Prácticas en seguridad de la información

TABLA DE CONTENIDO

Prácticas en seguridad de la información

1. OBJETIVO

Dar a conocer las actividades que todos los colaboradores de la Cámara de Comercio de Bogotá y demás grupos de interés, deben realizar para garantizar el cumplimiento de la Política de Seguridad de la Información, la cual está apoyada en el siguiente conjunto de prácticas, las cuales se basan en la Norma ISO/IEC 27002.

2. ALCANCE

Este documento aplica a todos aquellos usuarios tanto internos como externos sin excepción, que posean algún tipo de acceso o sean responsables por los activos de información de la Cámara de Comercio de Bogotá (Dato, Documento, Sistema de Información, Sistema de Almacenamiento de Información, Software, o Dispositivo), dispuesto en cualquier formato ya sea de manera digital, impresa, en medio audiovisual o archivados de la Entidad. Los grupos de interés que cubren estas políticas se han clasificado en los siguientes niveles:

- Colaboradores de Planta: son aquellas personas que han suscrito un contrato laboral con la Entidad y pueden ser de dos tipos:

  - Colaboradores con contrato de trabajo a término fijo

  - Colaboradores con contrato de trabajo a término Indefinido.

- Contratistas: son aquellas personas que tienen alguna relación con la Entidad y que pueden estar formalizada a través de:

  - Empresas de Servicios Temporales: Trabajadores en Misión

  - Asociados a Entidades Cooperativas

  - Empleados por Outsourcing: son aquellas personas que están vinculadas directamente con una entidad prestadora de servicios que suministra servicios a la CCB. Entre estas personas y la CCB no hay vínculo laboral de ninguna especie.

  - Personas naturales y/o jurídicas que prestan servicios relacionados con las tecnologías de la información y las comunicaciones a la Entidad, y cuya relación

laboral con la CCB se formaliza a través de contratos de prestación de servicios y/o de consultoría.

- Empleados Fondo de Empleados de la Cámara de Comercio de Bogotá.
- Entidades de Control:

  - Revisoría Fiscal.

  - Contraloría General de la República.

  - Superintendencia de Industria y Comercio.
- Filiales
- Otras Entidades:

  - Confecámaras (RUES).

  - DataCrédito – Computec.

  - DIAN.

  - Secretaría de Hacienda.

  - Secretaría de Planeación Distrital.

3. GENERALIDADES

3.1. DEFINICIONES GENERALES EN MATERIA DE SEGURIDAD DE LA INFORMACION

Esta sección contiene algunas definiciones importantes en materia de seguridad de la información:

- **Acuerdo de seguridad de la información (INF-SPI-F-001):** Es un documento que debe suscribir todo usuario, o tercero con el objeto de garantizar un adecuado tratamiento y protección de la información, así como una aceptación de las políticas de seguridad de la información que rigen al interior de la organización.
- **Administradores:** Usuarios a quienes la CCB ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la CCB, quienes estarán bajo la dirección de la Vicepresidencia de Operaciones e Informática. Dentro de los cuales están:

Rol	Función
Administrador de Sistemas de Información	Responsable por el funcionamiento de las plataformas (sistemas operacionales)
Administrador de usuarios y perfiles	Responsable de la creación de los usuarios de la red (Internet/ Correo electrónico)
Administrador de comunicaciones y servicios Web	Responsable por los medios de comunicación de la organización (redes, y comunicación con las sedes)
Administrador Seguridad Informática	Responsable de la configuración de los componentes de seguridad (Firewall/Proxy, sistemas de detección de intrusos, sistemas antivirus)
Administrador de Seguridad de la Información	Responsable por el seguimiento y la gestión del sistema de gestión de seguridad de la información.

Prácticas en seguridad de la información

- **Backup:** Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.
- **Contraseña:** Clave de acceso a un recurso informático.
- **LAN:** Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).
- **Monitoreo:** Actividades de verificación de las acciones realizadas por un usuario en la utilización de los recursos tecnológicos, así como a la información que accede.
- **Protector de pantalla:** programa que se activa a voluntad del usuario, o automáticamente después de un tiempo en el que no ha habido actividad en el computador.
- **Recursos informáticos:** Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, impresoras, programas, sistemas de aplicaciones y sus datos.
- **Seguridad de Información:** Es el proceso de proteger la información contra cualquier tipo de amenaza, busca preservar la confidencialidad, integridad y disponibilidad, de igual manera busca contribuir a la continuidad del negocio, disminuir los posibles daños e impactos que puedan llegar a presentarse, sobre la información o cualquier componente tecnológico de la entidad.
- **Amenaza:** Una actividad ya sea intencional o no, que busque causar daño a un activo. Puede ser manipulada a través de una vulnerabilidad.
- **Vulnerabilidad:** Es una falla o debilidad que puede ser explotada, con el objetivo de causar daño a un activo. Se considera la forma de explotar una amenaza.
- **Sesión:** Conexión establecida por un usuario con un Sistema de Información.

Prácticas en seguridad de la información

- **Sistema de control de acceso:** Elementos de hardware y/o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas, roles y perfiles definidas.
- **Sistema operativo:** Software que controla los recursos de un computador.
- **Usuario:** Toda persona que basado en un rol y perfil pueda tener acceso a un recurso informático de la CCB.
- **Usuarios externos:** Son aquellos clientes externos que utilizan los recursos informáticos de la CCB a través de Internet ó de otros medios y tienen acceso únicamente a información que previamente este definida por el propietario, responsable o custodio de la misma.
- **Usuarios externos con contrato:** Usuarios externos con los cuales la CCB establece un contrato y a quienes se da acceso limitado a recursos informáticos de acuerdo a las necesidades o propósito de la relación contractual.
- **Hardware:** Conjunto de componente(s) físico(s) que componen un sistema de cómputo.
- **Software:** Conjunto de aplicaciones y/o programas que se encuentran funcionando en cualquier equipo computacional.
- **Incidente de seguridad de la información:** Es un evento que impacta negativamente a un sistema de información, a una red, o una inminente amenaza de violación de la política de seguridad, o una práctica de seguridad de la entidad.
- **Licencia de Software:** Es la autorización o permiso concedido por el dueño del programa al fabricante o distribuidor para utilizarlo de una forma determinada y de conformidad con una condición convenida. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración, y el entorno de aplicación.
- **Copyright:** Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de

expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.

- **Propiedad Intelectual:** Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.
- **Open Source (Fuente Abierta):** Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.
- **Software Libre:** Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
- **Software no autorizado:** Es una copia ilegal de software que son utilizados sin tener la licencia exigida por ley.
- **Software de Dominio Público:** Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
- **Freeware:** Software que se distribuye sin ningún costo, pero su código fuente no es entregado.
- **Shareware:** Clase de software o programa, que se distribuye durante un periodo de tiempo sin ningún costo, después del tiempo requiere de su pago para su funcionamiento de manera legal.
- **Hardening:** Proceso que debe ser aplicado por los administradores de sistemas a cualquier recurso computacional que busca optimizar el sistema operacional y/o aplicaciones instaladas, basado en las mejores prácticas que existan por los fabricantes.
- **Plan de evacuación:** Plan que permite evacuar cualquiera de las localidades de la Entidad en caso de un siniestro.

