POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CUADRO CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción del Cambio**
01	21/11/2012	Creación Inicial del Documento (Sol 1136) se incluye dentro de la Documentación del SIGC
02	24/09/2014	Modificación (Sol. 1553) De conformidad al acuerdo 1262 de 20 de Dic. De 2013 se modifican los siguientes ítems: Numerales: 3, 4, 6.1, 6.2.1, 6.2.2, 6.3.1, 6.2.5, 6.4.6, 6.4.3.1, 6.4.3.2, 6.4.5, 6.4.6.5, 6.4.3.4, 6.4.3.3…...6.4.6 cambia a Subdirección administrativa y financiera, elimina coordinación de T.I y añade el proceso de tecnología de la información. Numeral 6.3.5 elimina la oficina de contratación y añade coordinación de procesos contractuales; actualización de la imagen institucional

1. INTRODUCCIÓN

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de la CDMB con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

2. ALCANCE Y APLICABILIDAD

Esta política aplica a toda la entidad, sus funcionarios, proveedores, contratistas, aprendices, practicantes, proveedores y judicantes de la CDMB y la ciudadanía en general que hagan uso de los recursos tecnológicos de la organización**.**

3. OBJETIVO

Regular el uso de las Tecnologías de Información y Comunicación en la CDMB, con el fin de optimizar su uso, garantizar la protección y seguridad de la institución, de su información y de su personal, y propender por una mayor eficiencia en el trabajo y continuidad en las operaciones.

La CDMB para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con los objetivos específicos de:

- Proteger la CDMB en lo concerniente a la infraestructura tecnológica, a la información, a los mismos servidores(as) y personal que presta sus servicios en la institución.
- Minimizar el riesgo en las funciones más importantes de la entidad.
- Definir un marco de referencia para direccionar el actuar del personal en el desarrollo de sus actividades, con miras a unificar la forma de realizar las tareas, propendiendo por el aumento de la productividad y la aplicación de las mejores prácticas de T.I.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Implementar el sistema de gestión de seguridad de la información.
- Establecer los lineamientos y directrices generales, relacionados con el uso de la plataforma tecnológica y la utilización de los servicios informáticos de la entidad, que debe seguir todo el personal de la CDMB, que permitan proteger los activos tecnológicos.
- Especificar e implementar las pautas para el desarrollo de las actividades que hacen parte de los procesos liderados por la Subdirección Administrativa y Financiera en especial el proceso de Gestión de Tecnología de la Información (Seguridad de la Información).
- Apoyar la innovación tecnológica.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes, judicantes y usuarios de la CDMB.
- Garantizar la continuidad de los procesos frente a incidentes.

4. SUPERVISIÓN DE POLÍTICAS

El proceso de Gestión de Tecnologías de la Información realizará revisiones, verificaciones y controles permanentes, para constatar el cumplimiento de estas políticas, así como la necesidad de ajustar o modificar las mismas.

5. VIOLACIÓN A POLÍTICAS

La violación a las políticas establecidas en este documento por parte de los servidores y servidoras, contratistas o usuarios de los recursos tecnológicos de la CDMB, dará lugar a la respectiva investigación de carácter disciplinaria, civil, penal y fiscal a que haya lugar.

6. POLÍTICAS

6.1 POLÍTICAS GENERALES DEFINIDAS POR LA COORDINACIÓN DE T.I.

- El proceso de Gestión de Tecnología de la información y la Subdirección Administrativa y Financiera revisa y aprueba todo proyecto tecnológico informático y/o de telecomunicaciones que se vaya a implementar en cualquier proceso del ente central.

- El proceso de Gestión de Tecnología de la información es responsable de definir y establecer los estándares y procedimientos para revisar y aprobar todo proyecto tecnológico informático y/o de telecomunicaciones que se vaya a implementar en cualquier proceso institucional.

- El proceso de Gestión de Tecnología de la información es responsable de definir y establecer los estándares y procedimientos para el desarrollo y mantenimiento de los sistemas de información.

- El proceso de Gestión de Tecnología de la información es responsable de evaluar y determinar las características técnicas necesarias para la adquisición de equipos de cómputo, equipos de telecomunicaciones y otros elementos, conforme a las mejoras prácticas y normas de seguridad informática.

- El proceso de Gestión de Tecnología de la información debe adoptar planes de mantenimiento para los sistemas de información y los elementos de la infraestructura tecnológica, que se ejecutarán de acuerdo a los lineamientos descritos en los mismos.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

- La CDMB ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

6.2 PROCESO GESTIÓN SOLUCIONES DE T.I.

6.2.1 Adquisición de Hardware.

- Las subdirecciones o coordinaciones remitirán al proceso de Tecnologías de la Información, acorde con las especificaciones diseñadas por ésta, sus necesidades de hardware para la gestión de los procesos de adquisición, con las debidas justificaciones y la respectiva transferencia de recursos.
- Para la adquisición de hardware, El proceso de Tecnologías de la Información evaluará los requisitos mínimos que se requieren para satisfacción de las necesidades de los Procesos en la CDMB y las tendencias tecnológicas del momento.

