CONCEJO DE BOGOTÁ, D.C.

RESOLUCIÓN No. 866 DEL AÑO 2008

(17-Octubre-2008)

"POR LA CUAL SE ADOPTAN LAS POLÍTICAS DE SEGURIDAD EN SISTEMAS DE COMPUTO PARA EL CONCEJO DE BOGOTÁ D.C.."

LA MESA DIRECTIVA DEL CONCEJO DE BOGOTÁ D.C.
En ejercicio de sus atribuciones legales y reglamentarias, especialmente las conferidas en el articulo 12 numerales 1° y 8° del Acuerdo 095 de 2003 y

CONSIDERANDO:

Que la Constitución Política en su Artículo 209 establece: "La Administración Publica, en todos sus órdenes tendrá un Control Interno que se ejercerá en los términos que señale la Ley" y establece los principios de la función pública.

Que el Modelo Estándar de Control Interno para entidades del Estado, se genera tomando como base el articulo primero de la Ley 87 de 1993, el cual se encuentra compuesto por una serie de Subsistemas, Componentes y Elementos de Control.

Que dentro del Subsistema de Control de Gestión de la citada norma en el componente 2.2. Información, se establece como Elemento de Control 2.2.3. lo referente a Sistemas de Información, el cual esta conformado por el conjunto de recursos humanos y tecnológicos utilizados para la generación de información, orientada a soportar de manera mas eficiente la gestión de operaciones en la Entidad Publica.

Que el presente manual tiene como fin definir las políticas Corporativas de Seguridad en Sistemas de Computo en el Concejo de Bogotá D.C.

Que la seguridad forma parte integral de todas las redes de cómputo, ya que la cantidad de datos que se maneja en los sistemas de información, excede nuestra habilidad para protegerlos sin el uso de técnicas automatizadas adecuadas.

Que la apropiación de políticas debe ser hecha por parte de todos los usuarios que acceden a servicios en la red del Concejo de Bogotá, pues de su universalización depende la disminución de riesgos y vulnerabilidades a los que la red se encuentra expuesta.

Que el fin esencial de estas Políticas de Seguridad es generar la base de normas mínimas para el correcto uso de la red del Concejo de Bogotá con un nivel de seguridad que otorgue a los usuarios la confidencialidad, integridad y disponibilidad de información que ellos necesitan, las cuales esperan crear y establecer una educación y una filosofía sobre la postura que debe adoptar el Concejo de Bogotá, con respecto a las amenazas que esta expuesta la red de datos.

Que el objetivo básico es el de proporcionar directrices adecuadas en los 10 dominios de control que establece la norma ISO 17799 a través de políticas claras que logren generar una nueva filosofía institucional con lineamientos que establezcan un limite entre lo que esta o no permitido, forjando una educación que conlleve a un ambiente mas seguro, para garantizar la integridad física y lógica de recursos e información de la red del Concejo de Bogotá.

CONCEJO DE BOGOTÁ, D.C.

RESOLUCIÓN No. 866 DEL AÑO 2008

(17-Octubre-2008)

"POR LA CUAL SE ADOPTAN LAS POLÍTICAS DE SEGURIDAD EN SISTEMAS DE COMPUTO PARA EL CONCEJO DE BOGOTÁ D.C.."

Que es necesario implementar políticas, puesto que los sistemas están expuestos a una serie de riesgos que aumentan a medida que se globalizan las comunicaciones, por lo cual la seguridad se ha convertido en un problema bastante serio, mas aun en entidades donde se maneja información altamente confidencial, como es el caso del Concejo de Bogotá.

Que por tal motivo es necesario adoptar una metodología apropiada, concordante con la Norma ISO 17799, para prevenir y enfrentar esta situación. Ya que el asegurar el sistema disminuye en un alto grado la vulnerabilidad en la información y amplia los beneficios para la Entidad.

Que así mismo, teniendo en cuenta que el más alto riesgo surge al interior de cualquier Institución, y que cada Entidad debe personalizar su forma de protección con una metodología eficiente, el Concejo de Bogotá, adoptara e implementara las políticas de seguridad para contribuir con la protección del sistema y mejorar la integridad de la red y la información.