- **Seguridad física:** Es el proceso mediante el cual la CCB aplica sistemáticamente las políticas, procedimientos y prácticas con el fin de asegurar la seguridad física de toda la Entidad.
- **Sistema de control de acceso:** Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas. En el caso de la seguridad física este sistema administra las puertas de acceso.

3.2. SEGUIMIENTO Y MEDICIÓN

A través de los reportes que se entreguen al Comité de Seguridad de la Información, en caso de que sea necesario.

4. METODOLOGIA

La Norma ISO/IEC 27002 código de prácticas en Seguridad de la Información, son un conjunto de controles que la entidad ha decido implementar dentro de la organización, estos se encuentran divididos en 11 dominios de trabajo los cuales están definidos así:

Dominio	Propósito del Dominio	Rol Responsable
Política de Seguridad de la Información	□ Control de la organización a través de la(s) políticas de seguridad de la información □ Respaldo total de la dirección en pro de la protección y seguridad de la información □ Gestión de las políticas de seguridad de la información	Oficial de Seguridad de la Información Comité de Seguridad de la Información
Seguridad de la información organizacional	□ Manejo de la seguridad de la información a nivel interno y externo □ Gestión del proceso de seguridad de la información □ Grupo de coordinación de seguridad de la información □ Identificación y asignación de responsabilidades	Oficial de Seguridad de la Información Comité de Seguridad de la Información

Prácticas en seguridad de la información

Dominio	Propósito del Dominio	Rol Responsable
Gestión de Activos	□ Control apropiado de los activos de información de la organización □ Asegurar una debida protección de todos los activos de información de la organización □ Definición de roles y responsabilidades del mantenimiento y cuidado de los activos □ Guías de clasificación de la información	Oficial de Seguridad de la Información Comité de Seguridad de la Información
Seguridad del Recurso Humano	□ Control de riesgos asociados con el personal □ Roles y responsabilidades del personal □ Concientización y entrenamiento □ Procesos disciplinarios	Gerente de Recursos Humanos
Seguridad física y ambiental	□ Prevenir el acceso físico sin autorización, el daño y/o interferencia en el negocio □ Prevenir el robo o pérdida de información, en las instalaciones, que intervengan en las actividades de la organización	Jefe de Seguridad Física

Prácticas en seguridad de la información

Dominio	Propósito del Dominio	Rol Responsable
Gestión de Comunicaciones y Operaciones	□ Asegurar el correcto funcionamiento de los sistemas de procesamiento de información □ Minimizar los riesgos de falla de los sistemas □ Proteger la integridad del software y la información □ Mantener el nivel de seguridad con terceros □ Mantener la integridad y disponibilidad de la información □ Protección de la información en red □ Prevenir la divulgación no autorizada, modificación, o destrucción de los activos y las actividades del negocio □ Mantener la seguridad de la información y software intercambiado con otras organizaciones □ Seguridad en comercio electrónico □ Monitoreo	Jefe de Infraestructura Tecnológica
Control de Acceso	□ Control del acceso a la información □ Asegurar acceso autorizado y prevenir acceso no autorizado a los sistemas de información □ Prevenir acceso no autorizado a los servicios de red □ Prevenir el acceso no autorizado a los sistemas operacionales □ Aseguramiento y mantenimiento de la computación móvil o teletrabajo	Jefe de Infraestructura Tecnológica Jefe de Solución de Software

Prácticas en seguridad de la información

Dominio	Propósito del Dominio	Rol Responsable
Adquisición, desarrollo y mantenimiento de sistemas de información	□ Seguridad de la información como parte integral de los sistemas de información □ Prevenir errores, perdida modificación o abuso de los sistemas de información □ Proteger la confidencialidad, integridad y autenticidad de la información a través de controles criptográficos □ Asegurar la seguridad de los sistemas de archivos □ Mantener la seguridad de los sistemas de aplicaciones y la información □ Manejo de vulnerabilidades de los sistemas de información	Jefe de Solución de Software
Gestión de Incidentes	□ Manejar de manera adecuada los incidentes de seguridad y que las acciones sean ejecutadas □ Procedimientos para el manejo y gestión de los incidentes	Oficial de Seguridad de la Información Comité de Seguridad de la Información
Gestión de la Continuidad del Negocio	□ Prevenir la interrupción de las actividades del negocio □ Proteger los procesos críticos del negocio, frente a una emergencia o un desastre, y su recuperación	Comité de Seguridad de la Información
Cumplimiento	□ Garantizar el cumplimiento frente a leyes, legislación, estatutos , regulaciones y/u obligaciones contractuales □ Asegurar el cumplimiento del sistema con las políticas, procedimientos y estándares de la organización	Oficial de Seguridad de la Información Comité de Seguridad de la Información Contraloría Interna

Prácticas en seguridad de la información

A continuación se describen para cada uno de los dominios relacionada un conjunto de prácticas basadas en la norma ISO/IEC 27002:

4.1 POLITICA DE SEGURIDAD

- **Documento de Política de Seguridad de la Información:** La entidad debe contar con un documento escrito y aprobado por la entidad donde se refleje la política de seguridad de la información de la organización.
- **Revisión de Política de Seguridad de la Información:** La revisión de la política deberá ser realizada de manera anual o de acuerdo a cambios significativos en la seguridad de la información y hacer de conocimiento de la entidad dichos cambios.

4.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

- **Comité de Seguridad de la Información:** La entidad posee un grupo interdisciplinario denominado Comité de Seguridad de la Información, el cual vela por el gobierno de la seguridad de la información en la entidad
- **Acuerdos de Seguridad de la Información:** Tanto empleados como terceros deben tener firmado un acuerdo relacionados con el manejo de información o de recursos de informática de la CCB.
- **Términos y condiciones para clientes de Internet:** Todos los clientes que usan Internet para comprarle a la CCB productos o servicios, aceptan los términos y condiciones impuestos por la CCB para la realización del negocio, antes de que la orden sea procesada. Esto se ve reflejado en el documento: Marco Legal, el cual está publicado en la Servicios Virtuales.
- **Definición clara de las responsabilidades de seguridad de la información en relación con terceros:** Socios de negocios, proveedores, clientes y otros asociados a los negocios de la CCB deben tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información y esta responsabilidad se debe ver reflejada en los contratos con la CCB y verificada por la Vicepresidencia de Tecnología.

Prácticas en seguridad de la información

- **Acceso por parte de terceros:** cualquier acceso por parte de un tercero a los recursos tecnológicos o a la información de la organización, debe haber cumplido con las autorizaciones respectivas y además estén debidamente firmados los acuerdos de confidencialidad respectivos.
- **Manejo de información con terceros:** Al momento de terminar relaciones con un tercero el cual maneje información de la organización, el tercero debe destruir de una manera adecuada la información o en su debido defecto devolver la información.
- **Acuerdos con terceras partes:** Dentro de los acuerdos de servicios con terceras partes se debe incluir una cláusula, la cual autorice a la CCB a realizar auditoria para validar los controles utilizados por los terceros para el manejo de la información de la organización.

4.3 GESTION DE ACTIVOS

- **Inventario de activos:** La entidad debe contar con un inventario de activos donde se defina de acuerdo a un criterio escogido, la importancia de dicho activo de información. Dentro del inventario es necesario identificar el propietario del activo de información.
- **Guía de Clasificación de la Información:** La entidad debe contar con un procedimiento que describa la forma en cómo se realiza el proceso de identificación, clasificación y valoración de los activos de información.

