Alcaldía Municipio
de Barrancabermeja

2335

RESOLUCIÓN No. ( )

POR MEDIO DE LA CUAL SE ESTABLECE EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN MUNICIPAL.

EL ALCADE MUNICIPAL DE BARRANCABERMEJA

En uso de sus facultades constitucionales y legales y en especial las consagradas en los artículos 209, 211 y 315 de la Constitución Política, la Ley 136 y la Ley 489de 1998 y,

CONSIDERANDO

Que el artículo 15 de la Constitución Política, establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Que la ley estatutaria 1266 de 2008 dicta las disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Que la ley 1273 de 2009 modifica el Código Penal, y crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- además de preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Que de conformidad con el artículo 3 del decreto número 1151 del 2008, la protección de la información del individuo es uno de los principios aplicables a la estrategia de gobierno en línea.

Que en los sistemas de información de la administración municipal se administra y almacena información personal de la ciudadanía, así como de los servidores públicos y contratistas que en ella laboran; información que debido a lo anteriormente mencionado debe poseer un nivel mínimo de seguridad.

Que las Políticas de Seguridad de la información brindan un nivel básico necesario para minimizar los riesgos que afecten de manera negativa la integridad, disponibilidad y confiabilidad de la información, teniendo en cuenta que el factor humano es el eslabón más débil en el ámbito la seguridad de la información.

Que se elaboró el documento de Políticas de Seguridad de la Información que fue realizado por un equipo interdisciplinario de la Administración Municipal el cual fue validado desde el punto de vista técnico y administrativo.

Que el objetivo principal de la implementación de las Políticas de Seguridad de la información es establecer una línea base de comportamiento de los servidores públicos y terceros con respecto al uso y manejo de la información.

En mérito de lo anteriormente expuesto,

R E S U E L V E:

ARTÍCULO PRIMERO: Se establece el cumplimiento obligatorio de las políticas de seguridad de la información de la administración municipal.

Alcaldía Municipio
de Barrancabermeja

2335

ARTÍCULO SEGUNDO: Adóptese el documento de Políticas de Seguridad de la Información por todo el personal de la Administración Municipal.

ARTÍCULO TERCERO: Los funcionarios de sistemas de la Alcaldía Municipal de Barrancabermeja, serán los encargados de realizar las capacitaciones adecuadas y necesarias acerca del cumplimiento de las políticas de seguridad de la información.

ARTICULO CUARTO: El profesional Especializado en Sistemas o quien haga sus veces, será el encargado de revisar a intervalos planificados o cuando se producen cambios significativos, la política de seguridad de la información, con el fin de garantizar que ésta sigue siendo adecuada, suficiente y eficaz.

ARTÍCULO QUINTO: La presente resolución rige a partir de la fecha de su expedición.

22 AGO 2012

ELKIN DAVID BUENO ALTAHONA
ALCALDE MUNICIPAL

VoBo. Dr. Gustavo Adolfo de la Ossa Sánchez – Jefe Oficina Asesora Jurídica.

Proyectó
JHON JAIRO JIMENEZ ALVAREZ
Profesional Especializado en Sistemas

POLÍTICAS DE SEGURIDAD
DE LA INFORMACIÓN

ALCALDIA MUNICIPAL
BARRANCABERMEJA

MAYO DE 2012

Políticas de Seguridad

CONTENIDO

Políticas de Seguridad

INTRODUCCION

La información es uno de los activos más importantes de una organización por lo que su integridad, confidencialidad y disponibilidad debe, de cierta manera, estar bajo un nivel de adecuado de seguridad aceptable, cumpliendo con códigos de buenas prácticas de seguridad de la información.

En el presente documento se establecerán las políticas de seguridad de la información que se deben cumplir para darle un manejo adecuado a su seguridad, permitiendo así su correcto tratamiento y respaldo.

1. SEGURIDAD FÍSICA Y PERIMETRAL

Objetivo.

Evitar el acceso físico no autorizado a las instalaciones de la Alcaldía de Barrancabermeja, al centro de cómputo de la oficina de sistemas y a la información de la organización.

1.1 Áreas Seguras.

- Todos los servidores y los sistemas de procesamiento de información de la Alcaldía Municipal, deberá contar con perímetros de seguridad física adecuados que impidan el acceso no autorizado al mismo.

