SUPERINTENDENCIA DE SERVICIOS PUBLICOS DOMICILIARIOS
OFICINA JURIDICA
PREPARADO POR
REVISADO POR

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

LA SUPERINTENDENTE DE DE SERVICIOS PÚBLICOS DOMICILIARIOS (E)

En uso de las facultades legales, en especial las conferidas por el artículo 79, numeral 15 de la Ley 142 de 1994 y por el artículo 5°, numeral 63, y el artículo 7° numerales 1, 33 y 34 del Decreto 990 de 2002 y

CONSIDERANDO:

Que el numeral 15 del artículo 79 de la Ley 142 de 1994 y el numeral 63 del artículo 5 y el numeral 33 del artículo 7 del Decreto 990 de 2002, señalan que es función de esta Entidad y del Superintendente de Servicios Públicos Domiciliarios, organizar todos los servicios administrativos indispensables para el funcionamiento de la misma. Lo anterior en concordancia con lo dispuesto por los numerales 1 y 34 del artículo 7 del Decreto 990 de 2002 los cuales establecen que es función del Superintendente de Servicios Públicos Domiciliarios señalar las políticas generales de la Superintendencia y expedir los actos administrativos, reglamentos, manuales e instructivos que sean necesarios para el cabal funcionamiento de la Entidad.

Que el artículo 79, numeral 16 de la Ley 142 de 1994, en concordancia con el artículo 5° numeral 21 del Decreto 990 de 2002, dispone que es función de la Superintendencia de Servicios Públicos Domiciliarios señalar, de conformidad con la Constitución y la ley, los requisitos y condiciones para que los usuarios puedan solicitar y obtener información completa, precisa y oportuna, sobre todas las actividades y operaciones directas o indirectas que se realicen para la prestación de los servicios públicos, siempre y cuando no se trate de información calificada como secreta o de reserva por la ley".

Que el artículo 8° numeral 15 del Decreto 990 de 2002, dispone que es función de la Oficina de Informática de la Superintendencia de Servicios Públicos Domiciliarios definir y administrar las políticas de seguridad en aspectos informáticos, para lo cual podrá tomar las medidas conducentes a fin de evitar los usos indebidos, congestión y daños que amenacen la operatividad de la entidad.

Que en desarrollo de uno de los objetivos estratégicos SIGME de la Superintendencia, el cual es asegurar que la sociedad cuente con información oportuna y confiable, resulta necesario implementar políticas de seguridad de la información con el fin de dar cumplimiento a las necesidades y requerimientos de la entidad relacionados con la integridad y disponibilidad de la información, así como la confidencialidad de la misma cuando a ello haya lugar conforme la Constitución Política o la Ley.

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

Que las políticas de seguridad de la información precisan la identificación de responsabilidades y la determinación de objetivos para la protección apropiada y consistente de los activos de información y la infraestructura tecnológica de la Entidad.

Que la implementación de las políticas de seguridad de la información busca reducir los riesgos, bien sean accidentales o intencionales, relacionados con la divulgación, modificación, destrucción o uso indebido de los activos de información.

Que como resultado del uso de las políticas de seguridad de la información, se busca que las áreas responsables de la información al interior de la Superintendencia, orienten y mejoren la administración de seguridad de los activos de información y provean las bases para el monitoreo de la misma a través de toda la Entidad.

Que en mérito de lo expuesto,

R E S U E L V E

ARTICULO PRIMERO - ADOPCIÓN: Adóptense las políticas de seguridad de la información para la Superintendencia de Servicios Públicos Domiciliarios, contenido en el Anexo que hace parte integral de la presente resolución, a través del cual se imparten instrucciones para el uso, administración e implementación de las mismas a través de los recursos tecnológicos y humanos.

ARTÍCULO SEGUNDO - OBJETIVO: El objetivo de la política de seguridad de la información para la SUPERSERVICIOS consiste en velar por mantener la integridad, disponibilidad y la confidencialidad de la información que es recibida, procesada, generada o que reposa en la SUPERSERVICIOS.

ARTÍCULO TERCERO - ALCANCE Y APLICABILIDAD: La presente resolución es aplicable a todos los funcionarios que forman parte de la SUPERSERVICIOS, así como a todas aquellas personas, naturales o jurídicas, públicas o privadas que desarrollen contratos o convenios con la entidad y que tengan acceso y/o hagan uso de la infraestructura tecnológica de la SUPERSERVICIOS.

Las violaciones a las políticas establecidas en esta resolución comprometerán la responsabilidad del infractor y podrán generar acciones disciplinarias contra los servidores públicos involucrados, sin perjuicio de las acciones civiles y/o penales a que haya lugar. Éstas últimas también predicables con los particulares infractores que tengan acceso y/o hagan uso de la infraestructura tecnológica de la SUPERSERVICIOS.

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

ARTÍCULO CUARTO - RESPONSABILIDAD DE LOS JEFES DE DEPENDENCIA Y DE LOS SUPERVISORES DE CONTRATOS. Son responsabilidades de los jefes de dependencia que encabezan la estructura a la que se refiere el artículo 6 del Decreto 990 y de los supervisores de contratos, las siguientes:

Informar la presente resolución a los funcionarios, de la SUPERSERVICIOS y a todas aquellas personas, naturales o jurídicas, públicas o privadas que desarrollen contratos o convenios con la entidad y que en virtud de ellos tengan acceso y/o hagan uso de la infraestructura tecnológica de la SUPERSERVICIOS.

Solicitar la activación de las claves de acceso a los diferentes activos de información, definiendo los niveles de acceso permitidos, bien sea cuando se trate de un nuevo usuario; o cuando un usuario actual haya sido trasladado de dependencia al interior de la SUPERSERVICIOS; o cuando a un usuario actual le hayan sido modificadas sus funciones, actividades y/o obligaciones.