4.4 SEGURIDAD DEL RECURSO HUMANO

- **Responsabilidad en Seguridad de la Información:** La responsabilidad por la seguridad de la información en las labores del día a día debe corresponder a cada colaborador de la organización.
- **Acuerdo y aceptación de la política y prácticas de seguridad de la información:** Todo usuario debe firmar el formato ***INF-SPI-F-001 Acuerdo de seguridad de la información***, antes de otorgarle cualquier tipo de información sin importar el medio en el que se maneje, o su identificación de

usuario y contraseña y sus respectivos privilegios para el uso de los recursos tecnológicos de la CCB, este acuerdo de confidencialidad también cubre a empleados temporales, consultores y toda aquella persona o empresa que de una u otra manera tenga acceso a la información de la organización, para facilidad de todos los colaboradores sea de planta, consultores, temporales se facilita la guía rápida de seguridad de la información, la cual debe ser leída antes de firmar dicho acuerdo de confidencialidad.

- **Términos y condiciones:** Toda relación contractual de la entidad con empleados, o terceros debe hacer mención debe tener firmado el acuerdo de seguridad de la información (acuerdo de confidencialidad).

- **Entrenamiento, concientización y sensibilización de los miembros de la organización.** Sin ninguna excepción, todos los empleados de la organización, deben poseer y atender las disposiciones de la organización referente al debido entrenamiento, la concientización y sensibilización que les permita el manejo apropiado y adecuado para la protección de la información y los recursos tecnológicos de la empresa.

  Los programas de concientización y entrenamiento deben cubrir todas las líneas y personas de la organización, iniciando desde la Alta Gerencia, generando su recorrido vertical hasta los usuarios finales, quienes deben sentirse motivados al involucrarse y al asumir el programa, si llegasen a observar algún cambio en los patrones de comportamiento de los miembros de la Alta Dirección. Será responsabilidad del área de Seguridad de la Información, el mantenimiento del programa de entrenamiento, concientización y sensibilización de todos y cada uno de los miembros de la organización, así como de su seguimiento y oportunidades de mejora, para su ejecución se requiere del apoyo de Comunicaciones Internas, este plan debe ser de ejecución anual, el cual está diseñado para utilizar diferentes medios de comunicación, de los cuales dispone la organización para hacer la respectiva difusión en los temas críticos en materia de seguridad y protección de la información.

  Los temas a incluir dentro de la concientización son los siguientes:

  - Administración y manejo de las contraseñas.
  - Manejo de tarjeta de identificación.
  - Protección contra virus.
  - Manejo de políticas y las implicaciones del no cumplimiento de las mismas.
  - Spam y correo anormal.

Prácticas en seguridad de la información

- Uso de los servicios de Internet.
- Ingeniería social.
- Manejo de incidentes.
- Manejo de información sobre Internet y el cifrado de datos.
- Manejo de portátiles y dispositivos móviles.
- Licenciamiento del software. Copyright.
- Software de la organización.
- Control de acceso físico y lógico.
- Registro de operaciones. Porque la empresa lo hace.
- Seguridad del escritorio.

Para el manejo de la información de la organización y la clasificación de la misma, es importante que de manera anual, se realice la programación de todos los temas a tratar con referencia al entrenamiento, concientización y sensibilización en aspectos de seguridad, estas temáticas se generan de los resultados obtenidos en la matriz de riesgos a los activos de información, así como de las novedades y variaciones identificadas por parte del área de Seguridad de la Información que se presenten o se informen a nivel del Comité de Seguridad de la Información como a la Vicepresidencia de Tecnología.

- **Cumplimiento de los programas de entrenamiento:** Todos los funcionarios de la organización deben acudir cuando sean convocados a los programas de entrenamiento y sensibilización en la protección de la información y recursos tecnológicos de la organización.

- **Inducción del nuevo personal:** Todo nuevo integrante de la organización deberá recibir una inducción adecuada acerca de las los lineamientos básicos de seguridad que la organización ha asumido.

- **Remoción de privilegios:** A la finalización de una relación entre un empleado, contratista, temporal o terceros; la línea de trabajo Infraestructura Tecnológica debe velar por remover de manera oportuna los privilegios de acceso a los recursos tecnológicos, e información de la organización, con base en la información que reporte el línea usuaria que solicitó su creación.

- **Procesos disciplinarios:** En caso de que un colaborador, proveedores, o socio de negocio incumplan las políticas por negligencia o intencionalmente, la entidad se reserva el derecho de tomar las medidas correspondientes, tales como acciones disciplinarias, suspensión, despido, acciones legales, reclamo de

compensación por daños u otros. No obstante la primera vez que se determine que un colaborador incumplió las practicas se le llamará la atención, si esto se repite se le informará al superior inmediato para que tome las acciones correspondientes, si continúa ocurriendo Recursos Humanos aplicará las sanciones que estime convenientes dependiendo de la gravedad del incumplimiento.

4.5 SEGURIDAD FÍSICA Y AMBIENTAL

- **Perímetro físico de seguridad:** La entidad tiene una serie de medidas de control de acceso físico que deben ser aplicadas a todos los colaboradores de la entidad, o personal externo a la CCB, dentro del conjunto de controles se tiene, sistema de control de acceso físico, circuito cerrado de televisión, servicios de vigilancia en las instalaciones, centro de recepción, sin ninguna excepción todos los colaboradores y personal externo no debe saltarse alguno de estos controles.
- **Control de acceso físico:** Los sistemas de control de acceso aplican para todo el mundo, por esta razón siempre que pase por una puerta debe deslizar su carnet y no permitir que ningún otro colaborador pase sin presentar el suyo. De igual manera los colaboradores de la CCB deben portar su carnet durante su permanencia en las instalaciones. En un lugar visible, y el cual es personal e intransferible.
- **Manejo de privilegios y remoción de los mismos:** Todos los empleados, contratistas y terceras partes deben tener asignados privilegios de acceso a las instalaciones de la entidad, es responsabilidad Seguridad Física, su manejo y control. En caso de finalización de contratos se deben eliminar inmediatamente los privilegios de acceso físico.
- **Manejo de tarjeta de acceso:** La reexpedición del carnet sólo se realizará por deterioro del mismo y para ello el colaborador deberá presentar el original en la oficina de Seguridad Física de la CCB, con el objeto de que se le reemplace este elemento. En caso de pérdida el colaborador debe: Reportar a CCB la pérdida del elemento mediante correo electrónico a Seguridad Física con copia a Recursos Humanos, con el fin de bloquear el carnet extraviado. Realizar pago en la caja de la CCB para la expedición de un nuevo carnet. Dirigirse al a oficina

de Seguridad Física de la CCB ubicada en la sede Salitre con la copia del denuncio y el pago realizado para que se le expida un nuevo carnet.

- **Personal externo de trabajo:** Las líneas de trabajo administradoras de los contratos de Outsourcing o que tengan a su cargo la coordinación de Contratistas, deben informar a la línea de Seguridad Física los ingresos de nuevo personal y salidas o terminación de contratos; a estas personas se les deberá exigir la prueba de su afiliación a la respectiva Administradora de Riesgos Laborales (ARL).