- El acceso de visitantes a los centros de procesamiento de información deberán ser registrados, contando como mínimo con la fecha, hora y objeto de la visita, dicha visita deberá ser supervisada por un profesional del equipo de trabajo de la oficina de sistemas.

- Las condiciones ambientales del centro de computo de la Alcaldía Municipal, debe ser monitoreado y controlado para mantener un ambiente adecuado para el optimo rendimiento del mismo.

- El centro de cómputo es área restringida y solo el personal autorizado por la oficina de sistemas podrá tener acceso a él.

- Cuando en las distintas dependencias existan dispositivos de red como Switchs o Routers, esto se considerará como área segura y deberá contener algún tipo de seguridad perimetral. En caso de no existir, los empleados contratistas o terceros

deberán abstenerse de moverlo, reubicarlo o de conectarse directamente a él sin la autorización previa de la oficina de sistemas.

1.2 Protección de los equipos de cómputo.

- Cada equipo de computo incluyendo periféricos como scanner, impresoras y fotocopiadoras, deberán tener un responsable designado, al cual se le hará entrega formal del equipo por medio de un acta firmada por cada una de las partes, este documento deberá contener las características y el estado inicial del activo así como la asignación de las responsabilidades.

- La ubicación de los equipos de escritorio y periféricos como impresoras, fotocopiadoras y scanner deberá ser la que menor riesgo tenga con respecto a posibles amenazas ambientales o accesos no autorizados, así mismo, el empleado o contratista deberá respetar dicha ubicación.
  La oficina de sistemas en cabeza de su profesional especializado en sistemas deberá estudiar y evaluar la ubicación de cada equipo de cómputo con el fin de bridarle la mayor seguridad posible.

1.3 Salida e Ingreso de Equipos

- Cualquier persona que acceda a las instalaciones del palacio municipal deberá registrar al momento de su ingreso: equipos de cómputo, equipos de comunicaciones (excepto por teléfonos móviles o celulares) y herramientas que no sean propiedad de la alcaldía de manera que se mantenga control sobre el tráfico de los equipos de computo que entran y salen. Para funcionarios públicos y contratistas se podrá declarar con anterioridad los equipos de cómputo de su propiedad con el fin de agilizar el ingreso.

- Los equipos de computo y de comunicaciones o cualquier otro activo de información de propiedad de la Alcaldía, podrán salir de las instalaciones del palacio municipal previa autorización de la unidad administrativa respectiva.

2. COMUNICACIÓN Y OPERACIÓN

Objetivo.
Mantener un adecuado manejo de los procedimientos tecnológicos y de los servicios de procesamiento de información.

Políticas de Seguridad

2.1 Gestión de Activos.

- Todos los activos de información deberán estar correctamente identificados, por medio de una lámina o sticker, dicha identificación deberá ser única independientemente del tipo de activo que se esté etiquetando.
- Todo retiro o baja de activos de tipo software deberá ser autorizado por la oficina de sistemas y el activo de tipo hardware será autorizado por almacén municipal.

- Siempre que se dé de baja un medio de almacenamiento como discos duros, memorias USB, entre otros, se debe destruir totalmente haciéndolos irrecuperables, así mismo debe quedar constancia de ello.

- El procedimiento que se utilice para la eliminación del medio, deberá ser aquel que minimice el riesgo de fuga de información.

2.2 Gestión de Incidentes.

- En el caso que un usuario sospeche o tenga conocimiento pleno sobre un incidente que ponga en riesgo la integridad de un activo, deberá reportarlo de inmediato a la oficina de sistemas describiendo el suceso.

- Cualquier incidente relacionado con la utilización de equipos de computo y de comunicación deben reportarse a la oficina de sistemas.

2.3 Uso de Software.

- Cualquier instalación de software deberá ser realizado o, autorizado y aprobado por la oficina de sistemas.

- Si se requiere el uso de software propietario, se deberá justificar el uso del mismo y solicitar la autorización a la oficina de sistemas a través de un oficio firmado por el director de la unidad administrativa o secretaría, indicando en que equipo o equipos deberá instalarse el programa.

- La adquisición de nuevos sistemas de información, deberán cumplir a cabalidad con el protocolo de desarrollo de software de la oficina de sistemas.