- El grupo de Tecnología de la Información gestiona la asignación de los equipos informáticos y telecomunicaciones u otros componentes que son entregados a los servidores, según las necesidades se renovación de equipos informáticos.

- En Almacén e Inventarios debe recepcionar los equipos informáticos y de telecomunicaciones de acuerdo con las directrices del proceso y las especificaciones técnicas establecidas en los contratos apoyados con el proceso de Tecnologías de la Información

6.2.2 Adquisición de Software.

- Las diferentes subdirecciones o dependencias remitirán al proceso de Tecnologías de la Información, acorde con las especificaciones diseñadas por ésta, las necesidades de licenciamiento de software (básico, especializado y utilitario) para la gestión de los procesos de adquisición, con las debidas justificaciones y la respectiva transferencia de recursos.

- El proceso de Tecnologías de la Información aplicará las mejores prácticas para la adquisición de programas especializados, con el fin de dar mayor cobertura a las necesidades y exigencias de los servidores públicos y los ciudadanos.

- El software adquirido debe estar amparado por las respectivas licencias de funcionamiento y debe contener la documentación técnica y operativa necesaria para permitir su operación y mantenimiento, soporte o la capacitación respectiva sobre el manejo del mismo.

- Se deberán adquirir las últimas versiones liberadas de los productos seleccionados y sólo en determinados casos, bajo situaciones específicas, la Subdirección Administrativa y Financiera, podrá autorizar su adquisición de forma distinta.

- En el momento de adquirir licencias para software especializado o de tipo OEM, se deberá tener en cuenta la actualización, la cual deberá ser comprada al momento de adquirir las licencias.

- Para la adquisición o desarrollo de sistemas hechos a la medida, éstos deben ajustarse al modelo de datos y a los estándares de desarrollo adoptados por la CDMB con el fin de garantizar la integridad, confiabilidad y seguridad de los mismos; igualmente deben obedecer a formar partes de las diferentes actividades de los procesos de la entidad, de ser nuevas actividades debe existir la formalización de estas actividades dentro del proceso a que hace referencia en el SIGC.

- Los Sistemas de Información deberán estar diseñados de una manera que posibiliten la integración con otros aplicativos que posea la CDMB.

- En los procesos de contratación de desarrollo de software específico o a la medida, la titularidad de todos los derechos patrimoniales sobre el conjunto del software aplicativo, código fuente, código ejecutable, las bases de datos, las interfaces, los componentes, la documentación y demás partes que se generen del sistema según los términos de referencia, corresponderán exclusivamente a la CDMB, por lo anterior la empresa contratista deberá transferir o ceder los derechos patrimoniales a la CDMB quien será su único propietario y no la empresa desarrolladora ni de los ingenieros de desarrollo.
- En el caso eventual que alguna dependencia realice una implementación sin el cumplimiento de lo estipulado por las políticas de TI, la Subdirección Administrativa y Financiera no tendrá ninguna responsabilidad sobre el soporte y mantenimiento de dichos aplicativos.

- En caso de ser absolutamente necesario el uso de software libre, se deberán tener en cuenta los siguientes aspectos para su adquisición y utilización:

  - Debe ser solicitado con justificación por el líder del área que lo requiere.
  - Tener el aval del proceso de Tecnologías de la Información para su instalación.
  - El programa debe cumplir con los requerimientos técnicos o necesidades de la dependencia solicitante.
  - El programa debe ser técnicamente compatible con el hardware y software de la CDMB. Debe ser actualizable y tener soporte técnico.
  - El programa debe ser escalable en sus funciones y garantizar la conservación de la información, propiedad intelectual y patentes.
  - El programa debe incluir la libertad de su utilización para beneficios de la organización y la modificación de su código fuente.
  - Se deberán dejar las condiciones plasmadas al adquirir la licencia, relativas a derechos y deberes de las partes, proveedor y usuario, bajo las cuales se distribuye.

6.2.3 Asignación de cuentas de usuario en el ERP.

- La asignación de usuarios y contraseñas en el sistema productivo ERP son de carácter personal e intransferible, por tanto la asignación de la cuenta dependerá de la disponibilidad de licencias que se tenga en el momento.
- No se asignarán claves en producción a consultores u otros terceros, diferentes a los usuarios finales autorizados por las dependencias.

6.2.4 Uso de las cuentas de usuario en el ERP.

- El usuario y la contraseña del sistema ERP son de uso personal e intransferible.

- El uso de una misma contraseña por varias personas o en varios equipos simultáneamente, se considera por la CDMB como una violación a la seguridad de la información, por lo que podría generar sanciones para los funcionarios dueños de las cuentas de usuario.

- Cada servidor o servidora es responsable de la información que se registre en el sistema ERP con su usuario.

- El sistema de información ERP solicitará automáticamente a cada usuario el cambio de contraseña cada 60 días. Para el cambio de contraseña, se debe considerar que esta debe ser diferente a las cinco contraseñas utilizadas anteriormente.

- El proceso de Tecnologías de la Información debe verificar periódicamente el correcto uso de las cuentas de usuario.