- **Ingreso de personal de aseo:** Para el caso del Edificio Salitre las personas que trabajan como contratistas u Outsourcing de Servicios Administrativos e Infraestructura, deberán hacer su ingreso por la recepción 2 de la carrera 68 D (costado oriental). Para el caso del Edificio Centro Empresarial Chapinero, las personas que trabajan como contratistas u Outsourcing de Servicio Administrativos e Infraestructura, deberán hacer su ingreso por la recepción del piso 1, calle 67 con carrera 9 costado sur oriental. Para el caso del edificio centro Empresarial sede Kennedy las personas que trabajan como contratistas u Outsourcing de Servicios Administrativos e Infraestructura, deberán hacer su ingreso por la calle 30 sur (costado-norte) con listado y número de cédula.

  Cuando esté previsto el ingreso de Grupos (Mayores a 5 Personas) a cualquiera de las instalaciones de la CCB, deberán informar mínimo con 1 hora de anticipación y remitir un listado de las personas a la Recepción o a Seguridad Física con el fin que establecer la forma más adecuada en la que ingresarán y que no ocasione traumatismos a estas líneas de trabajo, las cuales puedan incomodar a nuestros visitantes.

- **Atención de clientes externos:** Cuando se programen las reuniones periódicas con la Presidencia, las líneas de trabajo deberán coordinar no hacer citas con clientes en el horario establecido y así se evita generar incomodidades a los clientes, en último caso, deberán informar a la recepción con quien podrán remitirlos para que sean atendidos.

- **Reuniones corporativas de CCB:** Como medida de control de asistencia para las reuniones con la Presidencia, los Colaboradores deberán pasar el carnet por la lectora óptica ubicada en la puerta de acceso a los ascensores del Auditorio (Piso 1). Las personas que no tengan carnet con tarjeta de acceso deberán diligenciar la planilla física de asistencia (Centro Empresarial Salitre).

- **Buzón de correspondencia:** En todas las sedes se instalará un buzón para que allí se deposite la correspondencia interna que se distribuye en las sedes en horas de la mañana antes de la apertura de la sede.

4.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

- **Documentacion:** Infraestructura Tecnológica debe contar con una serie de procedimientos que describan la forma de operación del centro de cómputo. En ella se deben describir las responsabilidades de la línea y sus miembros en la administración y gestión de la tecnología.
- **Administrador designado:** Todo ambiente de producción debe tener designado un administrador, el cual se encarga de definir los privilegios de usuarios sobre el sistema, así como las labores de mantenimiento del sistema, la plataforma y/o la aplicación.
- **Entrenamiento compartido para labores técnicas críticas:** Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de la CCB.
- **Los computadores y sistemas de comunicación deben tener controles de acceso físico apropiados:** Todos servidores, equipos centrales de comunicaciones, o sistemas de almacenamiento de información (bases de datos) deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.
- **Ambientes separados de producción, desarrollo y pruebas:** Los sistemas de información o aplicativos de la entidad podrán contar con un ambiente de desarrollo, un ambiente de producción, y su correspondiente ambiente de pruebas bien sea a través de sistemas físicamente independientes o directorios o librerías que tengan sus sistemas de control de acceso muy bien definidos.
- **Monitoreo de infraestructura tecnológica:** La actividad de los sistemas será monitoreada por una herramienta que permitirá a los Administradores de los Sistemas, tomar acciones en caso de fallas.
- **Aseguramiento de las instalaciones de sistemas de información:** Para las actividades de hardening o afinamiento de los sistemas operacionales, tanto de servidores como estaciones de trabajo, es responsabilidad de Infraestructura

Tecnológica la aplicación de las Guías de Aseguramiento (Servidores Windows, Servidores Linux o Estaciones de Trabajo) posterior a la instalación del Sistema Operacional.

- **Actualizaciones, parches y bugs:** Infraestructura Tecnológica en cabeza de los Administradores de cada una de las plataformas con las que se cuenta, realizará los procesos de aplicación de parches y actualizaciones. En el Ambiente Windows, las actualizaciones se realizarán mensualmente de acuerdo a los Boletines, parches y actualizaciones liberados por Microsoft. Para los Ambientes Linux los procesos de aplicación de parches y actualizaciones se realizará de forma automática desde el sitio web del fabricante y de manera manual en los casos que dicho proceso lo requiera.

- **Tratamiento del código malicioso:** Todos los computadores, servidores y sistemas de información de la organización, deben tener software suministrado por la organización para la protección contra código malicioso.

- **Sistemas de detección de intrusiones:** Todo segmento de red accesible desde Internet debe tener un sistema de detección y prevención de intrusos (IDS/IPS) de tal forma que alerte y contenga posibles ataques.

- **Sistemas de protección perimetral:** Toda conexión a los servidores de la CCB proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por un sistema de protección perimetral (Firewall), con el fin de limitar y controlar el tráfico de red a los activos de información de la entidad.

- **Toda conexión hacia Internet debe pasar por el sistema de protección de perímetro:** El sistema de protección de perímetro (firewall) debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por dicho componente tecnológico.

- **Filtrado de contenido:** Todo el contenido dirigido y proveniente de Internet debe pasar por un sistema de filtrado de contenido, debe filtrar sin limitarse a elementos como applets de java, Macromedia, controles ActiveX, páginas de contenido adulto, extensiones riesgosas como la ejecución de programas (exe, bat, vbs), extensiones de librerías (dll, so, ko), extensiones de música y video (mp3, wav, avi, entre otros formatos).

Prácticas en seguridad de la información

- **Contraseña de los dispositivos:** Todo dispositivo de red de la organización debe tener una única contraseña, o un mecanismo de control de acceso adecuado.
- **SPAM:** Se debe tener un sistema de protección para restringir la recepción de correo no solicitado o SPAM, el administrador del sistema debe garantizar una adecuada configuración.
- **Scan del Correo electrónico:** Todos los mensajes entrantes y salientes del servicio de correo deben ser pasados por un sistema de control el cual filtre cualquier tipo de malware que sea identificado.
- **Almacenamiento de Backup:** La información del negocio, así como sus Backups deben estar almacenados en un ambiente protegido y con restricciones de control de acceso establecido.
- **Tipo de datos a los que se les debe hacer Backups y con qué frecuencia.** A toda información almacenada en los ambientes de servidor de la CCB, se le debe hacer Backups con la frecuencia necesaria soportada por los planes de contingencia. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada. De igual manera se deben elaborar dos copias con el fin de minimizar el riesgo por daño del medio de almacenamiento.
- **El sistema interno de direccionamiento de red no debe ser público:** Las direcciones internas de red y configuraciones deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.
- **Segmentos de la red:** Todos los servidores que prestan servicios en Internet deben estar ubicados en un segmento de red especial, protegidos por el sistema de protección perimetral (Firewall), con el fin de proteger la red Interna y los servidores internos. De igual forma los servidores internos deben estar separados de la red de usuarios internos y de las demás redes.
- **Restricción de acceso a Internet a terceros:** No se le deben otorgar privilegios de acceso a Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada por parte de quien tiene la relación contractual con el tercero. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para

la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Vicepresidencia de Tecnología.