- El nivel de acceso que deberán tener los usuarios a sus equipos asignados, serán los mínimos que le permitan ejecutar de manera correcta y suficiente sus actividades

diarias. En caso de que un usuario necesite privilegios de administrador en su sesión, ésta deberá ser aprobada y avalada por la oficina de sistemas.

2.4 Mantenimiento y Uso de Equipos.

- Solo el personal autorizado por el profesional especializado en sistemas realizará los mantenimientos y diagnósticos preventivos de los equipos de cómputo de la Alcaldía Municipal.
  Cuando este tipo de mantenimientos sea tercerizado, el profesional de sistemas deberá nombrar a algún profesional de su equipo de trabajo para realizar la respectiva supervisión técnica.

- Las configuraciones de los equipos de cómputo solo pueden ser modificadas por el personal autorizado por la oficina de sistemas.

- Todo archivo o información descargada desde la red o desde medios removibles como memorias USB, discos duros portátiles, discos compactos, entre otros, deberá ser revisado por el software antivirus antes de su utilización o apertura.

3. ACCESO LÓGICO

Objetivo.

Evitar el acceso no autorizado a los sistemas de información de la Alcaldía de Barrancabermeja.

3.1 Administración de Contraseñas.

- Los usuarios son responsables de la seguridad de sus contraseñas, tanto de su equipo como de los aplicativos a los cuales tiene acceso. Por ende, el usuario es responsable de todas las actividades realizadas con su nombre de usuario.

- Los usuarios deberán cambiar su contraseña periódicamente y estas no deberán contener información personal como nombres o números de teléfono, con el fin de que no se pueda inferir la contraseña con dicha información.

- Se debe evitar el almacenamiento de las contraseñas en papel o en registros digitales, a menos que estos tengan algún tipo de seguridad perimetral o de acceso.

- Cuando un usuario olvide, bloquee o extravíe su contraseña deberá solicitar a la oficina de sistemas que le realice la acción que le permita ingresar una nueva contraseña, y al momento de recibirla deberá cambiarla por una nueva

3.2 Acceso a los Sistemas de Información.

- El acceso a los sistemas de información críticos como el Software financiero, deberá ser accedido únicamente desde equipos seguros, evitando el acceso desde equipos públicos o salas de internet.

- Deberá evitarse el uso de la característica de los exploradores de "recordar usuario y contraseña", para evitar que personas no autorizadas accedan a los sistemas de información valiéndose de esto.

- Los accesos a sistemas de información WEB o aplicaciones WEB, deberán accederse digitando directamente la dirección en la barra de direcciones del explorador o siguiendo los enlaces del portal WEB de la Alcaldía. En todo caso deberá evitar el uso de buscadores, marcadores o accesos directos.

- Los privilegios establecidos a los usuarios en los sistemas de información deberán ser aprobados por el jefe de la unidad administrativa a la cual pertenecen.

3.3 Equipos desatendidos.

- Los usuarios deben finalizar las sesiones activas cuando finalice sus labores o dejar el equipo con en algún tipo de bloqueo cada vez que dejen el equipo desatendido.

4 RECURSO HUMANO

Objetivo.

Asegurar que los empleados y contratistas cumplan y entiendan las políticas de seguridad de la información y estén comprometidos con las responsabilidades que se les asignen.

4.1 Clausulas Contractuales.

- Todo empleado o contratista que sea asignado a la oficina de sistemas deberá firmar una clausula de confidencialidad o no divulgación de la información y de los controles de seguridad implantados en la Alcaldía Municipal.

- Dentro de las clausulas contractuales de todo empleado o contratista deberá existir un ítem que especifique la obligación de cumplir y someterse a las directrices de las políticas de seguridad de la Alcaldía Municipal.

- Todo desarrollo y producto ya sea tecnológico, industrial, documental, artístico, entre otros, que realice el personal de la alcaldía y contratistas como parte de sus labores contractuales, son propiedad de la Alcaldía Municipal, de igual manera esto quedará incluido dentro de los respectivos contratos.

4.2 Asignación de Activos y Accesos

- Los activos que se asignen a los empleados o contratistas, deberán ser devueltos en el momento que culmine la relación contractual o el contrato en cuestión. De igual manera, el equipo de cómputo asignado deberá ser para uso exclusivo de las funciones que le sean impartidas.