Solicitar de forma inmediata a la Oficina de Informática la inactivación de las claves de acceso a los diferentes activos de información, cuando un usuario ha sido desvinculado o ya no desarrolle contrato o convenio alguno con la SUPERSERVICIOS; cuando hayan sido suspendidas sus funciones y/o obligaciones; o cuando haya sido trasladado de dependencia al interior de la SUPERSERVICIOS.

Fomentar la participación activa de los funcionarios y personas naturales o jurídicas, públicas o privadas, que desarrollen contratos o convenios con la SUPERSERVICIOS, en los programas de concientización, sensibilización y capacitación de las políticas señaladas en la presente resolución.

ARTÍCULO QUINTO. VIGENCIA Y DEROGATORIA: La presente resolución rige a partir de la fecha de su publicación y deroga todas las disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

ÁNGELA PATRICIA ROJAS COMBARIZA

Proyectó: David Rodriguez, Victor Jaime
Revisó: Luis Alfredo Serrato Salázar – Jefe de la Oficina de Informática
Aprobó: Omar Urrea Romero - Secretario General (E)

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

ANEXO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUPERINTENDENCIA DE SERVICIOS PÚBLICOS DOMICILIARIOS

CAPÍTULO I

ARTÍCULO PRIMERO - OBJETIVO: Velar por mantener la integridad, confidencialidad y disponibilidad de la información que es recibida, procesada, generada o que reposa en la SUPERSERVICIOS.

ARTÍCULO SEGUNDO - ALCANCE Y APLICABILIDAD: La presente resolución es aplicable a todos los funcionarios que forman parte de la SUPERSERVICIOS, así como a todas aquellas personas, naturales o jurídicas, públicas o privadas que desarrollen contratos o convenios con la entidad y que tengan acceso a la información de la entidad y/o hagan uso de la infraestructura tecnológica de la SUPERSERVICIOS.

Las violaciones a las políticas establecidas en esta resolución comprometerán la responsabilidad del infractor y podrán generar acciones disciplinarias contra los servidores públicos involucrados, sin perjuicio de las acciones civiles y/o penales a que haya lugar. Éstas últimas también predicables contra los particulares infractores que tengan acceso a la información de la entidad y/o hagan uso de la infraestructura tecnológica de la SUPERSERVICIOS.

ARTÍCULO TERCERO - RESPONSABILIDAD DE LOS JEFES DE DEPENDENCIA Y DE LOS SUPERVISORES DE CONTRATOS. Son responsabilidades de los jefes de dependencia que encabezan la estructura a la que se refiere el artículo 6 del Decreto 990 2002 y de los supervisores de contratos, las siguientes:

Informar la presente resolución a los funcionarios de la SUPERSERVICIOS y a todas aquellas personas, naturales o jurídicas, públicas o privadas que desarrollen contratos o convenios con la entidad y que en virtud de ellos tengan acceso a la información y/o hagan uso de la infraestructura tecnológica de la SUPERSERVICIOS.

Solicitar la activación de las claves de acceso a los diferentes activos de información, definiendo los niveles de acceso permitidos, bien sea cuando se trate de un nuevo usuario; o cuando un usuario actual haya sido trasladado de dependencia al interior de la SUPERSERVICIOS; o cuando a un usuario actual le hayan sido modificadas sus funciones, actividades y/o obligaciones.

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

Solicitar de forma inmediata a la Oficina de Informática la inactivación de las claves de acceso a los diferentes activos de información, cuando un usuario ha sido desvinculado o ya no desarrolle contrato o convenio alguno con la SUPERSERVICIOS; cuando hayan sido suspendidas sus funciones y/o obligaciones; o cuando haya sido trasladado de dependencia al interior de la SUPERSERVICIOS.

Fomentar la participación activa de los funcionarios y personas naturales o jurídicas, públicas o privadas, que desarrollen contratos o convenios con la SUPERSERVICIOS, en los programas de concienciación, sensibilización y capacitación de las políticas señaladas en la presente resolución.

CAPITULO II

DEFINICIONES

ARTÍCULO CUARTO: Para efectos de la presente resolución, se adoptan las siguientes definiciones:

Activo de Información: Es un bien tangible o intangible, que es relevante para un sistema de información y que tiene asociado un valor referente al costo de sustitución, reputación, marca o prestigio.

Backup: Copia de seguridad o respaldo de información considerados lo suficientemente importantes para ser conservados.

Centro de cómputo: Lugar físico donde se concentra, procesa y almacenan los datos e información de una manera sistematizada y automática.

Confidencialidad: Requerimiento de seguridad de la información. Hace referencia a que únicamente usuarios autorizados pueden tener acceso a la información.

Contraseña segura: Aquella constituida por letras mayúsculas, letras minúsculas, números y cuya longitud debe ser mínimo de ocho (8) caracteres.

Control de acceso: Requerimiento de Seguridad de la Información. Hace referencia a denegar o conceder ciertos permisos a los usuarios que manipulan la información.

Corrreo electrónico institucional: Aquella cuenta de correo electrónico creada por la SUPERSERVICIOS para fines laborales. Esta cuenta se caracteriza por terminar en @superservicios.gov.co.

Descompilar: Traducir información o lenguaje de máquina a un lenguaje comprendido por el ser humano.

Desarrollo: Actividad consistente en trasladar las especificaciones de los requerimientos de software a un lenguaje de programación.

Disponibilidad: Requerimiento de Seguridad de la Información. Velar que los usuarios tengan acceso a la información y a sus activos asociados cuando lo requieran; lo anterior sin perjuicio de las políticas de protección que la SUPERSERVICIOS brinde a la información confidencial.