- **Reasignación de equipos:** Infraestructura Tecnológica debe antes de realizar el procedimiento de reasignación de un equipo a otro empleado de la organización, realizar una destrucción efectiva de la información almacenada en dicho componente tecnológico.
- **Instalación de sistemas operacionales:** Infraestructura Tecnológica debe instalar los sistemas operacionales con base en las guías recomendadas por el fabricante, tanto para las estaciones de trabajo como para los ambientes de servidores.
- **Procedimientos de retroceso:** Al momento de realizar modificaciones o cambios sobre sistemas de información, configuraciones o actualizaciones, se deben tener mecanismos que reviertan a los últimos cambios estables de un sistema de información, configuración o actualización realizada, es necesario por ende disponer de los Backups apropiados y actualizados de tal manera que se pueda contar con dicha información.
- **Software de identificación de vulnerabilidades:** Se deben realizar de manera periódica valoraciones de seguridad, test de intrusión a los ambientes de producción; estas pruebas deben ser realizadas por lo menos dos veces al año, tarea que debe ser realizada por el oficial de seguridad de la información. De igual manera cualquier sistema que pretenda entrar en ambiente de producción debe realizarse la respectiva prueba de seguridad o test de intrusión.
- **Contenido de los logs:** Se deben activar los logs de los sistemas operacionales de todos los servidores que soportan las aplicaciones, estos deben almacenar información asociada a la actividad del sistema.
- **Rotación de los logs:** Debe existir un proceso automático de rotación y archivo de los logs.
- **Protección de los logs:** Es necesario que existan controles de accesos tanto físicos como lógicos para restringir el acceso a los logs que la entidad genera, solo los administradores designados y/o personal de la contraloría interna, así como personal de seguridad de la información tendrán acceso a los mismos.

Prácticas en seguridad de la información

- **Sincronización de relojes para un registro exacto de eventos en la red:** Los computadores, impresoras, y demás componentes tecnológicos conectados a la red interna de la CCB deben tener sus relojes sincronizados con la hora oficial de Colombia.
- **Monitoreo de eventos de seguridad de la información:** La organización deberá contar con un sistema de monitoreo de eventos de seguridad de la información, donde pueda observar el comportamiento de manera centralizada de las posibles fallas de los sistemas de la entidad.
- **Solicitud de préstamo de recursos informáticos:** Toda solicitud para la utilización de un recurso informático, debe venir respaldada por la autorización del Jefe de la línea de trabajo respectiva y siguiendo los procedimientos establecidos para ello.
- **Configuración de sistema operativo de las estaciones de trabajo:** Solamente los funcionarios de Infraestructura Tecnológica están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

4.7 CONTROL DE ACCESO

- **Control de acceso centralizado:** Tanto el registro como la operación de acceso deben estar centralizados, no deben existir múltiples escenarios de control de acceso diferentes de los existentes para los sistemas de información y servicios ofrecidos para los colaboradores de la CCB, para los servicios ofrecidos a los clientes se debe dejar documentado el sistema de control de acceso a utilizar.
- **Revisión periódica y reautorización de privilegios de usuarios:** Los derechos de acceso a los usuarios serán revisados al menos una vez al año, con el fin de mantener un control eficaz de acceso a los datos y a los servicios de información, labor que será realizada por el propietario o responsable del Sistema de Información en acompañamiento de la Vicepresidencia de Tecnología a través del procedimiento definido para tal fin.
- **Identificación de usuarios:** Todos los usuarios de recursos tecnológicos e información deben poseer un identificador único.

Prácticas en seguridad de la información

- **Identificación de usuarios estándar:** Los identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente documentados en caso de ser utilizados.

- **Soporte para usuarios con privilegios especiales:** Todos los sistemas y computadores deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores. Se brindarán permisos de administrador a los usuarios que lo requieran, siempre y cuando exista una previa validación por parte de la Infraestructura de Tecnología a través del Coordinador de Soporte Técnico, en donde se valide que se requieren este tipo de permisos especiales para la administración de Software que no permite la misma bajo el tipo de usuario estándar.

- **Gestión de Privilegios:** Los privilegios asignados a los usuarios deben estar asociados a/o los Sistemas de Información que corresponda de acuerdo al rol del funcionario en la Entidad. Es responsabilidad del propietario del o los Sistemas de Información definir los privilegios y notificar a los administradores respectivos para su adecuada asignación.

- **Credenciales iniciales:** Las contraseñas iniciales otorgadas deben servir únicamente para el primer ingreso del usuario al sistema, en ese momento el sistema debe obligar al usuario a cambiar su contraseña.

- **Límite de intentos consecutivos de ingreso al sistema:** El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos fallidos el identificador del usuario debe ser bloqueado hasta nueva reactivación por parte del administrador, después que se compruebe la identidad del usuario.

- **Cambio de contraseña del administrador:** La contraseña del administrador de un sistema de información, o recursos tecnológico de la organización debe ser cambiada, al momento que exista una sospecha de una posible falla de seguridad.

- **Longitud mínima de las contraseñas:** Todos los sistemas de información de la organización deben validar que las contraseñas deben tener como longitud mínima 7 caracteres, de igual manera deben validar que no se involucren contraseñas en blanco.

Prácticas en seguridad de la información

- **Historia de las contraseñas:** Los sistemas de información, o componentes tecnológicos que involucren un proceso de autenticación de usuarios debe mantener historia de al menos las últimas 5 contraseñas utilizadas por parte de los usuarios, de tal manera que no puedan ser reutilizadas.

- **Vigencia de las contraseñas:** Todos los sistemas de información de la organización o cualquier recurso tecnológico que involucre un sistema de control de acceso basado en credenciales (login, contraseña), deben validar como vigencia de la contraseña un periodo de 30 días hábiles, pasado este tiempo la contraseña debe expirar y bloquear la cuenta del usuario.

- **Notificación de cambio de contraseñas:** Todos los sistemas de información de la organización o cualquier recurso tecnológico que involucre un sistema de control de acceso basado en credenciales (login, contraseña), deben notificar al usuario 10 días antes que su contraseña debe ser cambiada, por el vencimiento de la misma.

- **Sesión:** Todos los sistemas y computadores de la organización, debe tener involucrado un sistema de control de acceso, así como un conjunto de credenciales que lo habiliten para utilizar los recursos de la organización.

- **Permisos por defecto en sistemas de archivos:** Los accesos a los sistemas de archivos de red de la organización deben bloquear por defecto el acceso de usuarios no autorizados. Se excluyen las carpetas que hayan sido definidas de propósito PÚBLICO a la cual pueden tener acceso todos los usuarios para intercambio de archivos.

- **Automatización del cierre de sesión:** Sin excepción todos los sistemas de información, o recursos de la organización, debe tener habilitados la terminación de la sesión después de 3 minutos de inactividad sobre dicho recurso.