Que en merito de lo expuesto resuelve:

R E S U E L V E :

ARTÍCULO PRIMERO: Implementar las siguientes Políticas de Seguridad en los Sistemas de Cómputo del **CONCEJO DE BOGOTÁ DISTRITO CAPITAL**, teniendo en cuenta los siguientes aspectos:

1. REVISIÓN Y EVALUACIÓN

La aprobación de estas políticas de Seguridad están condicionadas, en su orden por:

- Responsable del Proceso Recursos Físicos - Sistemas
- Directora Administrativa y Financiera
- Mesa Directiva del Concejo de Bogotá

1.1. ACTUALIZACIÓN

Cualquier actualización, modificación y en general cambio que se realice a estas políticas de seguridad será bajo el estricto control, análisis y supervisión de el jefe de Información y Recursos Físicos- Sistemas, y los entes que figuren como diseñadores y autores de estas, de lo contrario la validez y responsabilidades recaerán sobre quien elabore dichos cambios.

1.2. ESCALABILIDAD

Los diferentes delegados, oficinas y áreas que operen con sus propias redes, computadores o que estén enlazados a la red principal, pueden agregar con la aprobación de Información y Recursos Físicos- Sistemas guías particulares complementarias, pero no pueden bajo ninguna circunstancia contradecir estas políticas.

Si la infraestructura crece en cuanto a la red de datos, tecnología o implementación de nuevas dependencias, departamentos, áreas, sucursales, se pueden aplicar estas mismas políticas, generando algunos posibles anexos donde se especifiquen las nuevas condiciones.

1.3. DELEGADOS DE CONTROL

El área de Información y Recursos Físicos – Sistemas debe crear y consolidar dos delegados, en cabeza del Director Administrativo y Financiero y el encargado del Procesos de Sistemas y cuya función sea controlar el cumplimiento de las políticas de seguridad, investigar y generar reportes para solicitar a los funcionarios el cumplimiento de las políticas definidas para aplicar criterios en el cumplimiento según su juicio cualquier acción que vaya en contra de las mismas.

1.4. SANCIONES

Las sanciones serán analizadas según el criterio de los respectivos delegados de control, así las sanciones serán impuestas por el Concejo de Bogotá, después de haber realizado los procedimientos de investigación y evaluación internos.

Las faltas en las que se incurra al violar estas políticas de seguridad, ocasionaran sanciones disciplinarias a los funcionarios, estas sanciones se evaluaran de acuerdo a las sanciones generales estipuladas por el Concejo de Bogotá, que aplicaran a las presentes políticas.

CONCEJO DE BOGOTÁ, D.C.

RESOLUCIÓN No. 866 DEL AÑO 2008

(17-Octubre-2008)

"POR LA CUAL SE ADOPTAN LAS POLÍTICAS DE SEGURIDAD EN SISTEMAS DE COMPUTO PARA EL CONCEJO DE BOGOTÁ D.C.."

2.- VIGENCIA DE LAS POLITICAS DE SEGURIDAD

- Estas políticas se seguridad entran en vigencia a partir de la fecha de expedición de la presente Resolución.
- Estas políticas deben ser revisadas anualmente por la Dirección Administrativa y Financiera a través de la Oficina de Información y Recursos Físicos – Sistemas, para realizar los respectivos ajustes necesarios.

3.- POLITICAS CLASIFICACIÓN Y CONTROL DE ACTIVOS

- Los recursos disponibles a través de la red serán de uso exclusivo para asuntos relacionados con las actividades del Concejo de Bogotá D.C..
- Corresponde a la Dirección Administrativa y Financiera a través del área de Información y Recursos Físicos - Sistemas administrar mantener y actualizar la infraestructura de la red.
- En concordancia con la ley y de común acuerdo con las políticas generales, Información y Recursos Físicos - Sistemas es el responsable de instalar y administrar el o los servidores Web. Es decir, solo permiten servidores de páginas autorizados por el área de Sistemas.
- El material que aparezca en la página de Internet del Concejo de Bogotá debe ser aprobado por el Comité de página Web del Concejo respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección como los que se aplican a cualquier material impreso).
- Toda información que sea enviada a listas de correo o grupos de discusión no debe llevar el logotipo oficial y deberá siempre responder a un comportamiento profesional y ético.
- La Dirección Administrativa y Financiera a través de la Oficina de Información y Recursos Físicos - Sistemas tiene la facultad de llevar a cabo la revisión periódica de los accesos a los servicios de información y conservar información del trafico.
- Todos los equipos conectados a la red del Concejo de Bogotá, aunque sean propiedad de la persona que lo utiliza, deben ejecutar regularmente el Software de antivirus permitido con la base de datos de virus más actualizada.