Dispositivo activo de red: Equipo electrónico autónomo que maneja la lógica de interconexión de redes LAN y/o WAN, enviando los datos al destinatario definido a través de un circuito virtual creado entre el origen y el destino.

Documento: Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares. Pueden ser públicos o privados.[1]

Documento Público: No se limitan a aquellos que son producidos por órganos públicos, sino que se extiende a aquellos documentos que reposan en las entidades públicas, los producidos por las entidades públicas y documentos privados que por ley, declaración formal de sus titulares o conducta concluyente, se entienden públicos.[2] Cobija: expedientes, informes, estudios, cuentas, estadísticas, directivas, instrucciones, circulares, notas y respuestas provenientes de entidades públicas acerca de la interpretación del derecho o descripción de procedimientos administrativos, pareceres u opiniones, previsiones y decisiones que revistan forma escrita, registros sonoros o visuales, bancos de datos no personales, etc.[3]

Hardware: Cualquier componente físico tecnológico. Artefactos físicos de una tecnología.

Infraestructura Tecnológica: Conjunto de hardware, software y servicios informáticos de la entidad.

Ingeniería Inversa: Proceso mediante el cual se busca obtener información a partir de un producto con el fin de comprender como está hecho y que lo hace funcionar.

---

[1] Artículo 251 del Código de Procedimiento Civil

[2] Corte Constitucional, sentencia T - 216 de 2004

[3] Corte Constitucional, sentencia T - 473 de 1992, artículo 74 de la Constitución Política.

Información Sensible: Aquella que debe ser especialmente protegida, pues su pérdida, divulgación, destrucción o alteración puede afectar la misión de la entidad.

Insumos: Todo bien consumible utilizado en el proceso productivo de otro bien.

Integridad: Requerimiento de Seguridad de la Información. Hace referencia a que la información permanezca completa e inalterada durante el proceso de generación, transmisión o recepción, salvo que por razones inherentes al proceso de comunicación, archivo o presentación se adicione algún cambio.

Material no autorizado: Material protegido por derechos de autor, marca comercial u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio, con contenido explícito sexual, pornografía infantil o con contenido ilegal de acuerdo a las normas vigentes.

Material multimedia: Que utiliza conjunta y simultáneamente diversos medios, como imágenes, sonidos, video y texto, en la transmisión de una información[4].

Plan de Contingencia: Son los procedimientos alternativos a la operación normal que permiten a la entidad seguir operando ante la eventualidad de una falla parcial o total. El objetivo es recuperarse ante un incidente interno o externo en el menor tiempo posible.

Red LAN: Una LAN (Red de área local) es un grupo de equipos (computadoras, impresoras y otros dispositivos) que pertenecen a la misma organización y están conectados dentro de la misma área geográfica.

Red WAN: Una **WAN** (Red de área extensa) conecta entre sí varias LAN atravesando importantes distancias geográficas, del orden del tamaño de un país o de un continente.

Servicio Informático: Medio informático para agregar valor al cliente proporcionándole el resultado que éste espera. El valor del servicio desde la perspectiva del cliente se traduce en utilidad (funcionalidad ofrecida por un producto o servicio – lo que hace) y garantía (como lo hace).

Software: Es todo conjunto intangible de datos y programas implementados para un sistema informático.

Software malicioso: Software que tiene como objetivo infiltrarse, dañar o controlar el sistema de un computador sin el consentimiento de su propietario.

[4] RAE. DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición. Disponible en www.rae.es. Consultado el 13 de enero de 2011.

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

Software P2P: Software que permite el intercambio directo de información, en cualquier formato, entre los equipos de cómputo interconectados (tales como Ares, Emule, Torrents, Kazaa y similares).

Trazabilidad: Requerimiento de Seguridad de la Información. Hace referencia a poder determinar quién, cuando, cómo y desde donde se realizan las operaciones sobre los datos.

Usuario: Hace referencia a todos los funcionarios de la SUPERSERVICIOS y personas naturales o jurídicas, públicas o privadas que desarrollen contratos o convenios con la entidad, y que tengan acceso y/o hagan uso de la infraestructura tecnológica de la entidad.

CAPÍTULO III

CONDICIONES DE USO DE LA INFRAESTRUCTURA TECNOLÓGICA

ARTÍCULO QUINTO – CONDICIONES DE USO: Al tener acceso a la infraestructura tecnológica de la SUPERSERVICIOS, los usuarios deben tener en cuenta las siguientes condiciones:

5.1 Uso de los recursos: La Infraestructura Tecnológica no será utilizada para actividades comerciales o para propósitos de entretenimiento, diversión o acceso/uso a material no autorizado. Los recursos son exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y/o obligaciones acordadas o contratadas. Es decisión del órgano directivo de la SUPERSERVICIOS no admitir alguna clase de entretenimiento, incluyendo aquellos preinstalados en los equipos de cómputo.

5.2 Derechos de acceso: La SUPERSERVICIOS podrá:

(a) Utilizar herramientas tecnológicas o procedimientos manuales para monitorear el uso de su Infraestructura Tecnológica y aquel material almacenado, publicado, enviado, recibido o creado a través de estos recursos.

(b) Otorgar o denegar el acceso a los recursos de la Infraestructura Tecnológica a los usuarios que soliciten acceso de acuerdo a las restricciones definidas para los mismos.