6.2.5 Gestión de incidentes y requerimientos en el sistema de información ERP.

- Los incidentes y requerimientos relacionados con el sistema ERP, deben ser reportados siempre por la herramienta de mesa de ayuda.

- Las labores continuas sobre el sistema de información ERP, dan origen a necesidades de solución de incidentes en la operación o nuevos requerimientos; para la atención a estas necesidades, el proceso de TI se apoya en un esquema de atención por niveles, con el objetivo de prestar un servicio escalonado en la medida de la complejidad del requerimiento.

- El proceso de TI atenderá los incidentes y requerimientos que sean registrados en la herramienta de gestión que opere la mesa de servicios.

- El proceso de TI es responsable del entrenamiento masivo a los servidores en los módulos del sistema ERP que utiliza la CDMB.

6.3 GESTIÓN DE INFRAESTRUCTURA DE T.I.

6.3.1 Uso/Instalación/Desinstalación de software.

- El proceso de Tecnologías de la Información es responsable de realizar la instalación, soporte, actualización y/o mantenimiento de software licenciado (básico o especializado), únicamente en los equipos que pertenecen a la infraestructura tecnológica de la CDMB.

- Las solicitudes para instalación de software se realizan a través de la herramienta de gestión utilizando el formato correspondiente. Los contratistas y practicantes no están autorizados para realizar este tipo de solicitudes.

- Ningún servidor público está facultados para usar, distribuir e instalar software que carezca de la licencia apropiada. Quien lo haga, incurrirá en violación a las políticas de operación relacionadas con seguridad de la información.

- En los equipos de la CDMB, no deberá instalarse ningún tipo de programa o software descargado por Internet u obtenido por otro medio, incluyendo software gratuito; a menos que exista autorización previa del Subdirector de la dependencia solicitante y de la Subdirección Administrativa y Financiera responsable de verificar la necesidad de licencia y de instalación para dicho software.

- Los servidores públicos deben respetar los derechos de la propiedad intelectual y utilizar el software propiedad de la CDMB de forma diligente, correcta y lícita; y se abstendrán de utilizarlo con fines contrarios a la ley o con fines de lucro.

- El software de mensajería instantánea, de chat, redes sociales u otros similares, es restringido y solo se autorizará una vez revisada y aprobada la solicitud y justificación de uso, la cual debe ser realizada por el respectivo líder del área en la cual se utilizará.

- Para la instalación de software especializado, los equipos de cómputo deberán cumplir con las especificaciones mínimas de hardware, definidas por la Subdirección Administrativa y Financiera

- Es responsabilidad de la Subdirección Administrativa y Financiera definir la lista de software autorizado y realizar un control exacto y estricto del licenciamiento.
- La Subdirección Administrativa y Financiera debe coordinar los planes de capacitación en software para los servidores y servidoras que lo requieran.

- Cuando se trate de software de pruebas, la mesa de servicios debe realizar la desinstalación una vez terminen las pruebas y devolver los medios al proceso de Tecnologías de la Información para su respectivo control.

- El proceso de Tecnologías de la Información es responsable de realizar revisiones periódicas para asegurar que sólo programas o software con licencia estén instalados en los equipos de la CDMB.

- El proceso de Tecnologías de la Información se reserva el derecho de retirar las licencias de software, en cualquier momento, a aquellos usuarios que hagan uso indebido del software o que incumplan total o parcialmente los términos de uso.

6.3.2 Administración de servidores.

- Cualquier servicio que se requiera configurar manualmente con una cuenta o tarea programada, se deberá hacer siempre a través de la mesa de servicios.

- El acceso remoto a los Servidores deberá realizarse con cuentas diferentes a la personal, definidas de acuerdo a los estándares vigentes.

6.3.3 Gestión de incidentes y requerimientos.

- La mesa de servicios constituye el único punto de contacto para reportar los incidentes o requerimientos a través de la herramienta de gestión.

- Solamente serán atendidos los incidentes y requerimientos que tengan asignado un número de ticket. No se acogerán solicitudes reportadas a través de otro medio.

- La atención de incidentes y requerimientos se realizará de acuerdo a las prioridades y tiempos de solución establecidos en los Acuerdos de Niveles de Servicio (ANS).

- El avance o reasignación de un incidente o requerimiento debe ser registrado en la herramienta de gestión para conocimiento de los usuarios.

- La base del conocimiento de la herramienta de gestión constituye una fuente de información que debe ser consultada por el personal de soporte para la solución de incidentes complejos y por los usuarios del servicio para la utilización de los formatos que se deben anexar a las diferentes solicitudes.

- Para dar atención a un incidente o requerimiento, a través de soporte telefónico, remoto o presencial, es necesario que el usuario que lo reportó se encuentre disponible. La intervención del Analista para dar atención, requiere de la presencia del responsable del equipo o de la persona en quien éste delegue.

- Para proceder al cierre de un incidente, luego de haber sido solucionado, el usuario debe entrar a la mesa de servicios y calificar el servicio a través de la encuesta de satisfacción.

6.3.4 Gestión de Cambios.

- El solicitante de un cambio puede ser un servidor, servidora o contratista de la CDMB, que de acuerdo con una necesidad, hace un requerimiento para modificar el estado de un componente de la Infraestructura Tecnológica.