CONCEJO DE BOGOTÁ, D.C.

RESOLUCIÓN No. 866 DEL AÑO 2008

(17-Octubre-2008)

"POR LA CUAL SE ADOPTAN LAS POLÍTICAS DE SEGURIDAD EN SISTEMAS DE COMPUTO PARA EL CONCEJO DE BOGOTÁ D.C.."

- La Dirección Administrativa y Financiera a través de la Oficina Información de Recursos Físicos - Sistemas del Concejo de Bogotá, serán los encargados de abrir los anexos (attachments) colocados en los mensajes de correo electrónico que sean recibidos de remitentes desconocidos o sospechosos ya que pueden contener virus.Siga las siguientes recomendaciones para evitar los virus informáticos:

1. Nunca abra archivos extraños o macros anexas de los mensajes de correo electrónico de origen desconocido, borre dichos archivos.
2. Borre los correos de tipo Spam (correos de publicidad distribuidos a muchos destinatarios).
3. Evite compartir archivos o carpetas con acceso de lectura/escritura a menos que sea absolutamente necesario.
4. Siempre revise los diskettes o CDS que vaya a utilizar en su equipo (virus scannig).
5. Regularmente haga una copia de respaldo (backup) de los datos mas importantes que almacene en su equipo

- Se deben crear backups periódicos del Servidor de Correo, de acuerdo a lo establecido por el área de Información y Recursos Físicos – Sistemas.
- No es permitido la distribución e instalación de software sin la licencia de uso adecuado adquirida por el área de Información y Recursos Físicos – Sistemas y acorde a la propiedad intelectual.
- Esta prohibida la copia no autorizada de material protegido por derechos de autor.
- No esta autorizado la introducción de software libre de dudosa procedencia en los equipos de cómputo o en los servidores.
- Se prohíbe la instalación de software o programas que ocasionen conflicto con la configuración de los equipos.
- Cada usuario es responsable de su clave por tal motivo esta prohibido permitir que segundas personas hagan uso de su cuenta. La prohibición incluye familiares y cualquier otra persona.

- Esta prohibido el uso de la infraestructura tecnológica para fines comerciales o algún tipo de acoso, difamación o calumnia.

- Esta prohibido, ejecutar cualquier herramienta o mecanismo o monitoreo de red o realizar el monitoreo de puertos o análisis de trafico de red, por personas diferentes al área de Información y Recursos Físicos - Sistemas.

- Esta prohibido burlar los mecanismos de seguridad, autenticación, autorización o auditoria de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

- Esta prohibido interferir o denegar servicios a usuarios autorizados, así como el uso de comandos o programas o el envió de mensajes con el fin de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

- Se prohíbe el acceso a los sistemas de configuración de los equipos, cualquier cambio en la configuración solo debe ser manipulada por los funcionarios del área de Información y Recursos Físicos – Sistemas.

- Los funcionarios del Concejo de Bogotá que disponen de una cuenta de correo electrónico activa, pueden utilizarla desde los diversos equipos destinados para ello y cumplir las siguientes recomendaciones:

    1. El pasword le será entregado al funcionario.

    2. Es responsabilidad del funcionario mantener la confidencialidad del pasword.

    3. Cada cuenta tendrá un espacio el cual será establecido de acuerdo a las necesidades de la función que el funcionario este desarrollando.

    4. Es responsabilidad del funcionario depurar su cuenta periódicamente para que exista espacio disponible.

    5. La vigencia de la cuenta comprende el periodo de la estadía del funcionario.

    6. El correo anterior a 15 días que este en el buzón de entrada será borrado automáticamente.

    7. Es responsabilidad del funcionario hacer buen uso de su cuenta, entendiendo por buen uso:

        a. El uso de su cuenta con fines laborales.

b. Leer diariamente su correo y borrar aquellos mensajes obsoletos para liberar espacio en su buzón de correo.

c. El uso de un lenguaje apropiado en sus comunicaciones.

d. El respetar las reglas de conducta en la red de Internet para las comunicaciones.

e. No permitir que segundas personas hagan uso de su cuenta.