(c) Acceder a la información con autorización y/o en presencia del usuario. En caso que el usuario no autorice el acceso a la información, se debe contar con la autorización del Jefe de Dependencia e informarlo al Jefe de la Oficina de Informática. Por otro lado, cuando el usuario custodio de la información se encuentre en alguna de las siguientes situaciones: enfermedad,

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

licencia, vacaciones, permisos, fallecimiento, terminación de la relación contractual, desvinculación laboral o imposibilidad de contacto, la SUPERSERVICIOS podrá acceder a esta información con la autorización del Jefe de Dependencia, quien previamente deberá solicitarla al Jefe de la Oficina de Informática. Sin embargo, la SUPERSERVICIOS tiene en cuenta las siguientes excepciones para acceder a la información:

i) No accederá a información que por ley constituye reserva. Sin embargo, la determinación de mantener en reserva o en secreto un documento público opera sobre su contenido más no sobre su existencia.

ii) No accederá a información que pueda desconocer derechos fundamentales, salvo que la persona involucrada y el jefe de la respectiva dependencia o su delegatario para tal efecto autorice su consulta.

iii) No accederá a información que pueda desconocer bienes constitucionalmente valiosos (derechos de terceros, la eficacia de las investigaciones estatales y los secretos comerciales e industriales).

iv) No accederá a información personal, sin perjuicio de las medidas a tomar por uso indebido de los servicios ofrecidos por la entidad.

d) La autorización de acceso a la información debe ser motivada por una o mas de las siguientes situaciones, teniendo en cuenta las excepciones enunciadas en el ítem (c) numeral 5.2

i) Por la Oficina de Informática en función del artículo 8 numeral 15 del Decreto 990 de 2002, que establece: "Definir y Administrar las políticas de seguridad en aspectos informáticos, para lo cuál podrá tomar las medidas conducentes a fin de evitar los usos indebidos, congestión y daños que amenacen la operatividad de la Entidad".

ii) Por necesidad de acceso a la información para el funcionamiento de la entidad.

iii) Por requerimiento expreso de una autoridad competente.

5.3 Uso no permitido: Los recursos asignados para el desempeño laboral, o para el desarrollo de funciones, actividades y/o obligaciones acordadas o contratadas, no deben ser utilizados para el almacenamiento de información personal, material no autorizado, material multimedia o de cualquier otro tipo que no sea necesario para el desarrollo normal de las labores.

5.4 Mal uso del recurso tecnológico: Los usuarios deben abstenerse de realizar acciones que impliquen un desperdicio de los recursos de la Infraestructura Tecnológica y/o insumos suministrados por la entidad, que conlleven a la monopolización, obstaculización, acaparamiento o uso personal de los recursos o que impliquen un riesgo para las políticas de seguridad de la SUPERSERVICIOS.

5.5 Uso inadecuado del software: Los usuarios deben abstenerse de efectuar cualquiera de las siguientes actividades:

(a) Copiar software licenciado o adquirido por la SUPERSERVICIOS, para uso personal o beneficio de terceros.

(b) Copiar las claves de los productos adquiridos por la SUPERSERVICIOS y utilizarlas para uso personal o beneficio de terceros.

(c) Instalar software adicional a los autorizados por la SUPERSERVICIOS en los servidores y equipos de cómputo de la entidad, con excepción de los utilizados para el desempeño laboral, función o actividades contratadas. En todo caso, el software instalado debe contar con la licencia respectiva.

(d) Introducir software malicioso en la Infraestructura Tecnológica de la SUPERSERVICIOS.

(e) Modificar, revisar, transformar, adaptar o copiar cualquier software de la SUPERSERVICIOS sin previa autorización, a menos que la licencia lo permita.

(f) Descompilar o realizar actividades de Ingeniería Inversa del software, sobre bases de datos u otros sistemas de información de la SUPERSERVICIOS a menos que sea un requerimiento expreso de sus funciones o de su labor contratada.

(g) Utilizar software y/o hardware que permita capturar el tráfico de datos generado al interior de la SUPERSERVICIOS a través de la Infraestructura Tecnológica. Si es requerido, se debe contar con la autorización expresa y por escrito del Jefe de la Oficina de Informática y ser parte de la función o labor contratada.

(h) Utilizar software, hardware o cualquier tipo de tecnología para capturar o interceptar tráfico de voz en su origen, destino o al interior de la SUPERSERVICIOS sin que medie autorización o solicitud escrita de autoridad competente.

(i) La SUPERSERVICIOS podrá grabar conversaciones de voz, con el fin de verificar la calidad del servicio prestado por los funcionarios o terceros particulares que tengan actividades o funciones contratadas por la entidad. Para tales efectos, así lo anunciará antes de darse inicio a la comunicación respectiva.

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

(j) Copiar o vender cualquier tipo de información sensible de la SUPERSERVICIOS sin la autorización respectiva.

5.6 Uso inadecuado del suministro eléctrico: Los usuarios deben abstenerse de conectar a las fuentes reguladas de suministro eléctrico (que en la SUPERSERVICIOS están identificadas con color naranja), dispositivos adicionales a los autorizados por la SUPERSERVICIOS.

CAPITULO IV

POLÍTICAS DE USO Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA

ARTÍCULO SEXTO – USO DE LA INFRAESTRUCTURA TECNOLÓGICA: La infraestructura tecnológica de la entidad que esté al servicio de los usuarios de la SUPERSERVICIOS debe ser utilizada teniendo en cuenta los siguientes criterios:

(a) Los usuarios deben abstenerse de dejar abierta la sesión de trabajo de los equipos de cómputo al dejar el puesto de trabajo. Deben asegurarse de bloquear la sesión, pues es responsabilidad de cada usuario las actividades que se generen con la cuenta asignada.

(b) Los usuarios deben apagar sus equipos de cómputo al culminar su jornada. Solo se podrán dejar activos aquellos equipos que cuenten con la autorización expresa y escrita del Jefe de la Oficina de Informática.

(c) No se permite la manipulación interna de hardware en los equipos de cómputo por personas ajenas a las autorizadas por la SUPERSERVICIOS.