- Las solicitudes de cambio deben ser reportadas a través de la herramienta de gestión diligenciando el formato establecido para ello.

- Únicamente el Comité de Cambios es el responsable de evaluar las solicitudes de cambios para su aprobación o rechazo.

- De acuerdo al impacto del cambio sobre el servicio, este siempre debe ser comunicado a los usuarios.

- Posterior a la ejecución de cualquier cambio, se debe comunicar a todos los implicados el estado del cambio y la manera en que el cambio se vio reflejado en la plataforma.

- Todos los cambios aprobados deben ser implementados en horarios no laborales; si por cualquier razón algún cambio se debe realizar en horario laboral, se debe garantizar que su implementación se llevará a cabo sin alterar los procesos involucrados y minimizando la interrupción de los servicios.

6.3.5 Gestión de Cuentas de Usuarios

- Las cuentas de red para contratistas dela CDMB, funcionarios con vinculación en carrera administrativa, provisionalidad, libre nombramiento y remoción, deben ser creadas o eliminadas a partir de las notificaciones enviadas a la mesa de servicios, por la Coordinación de Procesos Contractuales o Gestión del Talento Humano

- Las solicitudes para creación de cuentas de red de contratistas, practicantes de excelencia o personal educativo, sólo deben ser realizadas por subdirectores o coordinadores de oficina, a través de la herramienta de gestión y diligenciando el formato correspondiente.

- Los datos diligenciados en el formato para la creación de contratistas, practicantes de excelencia y personal educativo, deben ser acordes con el nombre (s) y apellido (s).

- Las cuentas de red de los contratistas, practicantes o judicantes caducan el día de terminación del contrato o en la fecha establecida para terminación de labores. En caso de darse la continuidad contractual, se debe solicitar su prorroga generando un caso en la herramienta de gestión.

- Las cuentas y buzones de correo de servidores nombrados en Comisión de Servicios, serán desactivadas durante el período que perdure la Comisión, si ésta se cumple en un organismo diferente a la CDMB y serán reactivadas una vez el Gestión de Talento Humano notifique el reingreso del servidor.

- Los permisos o privilegios asociados a la cuenta de un servidor público deben ser modificados o removidos cuándo éste cambie de rol o cuando éste se desvincule de la entidad.

6.3.6 Mantenimiento de equipos de cómputo.

- Todos los usuarios son responsables de informar a la mesa de servicios, cualquier falla o anomalía respecto al funcionamiento de los equipos de cómputo a su cargo, generando un caso en la herramienta de gestión. No se atenderán solicitudes de mantenimiento que se reporten por una vía diferente a la herramienta de gestión.

- El mantenimiento preventivo y correctivo de los equipos de cómputo de la CDMB está bajo responsabilidad de la mesa de servicios. Ninguna persona ajena está autorizada para realizar estas labores.

- La mesa de servicios no está autorizada para dar mantenimiento a equipos de cómputo que no pertenezcan a los activos tecnológicos de la CDMB.

- El personal técnico de la mesa de servicios tiene la autoridad para acceder a archivos individuales o datos cada vez que se realice un mantenimiento, reparación o chequeo masivo de equipos de cómputo. Sin embargo, no puede exceder su autoridad en ninguna de estas eventualidades, para usar esta información con propósitos diferentes a los de mantenimiento o reparación.

- Si un equipo requiere ser manipulado por personal del Laboratorio, el usuario tendrá la responsabilidad de ejecutar el respaldo de su información previamente.

- En el caso de solicitar un mantenimiento preventivo y correctivo masivo de los equipos de cómputo, éste debe ser programado y supervisado por el personal de la mesa de ayuda, con el acuerdo de las áreas afectadas, para evitar así retrasos e inconvenientes en los servicios y actividades de la organización.

6.3.7 Telecomunicaciones.

- Todos los requerimientos relacionados con la instalación o modificación de la infraestructura de telecomunicaciones (cableado estructurado, telefonía IP, enlaces de comunicación entre sedes), deben ser realizados a través de la herramienta de gestión.

- Cualquier proyecto que involucre la infraestructura de Telecomunicaciones (cableado estructurado, telefonía IP, enlaces de comunicación entre sedes) de la CDMB, debe ser reportado a la Administrativa y Financiera para su estudio, aprobación y acompañamiento durante el proceso.

- La manipulación y configuración de los equipos activos de red de la CDMB es responsabilidad de Subdirección Administrativa y Financiera a través del grupo de Tecnologías de la Información de la mesa de servicios.

- Sólo personal autorizado por la Subdirección Administrativa y Financiera puede hacer modificaciones en la infraestructura de red.

- Todo cambio o manipulación de los equipos de red que pueda alterar la disponibilidad de los servicios, debe ser aprobado por el Comité de Cambios.

- El ingreso de dispositivos móviles al dominio de la red corporativa se realiza solo con previa autorización de la Subdirección Administrativa y Financiera

6.3.8 Acceso al Centro de Datos (Data Center).

- El proceso de tecnologías de la información es el responsable de definir el personal que, por sus funciones, requiere acceso permanente al Data Center.