- El funcionario es responsable de tener backup de sus correos en su equipo a cargo o en su defecto en su cuenta en el servidor de correo.
- El Concejo de Bogotá se reserva el derecho de enviar al usuario la información que considere necesaria como un medio de comunicación institucional.
- El incumplimiento por parte del funcionario del buen uso de su cuenta puede ocasionar la suspensión y/o la cancelación de la misma.
- El área de Información y Recursos Físicos - Sistemas no se compromete a entregar mensajes de correo a cuentas de uso gratuito como Hotmail, Usa.net, correo Web, Yahoo, etc., solo al correo institucional.
- Para cualquier aclaración sobre password es necesario presentarse con carnet vigente en el área de Información y Recursos Físicos – Sistemas.

4.- POLITICAS SEGURIDAD DEL PERSONAL

- Todo usuario de la red del Concejo de Bogotá deben utilizar los recursos informáticos con criterios de racionalidad y únicamente para las labores propias de su función o en beneficio de la Corporación.
- Todo usuario de la red del Concejo de Bogotá debe cumplir las normas, los procedimientos y estándares establecidos y velar por su adopción en su área de influencia.
- Cada usuario que pertenezca al dominio debe tener una cuenta para poder acceder a la red y utilizar los recursos de dominio.
- Los administradores crean cuentas asignando un nombre, especificando datos de identidad y definiendo los derechos del usuario en el sistema.

- Cada cuenta incluye información del usuario, grupos a los que pertenece e información de las directivas de seguridad

- Todo usuario de la red del Concejo de Bogotá debe responder por los recursos informáticos (hardware, software, documentación, suministros, etc.) que le sean asignados de acuerdo con las normas del Concejo sobre el manejo de activos fijos.

- Todo funcionario del Concejo de Bogotá, que tenga a su cargo recursos informáticos será responsable por la aplicación de las medidas de seguridad establecidas por el área de Información y Recursos Físicos - Sistemas.

- Todo funcionario del Concejo de Bogotá debe responder por el adecuado manejo de la información (confidencialidad, integridad, y uso exclusivo para actividades propias del Concejo de Bogotá) respetando los derechos de propiedad industrial, patrimonial y moral del autor.

- Todo funcionario del Concejo de Bogotá debe garantizar que la información que sea de su responsabilidad esté disponible siempre que se requiera.

- Todo funcionario del Concejo de Bogotá debe mantener actualizado el inventario de hardware y software que este bajo su responsabilidad.

- Todo funcionario del Concejo de Bogotá debe revisar que los parámetros de impresión (tamaño del papel, impresora asignada, etc.) sean los adecuados con el fin de no imprimir documentos innecesariamente.

- Todo funcionario del Concejo de Bogotá debe notificar a la Dirección Administrativa y Financiera a través del Proceso de Sistemas cuando:

    1. Requiera capacitación o tiene inquietudes sobre el correcto uso de los recursos y servicios autorizados.

    2. Sospecha que el equipo está infectado por un virus (en este caso no deberá utilizarlo hasta cuando sea revisado).

    3. Sea transferido o cambie su función, para actualizar sus datos y/o desactivar los servicios no requeridos.

    4. No va a hacer uso de los servicios por más de 30 días, cualquiera que sea el motivo (vacaciones, licencias, retiro, etc.) para que sea desactivado temporal o definitivamente.

5. No requiera alguno de los servicios autorizados.
6. Requiera instalar un nuevo hardware o software.
7. Requiera trasladar o dar de baja un equipo con el fin de mantener actualizado el inventario de hardware y software.
8. Al retirarse de la Empresa, deberá hacer entrega formal al responsable de la dependencia, de los recursos asignados incluyendo passwords, información, etc.