(d) El personal encargado de la gestión, operación y administración de la Infraestructura Tecnológica debidamente autorizado por la SUPERSERVICIOS, podrá realizar en cualquier momento una inspección del software instalado en los equipos de cómputo.

(e) Los usuarios no utilizarán en ningún caso las herramientas suministradas, para cometer actos ilícitos.

(f) Los usuarios son responsables por los elementos de la Infraestructura Tecnológica asignada para sus funciones o para el desarrollo de la labor contratada o convenida.

ARTÍCULO SÉPTIMO – ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS. USO DE CONTRASEÑAS:

I. La administración de usuarios y contraseñas es responsabilidad del administrador asignado de cada sistema o aplicativo, para lo cual tendrá en cuenta los siguientes parámetros:

(a) Establecer un estándar para identificar de forma única a los usuarios.

(b) Definir la periodicidad de caducidad de las contraseñas, siempre y cuando el sistema o aplicativo lo permita.

(c) Mantener un registro actualizado de los usuarios, perfiles y permisos asignados, relacionando los recursos de la Infraestructura Tecnológica a los que tienen acceso.

(d) Definir y utilizar los mecanismos de contraseñas seguras para aquellos aplicativos y sistemas que así lo permitan.

II. Los usuarios deben seguir los siguientes lineamientos para el uso de las contraseñas:

(e) La contraseña es de carácter personal e intransferible. Por lo tanto, se presume que todas las acciones realizadas bajo la cuenta de usuario asociada, fueron ejecutadas por el usuario responsable de la cuenta.

(f) Es responsabilidad de cada usuario la salvaguarda de las contraseñas que le fueron entregadas o establecidas por el mismo.

(g) En el caso que la aplicación o sistema no permita el uso de contraseñas seguras, el usuario debe definir una contraseña teniendo en cuenta la definición de contraseña segura establecida en el artículo cuarto de la presente resolución.

(h) En el caso que la aplicación o sistema no obligue al cambio periódico de la contraseña, el usuario debe cambiarla periódicamente.

(i) Las contraseñas que utiliza el administrador de cada sistema, aplicativo o dispositivo de la Infraestructura Tecnológica de la entidad que lo requiera, debe ser proporcionada al jefe de dependencia responsable en sobres sellados y cada vez que las contraseñas sean cambiadas, incluyendo aquellas contraseñas que permiten acceso sin restricciones. En caso dado que esta función este siendo administrada por un tercero, se deberán entregar las contraseñas al jefe de dependencia responsable en sobres sellados y cada vez que las contraseñas sean cambiadas.

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

ARTÍCULO OCTAVO – RESPALDO DE INFORMACIÓN (BACKUP): La Oficina de Informática o quién esté a cargo de la gestión, operación y administración de la Infraestructura Tecnológica, es el responsable de la generación de copias de seguridad de la información de la SUPERSERVICIOS. En esta actividad se deben tener en cuenta las siguientes reglas:

(a) El personal encargado de la gestión, operación y administración de la Infraestructura Tecnológica, en conjunto con el usuario que solicite el backup de datos y/o archivos, deben definir qué información debe ser respaldada y la periodicidad para realizar las copias de seguridad, de acuerdo a los recursos de almacenamiento disponibles. El contenido del backup debe ajustarse a lo estipulado en el numeral 5.3 de la presente resolución.

(b) La realización de los backups de los servidores de la entidad es responsabilidad de la Oficina de Informática o quién este a cargo de la gestión y operación de la Infraestructura Tecnológica. Este procedimiento debe estar documentado. Así mismo, la Oficina de Informática o quién esté a cargo de la gestión y operación de la Infraestructura Tecnológica, debe elaborar el Plan de Backups de acuerdo a las necesidades expresadas por las áreas clientes o dueñas de la información.

(c) Las copias de seguridad deben permitir identificar claramente la información que contienen, el usuario solicitante, las fechas de generación del mismo, el tiempo de almacenamiento requerido, el método de generación y el método de recuperación.

ARTÍCULO NOVENO – USO DEL CORREO ELECTRÓNICO INSTITUCIONAL :

El correo electrónico institucional es un servicio de la entidad y por tal, su uso debe estar relacionado únicamente con temas laborales. El poseer información personal en las cuentas de correo electrónico institucional significa un uso indebido del servicio. En este sentido, cuando se realizan revisiones al correo electrónico institucional, no se está desconociendo el derecho a la intimidad, como lo sería la revisión de los correos electrónicos personales, ni se configura ninguna violación relacionada, teniendo en cuenta que siendo la SUPERSERVICIOS una Entidad Pública a la luz del artículo 14 de la Ley 57 de 1985, toda la información que en ella repose es pública, salvo las excepciones legales y constitucionales que se contemplen. La SUPERSERVICIOS respetará la privacidad de la información que es almacenada, publicada, enviada, recibida o creada con recursos tecnológicos de la entidad, teniendo en cuenta lo enunciado en los ítems (c) y (d) numeral 5.2.

i. Los usuarios deben hacer uso responsable de la cuenta de correo electrónico institucional, para esto deben tener en cuenta los siguientes aspectos:

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

(a) Es responsabilidad de cada usuario realizar constantemente la depuración del correo electrónico institucional mediante la opción *eliminar correo* o bajando a disco la información, para lo cual el usuario podrá solicitar la asistencia del administrador de la plataforma de correo electrónico, con el fin de no exceder la cuota de almacenamiento asignada.

(b) El correo electrónico institucional debe ser usado únicamente para aspectos relacionados con temas de la entidad, de ninguna manera debe ser utilizado para fines personales, entretenimiento, diversión, ofensa, intimidación, acoso, agresión, cadenas de envío masivo no relacionadas con temas de la entidad, tendencias políticas y discriminación racial o para el envío o recepción de material no autorizado.