- Es responsabilidad del personal autorizado mediante credencial, el cuidado y buen uso de la misma. Quien haga uso indebido de ésta se le retirará y se hará acreedor a las sanciones administrativas y disciplinarias.

- En caso de extravío o daño de la credencial, deberá reportarse inmediatamente al proceso de tecnologías de información para realizar el trámite correspondiente y la generación de una nueva.

- El ingreso al Datacenter de personas externas a la CDMB debe ser aprobado por el proceso de tecnologías de información y se realizará con el acompañamiento de una persona autorizada con credencial, previo registro en la planilla “Control de acceso al Data Center”. Su permanencia dentro del Datacenter, será controlada

- Ninguna persona, sin excepción, podrá ingresar al Datacenter sin la respectiva autorización.

- Es obligación de las personas autorizadas mediante credencial, notificar a la mayor brevedad posible al proceso de tecnologías de información, sobre cambios en sus obligaciones o actividades, que impliquen su desvinculación con el funcionamiento del Datacenter. Por lo anterior deberá presentar comunicación escrita, acompañada de la tarjeta magnética asignada.

- Para la instalación de equipos dentro del Datacenter, los técnicos autorizados deben realizar las actividades de ensamble, configuración y puesta a punto de los equipos, previa a la instalación dentro del Datacenter. Una vez se finalicen los trabajos se autorizará el ingreso al Datacenter. Los técnicos deberán asegurarse que todos los cables queden bien instalados y ordenados.

- El personal de mantenimiento o de limpieza del edificio, debe ser identificado plenamente, así como controlado y vigilado en sus actividades durante su permanencia en el Datacenter.

Normas de seguridad de cumplimiento obligatorio

Las personas autorizadas para ingresar al DataCenter deberán de cumplir con las normas de seguridad establecidas en el proceso de seguridad de la Información

- Introducir material magnético, inflamable o peligroso.
- Introducir armas o explosivos
- Introducir químicos o drogas ilegales.
- Introducir alimentos o cualquier tipo de bebidas.
- Introducir materiales radioactivos
- Cualquier otro artículo similar a los antes mencionados, que a consideración de la CDMB sea peligroso o dañino.
- Arrastrar objetos sobre el piso falso.
- Colocar cualquier tipo de elemento sobre los equipos.
- Utilizar cámaras fotográficas o cámaras de video.
- Alterar la configuración de los equipos o dispositivos.
- Sustraer material del Datacenter sin autorización.

- Alterar el orden o disposición de los elementos al interior del Datacenter.
- Fumar dentro del Datacenter.
- Usar taladros o similares en el Datacenter, sin autorización y acompañamiento.
- Utilizar la puerta de emergencia para abandonar el Datacenter, salvo cuando se trate de un evento que obligue su utilización.

6.4 PROCESO SEGURIDAD DE LA INFORMACIÓN

6.4.1 Administración de la plataforma de TI.

- El Grupo de Tecnología de la Información es la responsable de verificar que las políticas de seguridad en la red y en los equipos de cómputo de la CDMB, se lleven a cabo en forma correcta para optimizar su uso.

- Se debe llevar registro de los incidentes de seguridad más relevantes, así como de los eventos que afectan la plataforma de tecnología o sus servicios.

- El Grupo de TI debe definir un plan de mantenimiento para todas las bitácoras de sistemas de la organización en donde se determinen los tiempos de rotación, revisión, mantenimiento y eliminación de las mismas.

- Se deben definir los límites y conductos de comunicación de la administración de la plataforma de tecnología, tanto al interior como con entidades externas que interactúen con ella.

- Todo acceso remoto a un equipo de un usuario debe hacerse sólo con la autorización del usuario, por medio del programa que se utilice para establecer este tipo de conexión que cumpla con las condiciones de un canal de comunicación seguro.

- Antes de realizar cualquier cambio en la plataforma de tecnología, se deben tener backups de los dispositivos impactados, de manera que se pueda garantizar un plan de retorno completo en caso de ser necesario.

- Cualquier actividad en un ambiente de producción debe estar previamente detallada y aprobada por el Comité de Cambios, de manera que se minimice el impacto sobre los servicios afectados.

- Se debe garantizar la transferencia de conocimiento al interior de la organización para las labores de operación y administración de la plataforma.

- Todo personal que haga parte de las labores de administración de la plataforma de tecnología de la información, debe tener el conocimiento, experiencia y las capacidades idóneas para su correcta operación.

- Sólo personal autorizado tiene acceso a los dispositivos de la plataforma tecnológica de la CDMB con el usuario de administración definido por la Subdirección Administrativa y Financiera Este usuario es de uso personal e intransferible.

- La solicitud para cambio sobre las credenciales de cualquier usuario de un sistema de información debe ser realizada directamente por el propietario de la cuenta.

6.4.2 Usuarios y contraseñas.

- Todos los servidores, servidoras de la CDMB son responsables del adecuado uso y administración de sus cuentas y contraseñas de acceso a los diferentes recursos informáticos; en todos los casos, serán responsables de cualquier transacción que se realice utilizando su cuenta.