- Todo funcionario del Concejo de Bogotá, nunca deben abrir una sesión en un sistema de información y dejarla desatendida, ya que pueden ejecutarse acciones en esa sesión por otro usuarios.
- Todo funcionario del Concejo de Bogotá debe reportar los eventos no usuales que usted observe, ante Información y Recursos Físicos – Sistemas.
- Todo funcionario del Concejo de Bogotá debe Utilizar medidas que reduzcan el riesgo de pérdida, daño y fisgoneo de información.
- Todo funcionario del Concejo de Bogotá debe Proteger su equipo contra humedad, vandalismo, fuego, etcétera, asegurarse que NADIE coma, beba o fume junto al computador, Informarse dónde está el extintor más cercano, aprender a utilizarlo y verificar que es adecuado para atender incendios en equipo electrónico.
- Todo funcionario del Concejo de Bogotá de forma regular y programada, debe hacer copias de la información importante a su cargo y guardarla bajo llave fuera de su área de trabajo. Además, colocar etiquetas que identifiquen correctamente el contenido de los medios de almacenamiento (CDS, disquetes, cintas, etc.) registrando su nombre, o el de la persona que hizo las copias, y la fecha en que se realizó la copia.
- Todo usuario de la red del Concejo de Bogotá, tienen la obligación de cambiar su contraseña por seguridad y en el momento en que consideren que ha sido descubierta.
- El incumplimiento de estas normas de conducta por parte de los usuarios será sancionado mediante llamados de atención y las medidas disciplinarias necesarias para mantener la integridad del Concejo de Bogotá.

5.- POLITICAS DE SEGURIDAD FISICA Y AMBIENTAL

- Las instalaciones de procesamiento de información crítica o sensible para el Concejo de Bogotá deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con divisiones y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones por parte de terceros con o sin autorización.

- Los perímetros de seguridad deben estar claramente definidos.

- El área que contenga instalaciones de procesamiento de información debe ser físicamente sólido (por ej. no deben existir claros [o aberturas] en el perímetro o áreas donde pueda producirse fácilmente una irrupción).

- Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ej., mediante mecanismos de control, alarmas, cerraduras, etc.

- El acceso al Centro de Computo debe estar restringido exclusivamente al personal autorizado.

- Todas las puertas del perímetro de seguridad deben tener alarma y cerrarse automáticamente.

- Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso, asunto, nombre de quien autoriza su entrada, etc., deben ser ingresados en un registro de entrada de usuarios.

- Sólo se debe permitir el acceso a los visitantes que tengan propósitos específicos y autorizados.

- Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

- Se debe Verificar la existencia de 1 sola puerta de entrada y salida.

- Se deben implementar adecuados sistemas de detección de intrusos en el proceso de Sistemas, cuando no haya personal en las instalaciones. Los mismos deben ser instalados según estándares profesionales y probados periódicamente.

- Estos sistemas de detección de intrusos (SDI) comprenderán todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. También deben protegerse otras áreas, como las oficinas.

- Todos los equipos activos del Concejo de Bogotá, deben tener una identificación física basada en sus nombres, números de serie, características físicas y ubicación.

- No es permitido cambiar o modificar los registros e identificaciones físicas

- Todo equipo de computo (computadoras, estaciones de trabajo, portátiles, servidores, etc.), que este o sea conectado a la red o aquel que en forma autónoma se tenga y que sea propiedad de la Institución, debe sujetarse a las normas y procedimientos de instalación que emite el área de Información y Recursos Físicos - Sistemas.

- Los responsables de cada dependencia del Concejo deberán aplicar normas mínimas de seguridad física en las áreas en donde existan instalados microcomputadores, servidores, hardware de comunicaciones, documentación, etc. específicamente en cuanto a:

  1. Mecanismos para controlar el acceso sólo a personal autorizado, acordes con la sensibilidad del área.

  2. Mecanismos de extinción de fuego.

  3. Protección del cableado eléctrico y de la red.

  4. Conexiones eléctricas en buen estado.

  5. Conexión e identificación correcta de las tomas (Fase/Tierra/Neutro).

  6. La conexión a tierra deberá cumplir las especificaciones técnicas del fabricante de los equipos.

  7. Distribución correcta de cargas.

  8. Empalmes, paneles adecuados e identificados.

  9. Disposición de toma independiente para la conexión de otros aparatos eléctricos de alto consumo.

  10. Condiciones de temperatura y humedad adecuadas para los equipos.

11. Avisos preventivos que prohíban fumar, comer, beber, etc.

- El equipamiento debe ser ubicado en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.
- Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso.
- Los ítems que requieren protección especial deben ser aislados para reducir el nivel general de protección requerida.
- Se deben adoptar controles para minimizar el riesgo de amenazas potenciales, por ejemplo robo, incendio, explosivos, humo, agua (o falta de suministro, polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica, radiación electromagnética, etc.
- Se deben monitorear las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.
- Se debe tener en cuenta el uso de métodos de protección especial, como las membranas de teclado, para los equipos ubicados en ambientes industriales.
- Se debe considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización, por ej. un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle.
- Generar un registro de las aplicaciones, software, antivirus, sistemas operativos, actualizaciones, etc.; especificando sus características más relevantes como tipo, versión, tipo documentación, si necesita actualizaciones, etc.
- Se debe contar con un sistema automático de supresión de fuego en el cuarto donde se almacenen los servidores y especialmente donde se almacena las copias de respaldo y la documentación.
- Se debe contar con un sistema de Detección de fuego y humo.
- Se debe contar con un sistema de Aire acondicionado para asegurar un ambiente óptimo de trabajo para los equipos.

- Se debe asegurar el mantenimiento adecuado a los detectores de incendio, al sistema de alarma contra incendio, a las salidas de emergencia, a los paneles de distribución eléctricos y de potencia, a los suministros de potencia interrumpida, etc.

- El equipamiento del centro de cómputo debe estar protegido con respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas. Para ello debe contarse con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos.

- Para asegurar la continuidad del suministro de energía a los dispositivos del centro de computo hay que tener en cuenta los siguientes puntos:

1. Múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía.

2. Suministro de energía ininterrumpible (UPS)

3. Generador de respaldo.

- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño.

- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa (canaletas).

- El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.

- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.

- Se debe contar con la certificación de los puntos de la red para verificar su buen comportamiento.

- Esta prohibido mover o trasladar de sitio cualquier equipo activo, elemento de computo o red que se encuentren en el centro de computo, centros de cableado, el departamento de Información y Recursos Físicos – Sistemas y oficinas sin la correspondiente autorización.

- Esta prohibido resetear, apagar o desconectar los equipos activos, elementos de computo o red sin tener autorización para ello.

- Esta prohibido agregar o implementar nuevos equipos activos o elementos de computo o de red sin previo análisis y autorización administrativa.

- Esta prohibido en general, si no se cuenta con la debida autorización, cualquier clase de manipulación de los equipos activos, elementos de computo o red, por ser estos esenciales en el buen funcionamiento de la red de datos del Concejo de Bogotá.

- Todo equipo de computo (computadoras personales, estaciones de trabajo, servidores y demás periféricos), y los de redes de datos que sean propiedad del Concejo de Bogotá y que requiera ser actualizado para conservar o incrementar la calidad del servicio que presta, deberá realizarse por intermedio del área de Información y Recursos Físicos – Sistemas.

- La reubicación del equipo de cómputo será realizado únicamente por el personal autorizado del área de Información y Recursos Físicos – Sistemas.

- El área de Información y Recursos Físicos – Sistemas del Concejo de Bogotá notificara los cambios al equipo de inventarios (cambio de monitores, impresoras, etc.).

- El equipo de computo a reubicar, de propiedad del Concejo de Bogotá o bien externo se hará únicamente bajo la autorización del Área de Información y Recursos Físicos – Sistemas teniendo en cuenta que en el lugar a donde se hará la ubicación existan los medios necesarios para la instalación del equipo.

6.- POLITICAS GESTIÓN DE COMUNICACIONES Y OPERACIONES

- Se debe realizar un diseño e implementación de un plan para la gestión de la red.

- Se debe Implementar el uso de analizadores de tráfico y de red para monitorear es estado de la red por parte de los administradores de la red de datos del Concejo de Bogotá.

- Para el equipo de comunicación de datos, se debe verificar el tiempo medio de mantenimiento entre fallas (TMEF) dado por el proveedor con el fin de asegurarse de que el equipo de comunicación de datos tenga el tiempo medio entre fallas alto.

- Se debe contar con rutinas de software para recuperación y reinicio que recobren datos tales como los proporcionados por máquinas descompuestas, etc., para no tener que revisar el sistema entero de comunicación de datos, poder hacer una rápida recuperación y que solamente (tenga que retransmitirse) una sola transacción.

- Se debe hacer posible (si es factible) la implementación de un sistema de rastreo que asista en la localización de los problemas dentro del circuito de comunicación.