Prácticas en seguridad de la información

4.8 ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

- **Análisis y especificaciones de requerimientos de software:** La implementación de un nuevo sistema de información, así como la actualización del mismo debe estar bien planeado, administrado, y formalmente documentado asegurando que los riesgos asociados al proyecto sean mitigados usando una combinación de controles automáticos y manuales. Se deben especificar de manera clara los requerimientos de seguridad importantes, a la hora del diseño del sistema de información, garantizando el balance entre seguridad y los demás objetivos establecidos.
- **Desarrollo de software:** Todo sistema de información desarrollado para la entidad debe seguir un proceso formal de desarrollo asociado a una metodología para la construcción de software. Esta metodología debe tener actualizado un conjunto de las mejores prácticas y principios de tal forma que todos los desarrolladores de software lo utilicen al interior de la organización.
- **Seguridad en el Ciclo de Vida de Desarrollo de Sistemas de Información:** Para todos los sistemas de información de la entidad se debe considerar los requerimientos en materia de seguridad de la información desde el inicio del proceso de diseño del software hasta su puesta en producción.
- **Validación de los datos de entrada y rechazo de ítems manejados:** Toda transacción a ser entrada en un sistema de información debe ser sujeto de validación adecuada, de tal forma que se aseguren que los datos suministrados son correctos y no generan ningún riesgo a los sistemas de información, toda transacción que falle debe rechazar los datos de entrada y generar una notificación de la falla, la cual debe ser corregida.
- **Manejo de Fallas:** Sin excepción todo software desarrollado al interior de la organización o en outsourcing debe suministrar en el caso de una falla no esperada, un mensaje de error sin detalles, ni consideraciones de las fallas.
- **Seguimiento de errores y problemas de seguridad:** Todas las quejas sobre los errores de software, omisiones y problemas de seguridad que son atribuibles a los sistemas de información desarrollados al interior o en contrato con terceras partes se debe retornar nuevamente a los diseñadores, programadores y a todo el personal de desarrollo involucrado, para su adecuada corrección.

Prácticas en seguridad de la información

- **Cambios en la información:** Toda transacción sobre un sistema de información de la CCB que afecte información debe ser procesada siempre y cuando se valide y autorice el usuario que realiza la operación.
- **Manejo de transacciones rechazadas:** Toda transacción que por alguna circunstancia sea rechazada debe ser listada en algún reporte de manejo de excepciones hasta que sea reenviada nuevamente o resuelta la causa del rechazo. En los planes de trabajo de las líneas de trabajo se deben incluir las actividades necesarias para identificar los servicios en los cuales se requiere la implementación que maneje las transacciones rechazadas y realizar los diseños e implementaciones requeridas.
- **Autenticación e integridad de los mensajes:** Cuando dentro de los requerimientos de las aplicaciones se exija garantizar la integridad de un mensaje de datos se deberá implementar los mecanismos necesarios que garanticen dicho control a través de cualquier medio electrónico.
- **Validación de los datos de salida:** La salida de los datos de un sistema de aplicación debe ser validada para garantizar que el procesamiento de la información almacenada es el adecuado para la situación especificada.
- **Manejo de sistemas criptográficos:** Todo software construido por la entidad o construido por un tercero deberá utilizar un ambiente de cifrado de datos solo cuando dentro de los requerimientos funcionales del sistema de información se haya especificado, o cuando un requisito de ley así lo exija.
- **Utilización de librerías y módulos precompilados:** Bajo ninguna circunstancia en desarrollos al interior de la organización se deben utilizar librerías o módulos precompilados bien sean descargados de Internet o de otro medio a menos que se conozca la fuente del mismo, sea confiable y esté libre de cualquier vulnerabilidad conocida.
- **Ubicación de los códigos fuentes:** Se debe garantizar que los programas o librerías fuentes de las aplicaciones no residen dentro del mismo ambiente operacional sobre el cual está instalado, en el caso de ser aplicaciones que poseen código de ejecución.
- **Versión del Software:** Todos los sistemas de información de la organización tanto en ambientes de producción como en ambientes de desarrollo deben estar

a su versión más reciente y estable, que tenga soporte por el fabricante y/o desarrollador.

- **Cumplimiento del procedimiento para cambios y/o actualizaciones:** Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe cumplir con los procedimientos establecidos para tal fin.
- **Sistemas de control de cambios y versiones:** Se debe contar con un sistema de control de cambios y versiones que deben ser utilizado para controlar las modificaciones, cambios y documentación del software de la organización, así mismo debe existir un procedimiento formal que defina la utilización del manejo de versiones.
- **Documentación de cambios y/o actualizaciones:** Toda aplicación deben estar documentada a través de un conjunto de requerimientos definidos y aceptados por la organización, adicionalmente esta documentación debe estar actualizada y disponible para cuando se requiera.
- **Segregación de funciones:** Se debe garantizar que exista una clara segregación de funciones referente a administración del sistema, operación del sistema y desarrollo de sistemas de información.
- **Manejo de sesiones de usuarios:** Todo sistema de información desarrollado para la organización que cuente con sistemas multiusuario, debe contemplar la utilización de bloqueo de manera temporal o definitiva de una cuenta por intentos fallidos de login, de la misma manera deben prohibir múltiples sesiones de una cuenta de usuario.
- **Autorización de funciones:** Los sistemas de información de la organización debe manejar el concepto de definición de roles y perfiles, de tal forma que solo se habiliten la funciones, y/o menús a los cuales se autoriza a los usuarios.
- **Conexión a las bases de datos:** Por ningún motivo debe existir una conexión directa entre los usuarios finales de las aplicaciones y las bases de datos de producción, estas siempre deben pasar a través de las aplicaciones o servidores de aplicaciones definido para ello.
- **Conexión a las bases de datos desde las aplicaciones:** Por ningún motivo una conexión debe realizarse con el usuario de mayor privilegio en la base(s) de dato(s), siempre debe ser un usuario con el principio del menor privilegio.

Prácticas en seguridad de la información

- **Protección de la conexión a las Bases de Datos:** Con el objetivo de evitar que se pueda identificar la contraseña de conexión a las bases de datos, es de carácter obligatorio que toda conexión con cualquier base de datos, tanto para los ambiente de producción como de desarrollo deba realizarse utilizando el cifrado de los datos como mecanismo para proteger la confidencialidad e integridad de los mismos.

- **Acceso a los sistemas de almacenamiento:** Es indispensable que todos los accesos a sistemas de almacenamiento como Bases de Datos deben establecer distintos niveles de acceso tanto a los datos, registros, tablas y archivos, así como a configuraciones y funciones propias del sistema de almacenamiento de tal manera que se evite accesos inadvertidos o no autorizados.

- **Acceso del Administrador de la Base de Datos:** Es necesario que el ingreso a la base sea realizado por los administradores de bases de datos designados por la organización, para realizar las funciones de cambios, modificaciones, alteraciones y o actualizaciones tanto de los datos, registros, tablas y archivos, así como de configuraciones y actualizaciones del sistema de almacenamiento.

- **Separación de funciones en los sistemas de información:** Todo sistema de información de la organización debe mantener de manera clara y específicamente separados los módulos de configuración de los de módulos de funciones del negocio, y el registro de actividades deberá ser obligatorio para ambos casos.

- **Acceso a los ambientes de producción y la información:** El personal de desarrollo de sistemas de información no debe tener permisos de realizar procesos de actualización de los Sistemas de Información o del Sistema Operacional de los ambientes de producción, o copias de los sistemas de información y/o datos de los ambientes de producción; a excepción de la resolución de problemas sobre los mismos ambientes.

- **Registro de auditoría en sistemas:** Todo Sistema de Información que soporte la prestación de un servicio de negocio de la CCB, debe generar registros de auditoría que guarden las modificaciones, adiciones y eliminaciones de dicha información.

- **Soporte de las aplicaciones:** Todo software desarrollado al interior de la organización o por terceros debe suministrar el nivel adecuado de soporte para garantizar que la organización no se vea afectada, cualquier problema que se

presente en el software debe ser resuelto de la manera más eficaz y en un tiempo aceptable para la organización. De igual forma se debe suministrar el entrenamiento funcional y de operación al personal indicado, así como la documentación adecuada**.**

- **Planeación de pruebas de capacidad, funcionalidad, y seguridad:** Todo nuevo sistema a ser implantado dentro de la organización sea desarrollado en la entidad o por terceros deberá someterse a las debidas pruebas que se consideren necesarias que demuestren un nivel de funcionamiento, y de resistencia adecuados, adicional deben aplicarse pruebas de vulnerabilidad del software, de tal forma que se tengan niveles adecuados de seguridad aceptados por la entidad.