- Ningún usuario podrá revelar la contraseña a personal no autorizado o permitir su uso a terceros para actividades ajenas a la misión de la CDMB.

- El usuario debe cambiar la contraseña periódicamente según los requerimientos del sistema o cuando lo considere necesario.

- Los sistemas de información en donde se almacenen las credenciales de los usuarios deberán estar adecuadamente protegidos para evitar el acceso no autorizado.

- Las contraseñas utilizadas por los usuarios deben cumplir con los estándares establecidos por la Subdirección Administrativa y Financiera para la creación de contraseñas.

- Las contraseñas que estén asociadas a sistemas de información o aplicaciones nuevas deben ser cambiadas después de la primera vez de validación.

6.4.3 Uso aceptable de los recursos informáticos.

6.4.3.1 Computadores y portátiles

- Los servidores públicos son responsables del uso correcto y adecuado de los computadores, portátiles y demás elementos de cómputo entregados para el desarrollo de sus labores.

- Los equipos de cómputo que son asignados a los servidores para el desarrollo de sus actividades pertenecen a la dependencia específica. En caso que el servidor sea trasladado, estos equipos deben conservarse en la dependencia de origen.

- Ningún equipo puede ser trasladado sin autorización. Los traslados o cambios físicos deben ser efectuados únicamente por el personal de soporte de la mesa de servicios que cumplan con los requisitos para ello.

- No se permite retirar de las instalaciones de la CDMB o sedes externas, equipos de cómputo u otros dispositivos sin la debida autorización de la de la Subdirección Administrativa y Financiera.

- Los equipos de cómputo no deberán permanecer guardados o almacenados en las áreas de trabajo.

- El uso de medios de almacenamiento removibles (USB, reproductores mp3, entre otros), es de absoluta responsabilidad de los usuarios, quienes deben verificar que estos dispositivos se encuentren libres de virus o código malicioso, antes de utilizarlos en los equipos de la CDMB. No obstante, El proceso de Tecnología de la Información se reserva el derecho de bloquear en cualquier momento el uso de estos dispositivos si se detecta su uso indebido o que puedan afectar la seguridad de la información en la entidad.

- Los usuarios que requieran descargar de su inventario un elemento informático (teléfono, computador de escritorio, computador portátil, impresora, entre otros.), deberán tramitarlo mediante memorando al Grupo de TI para que este pueda ser reasignado de estar en buenas condiciones de operación.

- Cuando por alguna causa razonable determinada, se presuma el uso indebido de un computador o portátil, el proceso de Tecnología de la Información puede acceder cualquier cuenta, datos, archivos, o servicio de información perteneciente a el(los) involucrado(s) en el incidente, para investigar y aplicar las sanciones a que hubiere lugar, manteniendo siempre el debido proceso.

- La Subdirección Administrativa y Financiera debe monitorear constantemente los computadores y portátiles de la entidad a través de los medios correspondientes, para responder oportunamente frente a cualquier acción que atente contra la disponibilidad, seguridad o desempeño correcto de los mismos.

- La CDMB, no será responsable por las transacciones financieras electrónicas que realicen los empleados desde el computador asignado o desde cualquier computador que esté disponible para uso público y se encuentre en las instalaciones de la CDMB.

- La CDMB, permitirá, en cierto límite, el almacenamiento de información personal en los discos duros de los computadores asignados a cada empleado o contratista, sin embargo, no será responsable de dicha información ni se ejecutarán esfuerzos tendientes a su recuperación. Esta información no debe exceder del 10% de la capacidad del disco duro o máximo 20Gb, cumpliéndose siempre el de menor capacidad según la configuración del equipo asignado.

Prohibiciones

- Utilizar los equipos de cómputo de la CDMB para visualizar o almacenar material no permitido y/o obsceno o campañas políticas o publicitarias.

- Suplantar la identidad de otra persona ya sea física, telefónicamente o a través de cualquiera de los sistemas de información (por ejemplo correos o mensajes de texto).

- Fumar, comer, ingerir alimentos o colocar líquidos cerca a los equipos o elementos informáticos.

- Intentar o realizar accesos a cuentas de usuario que no sean las propias (utilizando cualquier protocolo o programa, telnet, ftp, etc.).

- Tener acceso o intentar modificar archivos, contraseñas o datos que pertenecen a otros.

- Utilizar los equipos de la entidad para introducir virus computacionales, programas espías o cualquier otro programa diseñado para dañar los equipos o el software utilizado en la CDMB, o de cualquier manera, arriesgar la seguridad de los equipos o la red institucional.

- Exportar los archivos de contraseñas o realizar cualquier manipulación sobre los mismos, en concreto, intentar averiguar las contraseñas de otros usuarios.

- Afectar o paralizar algún servicio por la ejecución o intento de ejecución de programas indebidos.

- Acceder, analizar o exportar archivos que sean accesibles a todo el mundo pero que no sean del usuario, salvo que se encuentre en una ubicación que admita su uso público.

- Instalar y configurar equipos o sistemas que puedan afectar o interrumpir el funcionamiento de la red.