- La protección física y lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier novedad al área de Sistemas.

- Corresponde a Información y Recursos Físicos – Sistemas autorizar cualquier adquisición y actualización de software.

- Las actualizaciones de software de uso común o mas generalizado se llevaran a cabo de acuerdo al plan de actualización que se realice en el área de Información y Recursos Físicos – Sistemas.

- La Dirección Administrativa y Financiera a través del área de Información y Recursos Físicos – Sistemas. es el responsable de realizar revisiones periódicas para asegurar que solo programas con licencia estén instalados en las computadoras de la Institución.

- Corresponde al área de Sistemas, la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento especifico a que tenga lugar.

- Corresponde al área de Sistemas dar a conocer las listas de personas que deban tener acceso a los equipos y brindar los servicios de mantenimiento básico.

- Queda estrictamente prohibido dar mantenimiento a equipos de cómputo que no son de propiedad de la Institución.

7.- POLITICAS CONTROL DE ACCESOS

- Tendrá acceso a los sistemas de información solo el personal del Concejo de Bogotá, que es titular de una cuenta de usuario o tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.

- El acceso a la información se hará de forma controlada y restringida, por los perfiles de acceso a los usuarios, que asignan privilegios a cada uno de ellos y al manejo de la información y recursos de la red.

- El manejo de información administrativa que se consideré de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

- Tendrá acceso a los sistemas de información solo aquellos usuarios de red o externos autorizados por el área de Información y Recursos Físicos – Sistemas.

- Los servidores de bases de datos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal del área de Información y Recursos Físicos – Sistemas.

- El control de acceso a cada sistema de información será determinado por el área de Información y Recursos Físicos – Sistemas responsable de generar y procesar los datos involucrados.

- El control de acceso a cada sistema de información será determinado por la dependencia que sea responsable de generar y procesar los datos involucrados.

sean fácil de recordar y que no tengan que ver con datos personales del usuario al cual se le asignara la contraseña.

- Todos los PCs, laptops y estaciones de trabajo deben tener configurados un protector de pantalla con clave y con un tiempo de espera máximo de 10 minutos cuando el equipo esté desatendido.

- El acceso de personal se llevara a cabo de acuerdo al perfil que otorgue Sistemas a los miembros del área, y que se encuentren en concordancia con la política de la Institución y debido a la naturaleza de estas áreas se llevara un registro permanente del personal que ingrese y salga, sin excepción.

- Información y Recursos Físicos – Sistemas debe proveer la infraestructura de seguridad para el ingreso a esta área según las políticas de seguridad Física y Ambiental.

- Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio critico estará sujeto a las normas emitidas por el director Administrativo y Financiero del Concejo.

CONCEJO DE BOGOTÁ, D.C.

RESOLUCIÓN No. 866 DEL AÑO 2008

(17-Octubre-2008)

"POR LA CUAL SE ADOPTAN LAS POLÍTICAS DE SEGURIDAD EN SISTEMAS DE COMPUTO PARA EL CONCEJO DE BOGOTÁ D.C.."

- Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

- Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que el área de Información y Recursos Físicos – Sistemas emita.

- Dado el carácter unipersonal del acceso a la red, el área de Información y Recursos Físicos – Sistemas verificara el uso responsable del uso de la red.

- El acceso lógico a equipos especializados de computo (servidores, enrutadores, switch, bases de datos, servidores centralizados y distribuidos, etc.) conectado a la red es administrado por el área de Información y Recursos Físicos – Sistemas.

- Para el caso especial de los recursos de servidores a terceros deberán ser autorizados por Información y Recursos Físicos – Sistemas.

ARTÍCULO SEGUNDO: La presente Resolución rige a partir de la fecha de su expedición.

Comuníquese y Cúmplase.

Dada en Bogotá, D.C., el día 17 de octubre de 2008

HIPÓLITO MORENO GUTIÉRREZ
Presidente

GERMAN AUGUSTO GARCIA ZACIPA
Primer Vicepresidente

JAIME CAICEDO TURRIAGO
Segundo Vicepresidente

Proyecto: Ing. Carlos Muñoz / Hernando Rojas M.
Reviso y aprobó: Dra. Patricia Duque Cruz
Reviso: Hernando Rojas Martínez
Olga Marlene Rodriguez