- **Utilización y uso de software de terceros:** Todo desarrollo de software por parte de terceros a ser utilizado por la organización debe poseer un acuerdo de licenciamiento, uso y acceso al software, de igual manera se deben especificar cuáles son las condiciones de utilización del código fuente y cuáles son los derechos de propiedad que deben ser tenidos en cuenta.

- **Dependencia de la autenticación de usuario en el sistema operativo:** Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Cualquier excepción debe tener la debida justificación y aprobación de la Vicepresidencia de Tecnología.

- **Incorporación de contraseñas en el software:** Ninguna contraseña deberá ser incorporada en texto visible en el código de un software desarrollado o modificado por la organización, los software de terceros deben tener la posibilidad de integrarse con los esquemas de autenticación de la organización.

- **Acceso del usuario a los comandos del sistema operativo:** Después de haber iniciado una sesión de la aplicación, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

Prácticas en seguridad de la información

4.9 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

- **Proceso de atención y administración de incidentes:** La entidad debe contar con un procedimiento documentado que relacione la forma en cómo se identifica, analiza y atiende un incidente de seguridad de la información, así como las responsabilidades de los involucrados dentro del proceso.
- **Reportes de eventos de seguridad:** Se debe reportar al Comité de Seguridad de la Información de acuerdo con los incidentes presentados durante un periodo definido.

4.10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

- **Plan de recuperación ante desastres:** Todo sistema de información debe tener definido un plan de contingencia para la restauración y recuperación de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación ante desastres, que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se deben crear planes de respuesta a emergencias con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Es deber de Infraestructura Tecnológica mantener documentado, actualizado, probado y mantenido dicho plan.
- **Personal competente en el Centro de Cómputo para dar pronta solución a problemas:** Con el fin de garantizar la continuidad de los sistemas de información, el Centro de Cómputo debe contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.
- **Pruebas del plan de contingencia:** El plan de contingencia y recuperación creado debe ser probado por lo menos una vez al año, y presentar un informe de la efectividad del mismo, a la Vicepresidencia Ejecutiva.

Prácticas en seguridad de la información

4.11 CUMPLIMIENTO

- **Uso personal de los recursos informáticos:** Los recursos informáticos de la CCB deben ser usados para fines laborales. Cualquier otro uso debe ser realizado de manera moderada de tal forma que no interfiera con la productividad de la persona o con las actividades propias de la organización.
- **Responsabilidad de la Identificación del usuario:** Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada dicha identificación. Los usuarios no deben permitir que otros usuarios realicen labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la Cámara de Comercio de Bogotá (CCB).
- **Uso del software entregado:** Cuando la CCB realiza contratos de licenciamiento de software, la entidad subscribe con los fabricantes un contrato de "LICENCIA DE USO" para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad.
- **Declaración de reserva de derechos de la CCB:** La CCB usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos la CCB se reserva el derecho y la autoridad de:

  1. Restringir o revocar los privilegios de cualquier usuario;

  2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y,

  3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la CCB. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, con conocimiento del Jefe inmediato, siempre con el concurso del Vicepresidente de tecnología o de quién él delegue esta función.

Prácticas en seguridad de la información

- **Acceso no autorizado a los sistemas de información de la Entidad:** Los usuarios tienen la prohibición de obtener acceso a sistemas de información a los que no se tiene privilegios e igualmente se prohíbe cualquier modificación o consulta de la información contenida en el sistema. Esto implica la prohibición de capturar contraseñas, llaves de cifrado y otros mecanismos de control de acceso que le puedan permitir obtener acceso a sistemas no autorizados.
- **Posibilidad de acceso no implica permiso de uso:** Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario.
- **Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos:** Los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato a la línea de trabajo de Seguridad de la Información.
- **Dejar sistemas desatendidos:** Los usuarios no deben dejar el computador desatendido sin cerrar primero la sesión iniciada.
- **Control de recursos informáticos entregados a los usuarios:** Cuando un usuario inicie o termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse igualmente un inventario del estado del mismo. El empleado será responsable de los desperfectos o daños que por su negligencia haya ocasionado a la máquina.
- **Protección por Defecto de Copyright:** Todos los colaboradores de la organización deben revisar, e investigar los derechos de propiedad intelectual para todo material, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito que esté relacionado con la entidad.
- **Prohibición de instalación de software y hardware en los computadores de la organización:** La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios autorizados de la Vicepresidencia de Tecnología. Solamente bajo la autorización de Infraestructura Tecnológica se permitirá la instalación de software no contemplado al momento inicial de configurada la estación.

Prácticas en seguridad de la información

- **Esquemas de licenciamiento de fuente abierta y/o libre distribución:** La instalación de software que posee algún tipo de esquema de licenciamiento diferente al que posee la organización (Dominio Público, Shareware, Freeware, entre otros), no podrá ser instalada, hasta el momento que se solicite la autorización respectiva por parte de Infraestructura Tecnológica.
- **Juegos no pueden estar almacenados sobre un computador:** Bajo ninguna circunstancia es posible almacenar o usar cualquier juego en los recursos computacionales suministrados por la Cámara de Comercio de Bogotá.
- **Uso de dispositivos móviles:** Es responsabilidad de los usuarios revisar cualquier medio extraíble (memorias USB, CDs, DVDs, teléfonos móviles USBs, cámaras con memoria con conexión a USB y en general cualquier dispositivo que almacene archivos y que se pueda conectar al computador a través de puerto USB), que sea conectado al computador de tal manera que se eviten posibles contagios de malware o infección electrónica.
- **Confidencialidad de las contraseñas:** La contraseña que a cada usuario se le asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible, cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.
- **Identificación única para cada usuario:** Cada usuario tendrá una identificación única, acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores.
- **Almacenamiento de contraseñas:** Ninguna contraseña debe ser guardada de forma legible en archivos "Bach", scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Se recomienda no tener su contraseña en cualquier medio impreso.
- **Sospechas de compromiso deben forzar cambios de contraseña:** Toda contraseña deberá ser cambiada por el usuario de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.
- **Revelación de contraseñas:** Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean

funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios.