- Dañar física o lógicamente los equipos o la infraestructura informática.

- Utilizar cualquiera de los recursos informáticos de la CDMB para fines diferentes a las funciones inherentes al empleo o a las contractuales.

6.4.3.2 Uso del Correo Electrónico Institucional

- El correo electrónico institucional de la CDMB debe ser utilizado únicamente para propósitos laborales.

- Los servidores públicos de la CDMB son completamente responsables de las actividades realizadas con sus cuentas de acceso y su buzón de correo.

- Ya que los buzones de correo tienen una capacidad de almacenamiento limitada, los usuarios deben verificar y depurar periódicamente su buzón con el fin de garantizar la recepción de nuevos correos.

- En caso de ausencia prolongada o vacaciones de un servidor público, se debe recurrir a mecanismos alternos como redirección de mensajes. En ningún caso se deben utilizar las cuentas de correo electrónico pertenecientes a otras personas.

- Los servidores que identifiquen en su correo contenido sospecho o con posibles virus, deben notificarlo a la Mesa de ayuda.

- La cuenta de correo electrónico cuenta con una capacidad máxima de 20 Mbytes para buzón y envío, en caso de requerir de una capacidad mayor a la mencionada, se debe solicitar al proceso de Tecnologías de información mediante oficio o correo debidamente justificado y autorizado por el Subdirector o coordinador de la oficina respectiva.

- Se prohíbe el envío de mensajes personales u ofensivos; injuriosos, cadenas de mensajes o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el nombre de la CDMB.

- Los mensajes de correo electrónico deben ser considerados como documentos formales; por lo tanto, se deben respetar los lineamientos y recomendaciones establecidos para este tipo de documentos.

- Al enviar un correo, se debe evitar el uso de las opciones de confirmación de entrega y lectura, a menos que sea un mensaje demasiado importante; ya que esto puede provocar tráfico en la red.

- Para envió de información masiva y/o institucional, que por necesidades especificas de un área requieran ser enviados a toda la CDMB, debe manejarse únicamente por medio del correo electrónico institucional. Este envió debe ser autorizado por el grupo de Comunicaciones y enviado a través de los correos autorizados para este fin. No se deben utilizar cuentas de correo electrónico personales para estos propósitos. El Grupo de Tecnología enviará los mensajes de carácter técnico especial de forma masiva de ser requeridos.

- En lo posible, el correo electrónico debe ser el medio por el cual se deben manejar las comunicaciones de la entidad, disminuyendo el manejo de documentación impresa; se recomienda al usuario incluir al final de sus correos el mensaje: “No imprima este correo a menos que sea absolutamente necesario. El medio ambiente es cosa de todos” o “Gracias por considerar el medio ambiente antes de imprimir este documento.”

6.4.3.3 Acceso a internet.

- El acceso a internet estará controlado con políticas de acceso y deberá estar autorizado por los correspondientes Subdirectores o Jefes de Oficina donde se especifique su necesidad.

- Está estrictamente prohibido cualquier uso de internet con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral que dio origen a la habilitación del servicio, en caso de ser detectado esta actividad de procederá a la suspensión temporal o definitiva de este servicio.

- No se permite el acceso a páginas de entretenimiento o páginas que contengan material discriminatorio, difamatorio, consumidor de ancho de banda, no productivo, acosador, ofensivo, pornográfico u obsceno. La Subdirección Administrativa y Financiera se reserva el derecho de utilizar software que permita identificar y bloquear el acceso a estos sitios.

- Si bien la Subdirección Administrativa y Financiera es responsable del uso de programas anti-virus, no puede garantizar que los sitios de Internet visitados por los usuarios carezcan de virus o código malicioso, por lo que no se permite, en ningún caso, la descarga de archivos o programas de cualquier tipo; de ser requeridos se debe realizar la correspondiente solicitud utilizando la mesa de ayuda (SHD).

6.4.3.4 Computadores con internet móvil

- La solicitud de aprobación de este servicio se deberá realizar a través de la herramienta de gestión disponible, y por intermedio del Subdirectores.

- La autorización de instalación del servicio la deberá realizar la Subdirección Administrativa y Financiera de acuerdo a las condiciones solicitadas y garantizando el cumplimiento de esta política.

- La asignación del servicio de internet móvil estará sujeta a un equipo previamente autorizado perteneciente a la CDMB, para su utilización en actividades administrativas.

- La utilización de acceso a internet móvil, deberá estar limitada al uso para el cual fue solicitado dicho servicio.

- No se permite el acceso a los equipos con credenciales administrativas.

- Los equipos no deberán estar configurados para acceso sin credenciales.

- Las políticas de navegación configuradas para estos equipos deberán ser iguales o más restrictivas a las configuradas en el proxy central de la Administración.

- Las opciones de configuración del navegador deberán ser establecidas con el fin de minimizar la posibilidad de reconfiguración de estas por parte del usuario o de un tercero.

- El antivirus y cualquier otro sistema de seguridad deberán estar configurados con el nivel máximo de seguridad.

- La instalación y configuración de los equipos se debe realizar de tal forma que se aseguren las actualizaciones automáticas críticas.