(c) El envío de correos electrónicos masivos a través del correo electrónico institucional está permitido solo para los usuarios autorizados y su contenido debe ser con fines institucionales. Esta autorización está a cargo del Director Administrativo de la SUPERSERVICIOS o de la persona que ejerza sus funciones.

(d) Todo correo electrónico que sea enviado desde el correo institucional debe llevar un pie de página cuyo contenido trate acerca de la exclusividad de la información enviada, de la integridad y confidencialidad del mismo. Este mensaje debe ser generado automáticamente y debe visualizarse al final del correo.

ii. La administración de las cuentas de correo electrónico institucional de la SUPERSERVICIOS debe seguir los siguientes lineamientos:

(a) El correo electrónico institucional es asignado a los funcionarios y contratistas de la SUPERSERVICIOS en el momento de iniciar funciones o labores contractuales con la entidad, según lo estipulado para la gestión y administración de usuarios de servicios tecnológicos del proceso Gestión y Operación de la Infraestructura Tecnológica.

(b) Los estados en los que se puede encontrar una cuenta de correo institucional son:

Activa: Aquella cuenta operativa, asignada a un usuario, con la contraseña entregada a éste para su uso y bajo su responsabilidad.

Eliminada: Aquella cuenta que no es operativa y que deja de estar asignada a un usuario, ya sea por su desvinculación de la entidad, por solicitud expresa del responsable de la cuenta o del Jefe de Dependencia del usuario. La información de la cuenta, incluyendo documentos compartidos debe ser respaldada (realización de backup).

Suspendida: Aquella cuenta que no es operativa y aunque no es accesible por el usuario continúa asignado a éste. La información asociada a la cuenta no debe ser eliminada.

(c) La SUPERSERVICIOS podrá crear y asignar cuentas de correo electrónico institucional a las aplicaciones de la entidad cuando esto sea un requerimiento para el funcionamiento de la aplicación. Así mismo, se podrán asignar cuentas de correo electrónico institucional a dependencias, cargos y otras que sean requeridas para funciones especiales.

(d) Las cuentas de correo electrónico institucional deben ser eliminadas cuando un funcionario o contratista ya no tenga vínculo laboral o contractual con la entidad, de acuerdo a lo estipulado para la gestión y administración de usuarios de servicios tecnológicos del proceso Gestión y Operación de la Infraestructura Tecnológica.

(e) Las cuentas de correo electrónico deben ser suspendidas cuando el usuario que la tenga asignada suspenda temporalmente su vinculo laboral o contractual por más de un mes calendario. No obstante, las cuentas de correo electrónico asignadas a funcionarios o contratistas que no presenten ingreso durante más de dos meses calendario continuos deberán ser suspendidas por el administrador del correo sin necesidad de solicitud expresa. Después de tres meses calendario continuos sin reportar ingreso, una cuenta de correo electrónico institucional asignada a un funcionario o contratista deberá ser eliminada por el administrador del correo electrónico, no sin antes respaldar la información de la misma y los documentos asociados sin necesidad de solicitud expresa.

ARTÍCULO DÉCIMO – ADMINISTRACIÓN DEL INVENTARIO DE LA INFRAESTRUCTURA TECNOLÓGICA:

(a) El grupo de Almacén e Inventarios de la SUPERSERVICIOS, en cumplimiento de sus funciones, ejerce el control sobre la asignación, redistribución y disposición de los equipos de cómputo y consumibles adquiridos por la Superintendencia de Servicios Públicos Domiciliarios.

(b) Ni el grupo de Almacén e Inventarios, ni la Oficina de Informática de la Superintendencia de Servicios Públicos Domiciliarios se hacen responsables de la información que contenga el equipo de cómputo. De ser necesario realizar una copia de seguridad de la información, el funcionario debe realizar la gestión por medio del personal encargado de la gestión, operación y administración de la Infraestructura Tecnológica.

(c) El personal encargado de la administración de la Infraestructura Tecnológica de la SUPERSERVICIOS mantendrá actualizadas las hojas de vida de la Infraestructura Tecnológica.

(d) Al término de vinculación con un usuario determinado, el jefe de la dependencia o el supervisor del contrato respectivo, deberá determinar si se requiere realizar la entrega en medio magnético de la información relevante del equipo de cómputo asignado, para lo cual, debe solicitar la colaboración del administrador de la Infraestructura Tecnológica.

(e) A los equipos de cómputo (servidor o estación de trabajo) de la SUPERSERVICIOS, antes de ser reasignados o dados de baja, se les debe realizar un procedimiento para eliminar cualquier dato existente. Lo anterior, aplica a cualquier medio de almacenamiento (memorias USB, discos duros) nuevo, reasignado o dado de baja.

ARTÍCULO DÉCIMO PRIMERO – USO GENERAL DE LOS SERVICIOS DE RED:

(a) El administrador de Centro de Computo y/o las personas autorizadas realizarán periódicamente monitoreo de los diferentes servidores y servicios e informarán los resultados al Jefe de la Oficina de Informática. Los usuarios que necesiten utilizar herramientas para el monitoreo deben justificar ante el Jefe de la Oficina de Informática la razón de tal necesidad.

(b) El administrador de Centro de Computo y/o las personas autorizadas para el monitoreo o captura de tráfico por la red de datos, deben hacer uso de esta información únicamente con fines de detección de anomalías o problemas en la Red LAN o WAN.

(c) El acceso a los recursos de red de voz y datos es exclusivo de los usuarios de la SUPERSERVICIOS, el uso para terceras personas debe ser autorizado expresamente por los jefes de área a que se refiere el artículo 6 del Decreto 990 de 2002.