- **Auditoria periódica a las contraseñas de los usuarios:** Solamente la auditoria de Sistemas o la línea de trabajo de Seguridad de la Información realizarán auditorías a las bases de datos de las contraseñas de los usuarios, con el objetivo de dar cumplimiento a las labores de monitoreo de cumplimiento a las políticas de seguridad de la información.
- **Uso obligatorio de contraseña en el protector de pantalla:** Todas las estaciones de trabajo de los usuarios deben tener activado el protector de pantalla institucional protegida por contraseña, adicional a que no se debe instalar un papel tapiz diferente a los especificados.
- **Manejo, Acceso y Uso de la Información:** La Información de la Cámara de Comercio de Bogotá debe ser usada única y exclusivamente para los propósitos de la función que desempeña el colaborador dentro de su entorno laboral. De igual manera el uso y acceso de la información de la organización debe ser consistente con las políticas que existan.
- **Propiedad legal de los archivos de los sistemas de información y mensajes:** La Cámara de Comercio de Bogotá tiene la propiedad legal del contenido de todos los archivos almacenados en cualquier sistema informático suministrado por la organización así como cualquier mensaje de datos transmitido vía estos sistemas. La Cámara de Comercio de Bogotá se reserva el derecho de utilizar la información para el desarrollo de sus actividades.
- **Medios Removibles:** Los colaboradores de la organización no deben almacenar información de la entidad en ningún medio removible (Diskette, USB, Discos Externos).
- **Uso de Internet para propósitos personales:** El uso de Internet se asigna para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. El uso de Internet con propósitos personales está permitido siempre y cuando este no afecte de ninguna forma la productividad del personal y no cause conflictos con las actividades propias de la organización.
- **Uso de Correo Electrónico:** El correo electrónico debe ser usado únicamente con prioridad para los propósitos del trabajo. Se recomienda usar términos y

expresiones adecuadas como en otros medios de comunicación formal de la organización, para que no sean interpretados al relacionarse con clientes o terceros como la postura oficial de la organización. Todo mensaje de correo electrónico (e-mail) deberá contener en la parte inferior el siguiente mensaje: "Este es un mensaje de carácter confidencial de la Cámara de Comercio de Bogotá. Si usted no es el destinatario del mismo o no está autorizado para recibir este mensaje en nombre del destinatario, absténgase de usar, copiar, divulgar o en cualquier otra forma esta información. Las opiniones o información de tipo personal o no directamente relacionadas con los asuntos de la Cámara de Comercio de Bogotá que contenga este mensaje no se deben entender como respaldadas por esta. Si recibió este mensaje por error por favor comuníquese en forma inmediata con su remitente ".

- **Formalidad del correo electrónico:** Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.
- **Preferencia por el uso del correo electrónico:** Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.
- **Propietarios del buzón de correo:** La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.
- **Mensajes prohibidos:** Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos 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.
- **Respuestas a correo electrónico no solicitado:** Bajo ninguna circunstancia los usuarios que reciban correo no solicitado deben responder a quien envía el mensaje.
- **Restricción para el envío masivo de mensajes de correo electrónico a nivel externo:** Tan solo el Presidente Ejecutivo, los Vicepresidentes, el Gerente de Recursos Humanos, el Gerente de Formación Empresarial y el Gerente de

Relacionamiento con el Cliente, podrán solicitar a la Vicepresidencia de Tecnología el envío masivo de mensajes de correo electrónico dirigidos a clientes de la Cámara.

- **Bloqueo de Acceso:** La organización puede utilizar componentes tecnológicos que permitan el bloqueo a sitios de Internet que se consideren cuestionables o cuyo propósito no sea el estrictamente de su función.
- **Visitas y Descargas de Internet:** Los usuarios de la organización deben abstenerse de descargar a través de Internet videos, audio, imágenes de gran tamaño, a menos que estas descargas estén debidamente justificadas para propósitos laborales, de la misma manera el acceso, observación o cualquier forma de utilización de sitios Web que en su contenido contemple pornografía, juegos, racismo o que de alguna forma atenten contra los derechos fundamentales, normatividades de ley, reglamento interno de trabajo, la presente normatividad o demás reglas que rigen a la entidad.
- **Direcciones de correos institucionales:** Todas las direcciones de correo electrónico externo asignados a los usuarios internos de la CCB, deben corresponder con la función que desempeñan. No deben asignarse direcciones externas de carácter personal. Se exceptúan los miembros del Comité Directivo y aquellas solicitudes justificadas por un miembro del Comité Directivo.
- **Todo buzón de correo debe tener un responsable:** Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones que se utilizan en los sistemas de información de la organización
- **Control de Tráfico en Internet:** La organización está en todo su derecho de monitorear de manera continua y constante el tráfico que circula hacia o de Internet.
- **Monitoreo del correo electrónico:** La organización se reserva el derecho de monitorear y/o revisar los mensajes de correo electrónico corporativo sin notificar al usuario de la acción a realizar.
- **Manejo de archivos adjuntos:** Los usuarios deben abstenerse de abrir archivos adjuntos de mensajes los cuales desconozcan el remitente.
- **Foros públicos:** Los colaboradores de la organización deben abstenerse de participar en comunidades, foros, blog y demás medios electrónicos de

intercambio de información, con información relevante de la organización, a menos que está esté debidamente autorizada.

- **Responsabilidad de las copias de respaldo de los usuarios:** La información y los datos almacenados sobre computadores o portátiles se le deben realizar un Backups con regularidad. Es responsabilidad del usuario que se realice el procedimiento.
- **Revisiones de sistemas de información:** La línea de trabajo de Seguridad de la Información debe tener autorización para revisar la configuración, programación, mantenimiento, entrenamiento, y monitorear los sistemas de información de la organización.
- **Responsabilidad y propiedad:** Tanto la línea de trabajo de Seguridad de la Información, Infraestructura Tecnológica, así como Solución de Software, no son los responsables, ni dueño de ninguna de la información de la organización, a excepción de los documentos e información producidas en las respectivas líneas de trabajo.
- **Deshabilitar controles de seguridad:** A menos que exista una autorización de la Vicepresidencia de Tecnología, ningún sistema de control de la infraestructura de seguridad debe ser desactivado, inhabilitado, desconectado, apagado, o sobrepasado.

Prácticas en seguridad de la información

5. CONTROL DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	13/Jun/11	Creación del documento.
2	13/Dic/11	Se actualizan los capítulos de gestión de comunicaciones y operaciones, control de acceso y adquisición desarrollo y mantenimiento de los sistemas de información en los siguientes aspectos: ✓ Aseguramiento de las instalaciones de sistemas de información ✓ Actualizaciones, parches y bugs ✓ Revisión periódica y reautorización de privilegios de usuarios ✓ Gestión de privilegios ✓ Protección de la conexión a las Bases de Datos ✓ Acceso a los ambientes de producción y la información ✓ Privilegios de desarrolladores de sistemas de información ✓ Registro de auditoría en sistemas
3	27/Dic/2013	Se modifica el documento en los siguientes aspectos: • Se mejora la redacción del **Objetivo** y el **Alcance** para mayor compresión. • Se realiza una actualización de los cargos y áreas correspondientes, de acuerdo con la nueva estructura organizacional de la CCB. • En el numeral **4.4 Seguridad del Recurso Humano** se incluye la concientización como un aspecto que hace parte del entrenamiento y la sensibilización. Adicionalmente, se establecen los mecanismos y los temas que se deben divulgar dentro del proceso de concientización. • En el numeral **4.7 Control de acceso** se ajusta: ** Se cambia el aspecto "*Identificación de usuarios genéricos*" por "***Identificación de usuarios***

Prácticas en seguridad de la información

		estándar". ** En el literal "*Soporte para usuarios con privilegios especiales"* se especifica que se brindarán permisos de administrador a los usuarios que lo requieran, siempre y cuando exista una previa validación por parte de la Infraestructura de Tecnología, en donde se valide que se requieren este tipo de permisos especiales para la administración de Software que no permite la misma bajo el tipo de usuario estándar. • En el formato ***INF-SPI-F-001 Acuerdo de seguridad de la información*** se actualizan las rutas e hipervínculos de consulta de la política y las prácticas de seguridad de la información.