- Todas las políticas y controles se deberán configurar por la Subdirección Administrativa y Financiera en aras de garantizar y mitigar riesgo de seguridad de estos equipos.

6.4.3.5 Recurso de conexión VPN.

- El servicio de VPN es administrado por la Subdirección Administrativa y Financiera por ende es responsabilidad de ésta velar por su uso adecuado y controlado.

- El servicio de VPN será asignado a los servidores, contratistas o consultores de la CDMB, quienes para el desarrollo de sus actividades lo requieran según lo determine el Líder de Proyecto o el Líder del Programa al cual pertenezca, quien a su vez debe realizar la solicitud debidamente justificada a través de la herramienta de gestión diligenciando el formato establecido para ello.

- El uso de la cuenta asignada para el servicio es responsabilidad de quien la solicita; de igual manera la solicitud para activación, modificación o retiro de los permisos asignados.

- La fecha de caducidad de la cuenta VPN asignada a usuarios que no se encuentren en los servicios de directorio de la red de cómputo, no podrá superar la fecha de vencimiento del contrato.

- La cuenta VPN asignada a usuarios que se encuentran en los servicios de directorio, caducará con el vencimiento de su cuenta de usuario en el servicio de directorio.

- El uso de VPN sobre servidores, equipos de comunicaciones, almacenamiento, backup y demás elementos de la infraestructura de TI sólo se otorgará al personal que defina la Subdirección Administrativa y Financiera.

- El uso de VPN sobre los servidores, sólo se otorgará para ambientes de desarrollo. Para ambientes de producción, el tiempo será limitado sin superar las 24 horas y bajo la supervisión de personal de Tecnología de la Información o de quien ésta delegue.

- La clave de acceso, se enviará en un archivo cifrado al correo electrónico registrado en el formato de solicitud.

- La cuenta de acceso es de uso exclusivo para quien se le ha asignado los permisos o privilegios del servicio.

- Las cuentas VPN que no se utilicen durante un periodo superior a 90 días calendario serán eliminadas, cumplido este tiempo.

- Para otorgar una cuenta VPN, debe indicarse claramente los recursos tecnológicos a los cuales se va a acceder, puertos y servicios asociados. De igual forma, una descripción clara de lo que se desee trabajar. Todo esto previa autorización del personal del proceso de Tecnologías de la Información.

6.4.4 Confidencialidad de la información

- La transferencia de información de carácter sensible y/o confidencial de la CDMB hacia otra empresa o persona externa debe hacerse a través de un contrato en el que se incluyan especificaciones sobre el tipo de información que será suministrada y acuerdos de confidencialidad entre las partes.

- Toda cláusula de confidencialidad debe ser siempre revisada y aprobada por la oficina Jurídica.

- Bajo ninguna circunstancia las empresas o personas externas distribuirán o utilizarán la información confidencial entregada por la CDMB para fines diferentes a los especificados en las cláusulas de confidencialidad.

- Los proveedores o personas externas que ingresen a la CDMB y tengan acceso a información sensible o a la infraestructura tecnológica deberán acogerse a las políticas de seguridad de la información y a los controles establecidos en cuanto a niveles de acceso, horarios y caducidad de los mismos.

- Los proveedores y empresas consultoras de la CDMB deberán mantenerse actualizados sobre las políticas de seguridad vigentes para dar un buen manejo a los activos de información. Al terminar el vínculo laboral de los servidores y servidoras con la organización

- La terminación laboral de los servidores y servidoras con la organización debe seguir el procedimiento establecido de manera que se denieguen los accesos a todos los sistemas de información inmediatamente.

- Al finalizar un contrato con un proveedor, se debe garantizar que los accesos a la información sensible institucional sean restringidos totalmente.

6.4.5 Gestión de continuidad del negocio.

- Se deben desarrollar planes de recuperación de desastres para los sistemas o procesos críticos que presenten niveles de riesgo no aceptables para el negocio. Estos planes deben ser incluidos por la Subdirección Administrativa y Financiera dentro de la estrategia de continuidad del negocio.

- El proceso de TI debe tener claramente identificado los activos involucrados, las amenazas y el impacto sobre los activos para definir el Plan de Continuidad del negocio.

- Cada área responsable de sus procesos, deberá realizar pruebas periódicas al Plan de Continuidad del negocio.

6.4.6 Gestión de Incidentes de Seguridad

- Cualquier evento de seguridad que atente contra la imagen corporativa o la seguridad de la información institucional, debe ser atendido oportunamente por el área de TI, conforme a los procedimientos establecidos y leyes que le apliquen.

- Todo acceso no autorizado a sistemas de información, deberá efectuarse sólo como parte de un proceso legal iniciado por control interno, después de efectuarse una cadena de custodia y tener la aprobación fiscal.

- El proceso de TI es responsable de atender los incidentes de seguridad de acuerdo a los procedimientos establecidos al interior de la CDMB. En caso de requerir escalamiento con entidades externas como proveedores de Internet, policía u otras entidades de emergencia o disciplinarias, se deben seguir los conductos dispuestos para tales casos.