(d) El acceso remoto a los servidores, equipos de cómputo o recursos de red debe realizarse a través de canales de comunicación seguros. El Jefe de la Oficina de Informática debe autorizar el acceso remoto al usuario solicitante.

(e) Los usuarios deben abstenerse de conectar dispositivos activos de red o cualquier otro hardware a la red de datos o voz sin la autorización del Jefe de la Oficina Informática o el tercero encargado de administrar de la red LAN o WAN.

(f) Los usuarios no deben destruir, manipular, monitorear o capturar la información que circula por la red de datos o voz. El monitoreo o captura está supeditado a la estipulado en los literales (a) y (b). La grabación de conversaciones de voz está supeditado a lo estipulado en el numeral 5.5 literal (i).

(g) La Oficina de Informática podrá utilizar herramientas tecnológicas (Hardware o Software) para controlar, detectar, prevenir o monitorear el uso de los recursos de la red de datos y voz.

ARTÍCULO DÉCIMO SEGUNDO – USO GENERAL DE INTERNET E INTRANET:

(a) El administrador del Centro de Cómputo o el tercero autorizado de acuerdo a las directrices para el uso general de Internet descrito en este artículo, podrá controlar o limitar el acceso a páginas web, servicios de carga y descarga de cualquier tipo de información, acceso a material multimedia en línea y material no autorizado, cuando su uso no esté sustentado en la necesidad del desempeño laboral, función o actividad contratada. Las excepciones deben ser justificadas por el Jefe de Dependencia o ser ordenadas por la(el) Superintendente, la(el) Secretaria(o) General, o el(la) Director(a) Administrativo(a).

(b) Los usuarios de la SUPERSERVICIOS deben abstenerse de utilizar los servicios de internet para fines de entretenimiento, ocio o acceso a material no autorizado, para lo cual la Oficina de Informática o el administrador del Centro de Cómputo dispondrá de una herramienta informática que permita realizar este control de manera automática. Las excepciones deberán ser justificadas por el Jefe de Dependencia o del Supervisor del usuario respectivo.

(c) El administrador de Centro de Cómputo utilizará herramientas para el control y monitoreo del uso de los recursos de Internet. La información recolectada será utilizada para generar informes semanales debe contener como mínimo: las direcciones IPs de los usuarios que accedieron a material no autorizado, páginas más visitadas de alto consumo del canal de Internet, las direcciones IPs de los 10 usuarios que más acceden a material multimedia en línea, las 10 páginas más visitadas. Los resultados de los informes deben ser entregados al Jefe de la Oficina Informática o a quien este delegue. Los usuarios que necesiten utilizar herramientas para el control o monitoreo deben justificar el por qué y tener la respectiva autorización escrita del Jefe de la Oficina de Informática para poder realizar dicha labor.

(d) Se prohíbe el acceso, carga, descarga, copia, reproducción, almacenamiento o circulación de cualquier tipo de material relacionado con pornografía infantil. Si este comportamiento es observado o detectado, debe ser informado inmediatamente a las autoridades correspondientes y al jefe de área inmediato.

(e) Los usuarios de la SUPERSERVICIOS deben abstenerse del uso de programas de intercambio de material multimedia o material no autorizado utilizando software P2P (tales como Ares, Emule, Torrents, Kazaa y similares) y haciendo uso de los servicios de la red de Internet de la entidad. Asi mismo, servidores de carga/descarga masiva de archivos (tales como Megaupload, Rapidshare y similares).

CAPITULO V

SEGURIDAD FÍSICA Y LÓGICA

ARTÍCULO DÉCIMO TERCERO – SEGURIDAD FÍSICA: Por medio de las siguientes políticas de seguridad se establecen buenas prácticas en la forma de actuar por parte de los usuarios de la SUPERSERVICIOS, en relación con la infraestructura tecnológica y los sistemas de información de la entidad.

i. Protección del hardware:

(a) Los equipos de cómputo de la SUPERSERVICIOS son de uso exclusivo de los funcionarios y de los terceros particulares que desarrollen actividades o funciones contratadas con la entidad de la entidad, bajo ningún motivo deben ser manipulados por personas no autorizadas.

(b) Los usuarios de la SUPERSERVICIOS deben portar el carné que los acredita como tales, en un lugar visible, con el fin de llevar un control y un mejor manejo de la identificación de las personas que ingresan a las instalaciones. En caso en que el funcionario o el tercero particular que desarrolle actividades o funciones contratadas con la entidad no porte el carné, deberá proceder según circular interna 20085000000124 del 03-09-2008, 20095000000024 del 23-01-2009 y 20105000000164 del 05-10-2010 o las que la modifiquen, sustituyan o adicionen.

(c) Solo las personas autorizadas por la Oficina de Informática podrán revisar, instalar, configurar y dar soporte a los equipos de cómputo de la SUPERSERVICIOS.

(d) El área encargada de realizar el traslado de equipos de computo, deberá informar de dichos movimientos al encargado de la gestión, operación y administración de la Infraestructura Tecnológica de la Entidad. Se exceptúa el traslado de equipos de cómputo portátiles, video beams y similares por parte de funcionarios o terceros particulares que desarrollen actividades o funciones contratadas con la entidad de la SUPERSERVICIOS.

ii. Protección de Datos:

(a) Todo usuario de la infraestructura tecnológica de la SUPERSERVICIOS es responsable por la integridad, confidencialidad y disponibilidad de la información que manejen.

(b) Todo usuario de la infraestructura tecnológica de la SUPERSERVICIOS debe ser consciente de la información sensible que maneja. De esta manera toda impresión de documentos que contenga información sensible y/o que con tenga firmas en ellos, no podrá manejarse como papel reciclable. Esta información debe ser destruida cuando ya no sea necesaria para el desempeño de sus funciones o labor contratada o convenida.