- Los accesos a sistemas de información, correo electrónico institucional y a áreas restringidas, deberán ser retirados o deshabilitados una vez culmine la relación contractual con el empleado o el contrato de prestación de servicios con el contratista. Así mismo, se deberá reasignar los privilegios o permisos a los empleados que sean reubicados o transferidos entre dependencias.

5 RESPALDO

Objetivo.

Resguardar la información almacenada en los equipos de cómputo utilizado por personal de la Alcaldía y Contratistas.

5.1 Respaldo de la Información.

- Cada usuario es responsable de la información producida y derivada de su trabajo y de sus funciones. El usuario deberá realizar una copia de seguridad periódicamente de la información que consideren relevante y cuando el equipo sea enviado a mantenimiento, previendo así la pérdida involuntaria de información derivada del proceso de mantenimiento.

- En caso de solicitar la ejecución de una copia de respaldo, el personal de sistemas solo estará obligado a rescatar la información pertinente a su labor más no a la información personal del usuario.

6 REDES Y TELECOMUNICACIONES

Objetivo.

Asegurar el correcto uso de la red de datos y de los servicios que se prestan por ese medio.

6.1 Uso del correo electrónico Institucional

- El correo electrónico institucional es personal e intransferible, cada usuario mantiene su propia cuenta y está prohibido el utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo.

- El usuario debe utilizar el correo electrónico exclusivamente para desempeñar las funciones que le fueron asignadas por su cargo, empleo o comisión; cualquier otro uso del correo electrónico está prohibido.

- Los usuarios deben tratar los mensajes de correo electrónico institucional y archivos adjuntos como información de propiedad de la Alcaldía de Barrancabermeja. Los mensajes de correo electrónico institucional deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- La Alcaldía de Barrancabermeja, se reserva el derecho a acceder y revelar todos los mensajes transmitidos por este medio para cualquier propósito, y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática o realizado acciones no autorizadas.

6.2 Acceso a redes públicas (Internet).

- Las páginas web de redes sociales así como otros de la misma índole, son inaccesibles desde la red cableada del palacio municipal; para conocer el listado completo de las páginas bloqueadas se deberá elevar la consulta a la oficina de sistemas.

- El acceso a Internet provisto para el personal del palacio municipal a través de la red es de uso exclusivo para el desarrollo de las actividades relacionadas con las necesidades del puesto y función que desempeña.

6.3 Acceso a la red de la alcaldía municipal.

- Los usuarios del servicio de la red del municipio, al aceptar el servicio están aceptando que:
  - Serán sujetos de monitoreo de las actividades que realizan en internet.
  - Saben que existe la prohibición al acceso de páginas no autorizadas.
  - Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
  - Saben que existe la prohibición de descargar software sin la autorización del Área de Sistemas.

6.4 Violaciones a la Seguridad

- El uso de equipos o herramientas para hallar vulnerabilidades o explotación de recursos sin la respectiva autorización de la oficina de sistemas, se considerará como ataque informático.

- Está prohibido realizar pruebas a los controles de los diferentes elementos de tecnologías de la información y las comunicaciones. Ninguna persona puede probar o intentar comprometer los controles internos.

7 CUMPLIMIENTO

Objetivo.

Asegurar el cumplimiento de normativas legales internas de la Alcaldía Municipal así como cualquier ley que aplique en las respectivas labores.

7.1 Propiedad Intelectual.

- Está prohibido por las normas de derechos de autor y por la Alcaldía de Barrancabermeja, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Alcaldía de Barrancabermeja.

- Los sistemas desarrollados por personal interno o contratistas son propiedad intelectual de la Alcaldía de Barrancabermeja, así mismo este apartado debe ser incluido como clausula dentro del contrato de prestación de servicios del contratista. (4.1)

7.2 Cumplimiento de las políticas

- Los directores de cada área administrativa, deberán revisar con regularidad en su área de responsabilidad el cumplimiento de las políticas de seguridad implementadas por la oficina de sistemas.

ELKIN DAVID BUENO ALTAHONA
Alcalde Municipal 2012 – 2015

JHON JAIRO JIMENEZ ALVAREZ
Profesional Especializado en Sistemas