de Riesgo y trabajar bajo su coordinación en las actividades relacionadas con la implantación de las recomendaciones de la Auditoría. Facilitar la consecución de la información requerida por el Auditor para la realización de sus labores en la ejecución del procedimiento
- Canalizar los reportes del Help Desk relacionados con la Seguridad y ser el primer filtro en la catalogación de problemas candidatos a ser incidentes para su reporte al área de Seguridad. Apoyar al representante de Help Desk en el análisis de posibles incidentes de Seguridad en los incidentes reportados.
- Evaluar y prestar atención de primer Nivel al incidente de Virus, Notificar y enviar documentación relacionada al Coordinador de Riesgo.
- Realizar las actividades de monitoreo de acuerdo con el plan establecido en coordinación con el Coordinador de Riesgo y otras áreas de la entidad incluyendo planeación, ejecución y documentación. Iniciar la ejecución de los procedimientos para el tratamiento de los hallazgos del monitoreo documentando los resultados obtenidos
- Recolectar la información de los mecanismos de registro y control, monitorear la información resultante e identificar desviaciones.

	Revisó	Aprobó
Nombre	Carlos Eduardo Alarcon/ Andres Messa	Esteban Piedrahita Uribe
Firma		
Cargo	Gerente de Aseguramiento Corporativo/Gerente de Tecnología y Procesos	Presidente
Fecha	Enero 13 de 2016	Enero 13 de 2016