(c) Los usuarios de la infraestructura tecnológica de la SUPERSERVICIOS no deben dejar expuestos en su lugar de trabajo documentos o material sensible, cuya divulgación o pérdida pueda afectar los intereses de la SUPERSERVICIOS.

(d) Los usuarios de la infraestructura tecnológica de la SUPERSERVICIOS no deben hacer uso indebido de la información sensible a la que tengan acceso. Dicha información es para uso exclusivo en el cumplimiento de las funciones u obligaciones asignadas.

(e) Antes de eliminar una cuenta de correo electrónico institucional , se debe respaldar la información asociada a la cuenta, incluyendo los documentos compartidos.

iii. Copias de seguridad:

(a) La Oficina de Informática o el administrador de la Infraestructura Tecnológica debe velar por mantener las medidas necesarias para salvaguardar la integridad, confidencialidad y disponibilidad de la información a la que se le hace copias de seguridad.

(b) La Oficina de Informática o el administrador de la Infraestructura Tecnológica es el responsable de velar por la confiabilidad de las copias de seguridad para que puedan ser restauradas y por ende usadas posteriormente.

iv. Seguridad Lógica:

(a) Todos los sistemas de información sensibles de la SUPERSERVICIOS deben ser utilizados mediante el uso de un usuario y contraseña. De la misma manera se deben establecer roles que definan privilegios al acceder a la información de la entidad.

(b) Es un deber del administrador de la Infraestructura Tecnológica la sincronización aûtomática de la hora en los distintos servidores y demás elementos de la Infraestructura Tecnológica, con la hora de los servidores de la Superintendencia de Industria y Comercio (SIC) o de la entidad que registre la hora oficial para Colombia. De esta manera se asegura la confiabilidad y la integridad de las transacciones realizadas en los sistemas de información de la SUPERSERVICIOS.

ARTÍCULO DÉCIMO CUARTO – CENTRO DE CÓMPUTO: El centro de cómputo está diseñado para alojar los datos que son generados, procesados o recibidos en la SUPERSERVICIOS. Por consiguiente, el centro de cómputo es un área restringida y ningún usuario debe ingresar sin autorización del Jefe de la Oficina de Informática o por el administrador del centro de cómputo. Se deben tener en cuenta los siguientes aspectos:

RESOLUCION No. SSPD - 20115000009075 DEL 13-04-2011

Por la cual: **Se establecen las políticas de seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios**

(a) El ingreso al centro de cómputo solo podrá ser efectuado por las personas autorizadas. Dicho acceso debe ser controlado a través de mecanismos biométricos.

(b) Las personas que ingresen al centro de cómputo deben acatar las normas mínimas de seguridad como lo son:

- No ingresar ningún tipo de alimento ni bebidas.
- No accionar la alarma sin razón evidente.
- No manipular ningún tipo de objeto que pueda ocasionar que las alarmas y sistemas de seguridad se accionen.
- No operar ningún equipo de cómputo sin autorización del administrador del centro de cómputo.
- No realizar labores de limpieza utilizando productos que puedan ocasionar daños a los elementos alojados en el centro de cómputo.
- No desconectar ningún elemento alojado en el centro de cómputo sin la autorización del administrador del centro de cómputo.

ARTÍCULO DÉCIMO QUINTO – INSTALACIONES ELÉCTRICAS: La SUPERSERVICIOS debe contar con un procedimiento definido donde se indique la prioridad de suministro de energía alterna a los distintos componentes de la Infraestructura Tecnológica.

ARTÍCULO DÉCIMO SEXTO - PLAN DE CONTINGENCIA: La SUPERSERVICIOS debe contar con procedimientos alternativos a la operación normal, que permiten a la entidad seguir operando ante un incidente interno o externo no catastrófico.

La Oficina de Informática o el administrador de la Infraestructura Tecnológica elaborará y mantendrá actualizado el plan de contingencia de la Infraestructura Tecnológica, teniendo en cuenta las necesidades de las diferentes dependencias de las SUPERSERVICIOS. Con el propósito de cumplir con el plan de contingencia de la Infraestructura Tecnológica, se deben cumplir los siguientes aspectos:

(a) Se debe tener un plan de contingencia para los servicios de información de la SUPERSERVICIOS, en los cuales se tengan procedimientos que permitan tener una continuidad en el servicio, en el momento en que se presenten fallas no catastróficas en los sistemas.

(b) Se debe realizar por lo menos una prueba al año al plan de contingencia por parte de la Oficina de Informática, con el fin de verificar la efectividad del mismo y generar las acciones correctivas o de mejora que se requieran.

(c) Cada vez que se adquieran nuevas tecnologías, debe ser revisado el plan de contingencia para involucrar los controles de las mismas.

ARTÍCULO DÉCIMO SÉPTIMO – DERECHOS DE PROPIEDAD INTELECTUAL. La SUPERSERVICIOS no permitirá ni tolerará, bajo ningún motivo, la violación de derechos de propiedad intelectual. En consecuencia, los usuarios de la Infraestructura Tecnológica de la SUPERSERVICIOS se abstendrán de realizar acciones que atenten contra estos derechos, so pena de las denuncias y sanciones a que haya lugar.

ARTÍCULO DÉCIMO OCTAVO – SANCIONES: El incumplimiento de las disposiciones contenidas en la presente resolución, podrá dar lugar, según corresponda, a la iniciación de las investigaciones y aplicación de las acciones pertinentes, de conformidad con lo dispuesto es las disposiciones legales vigentes. La Oficina de Informática dará aviso al estamento correspondiente ante cualquier eventualidad.