ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SALUD

SECRETARIA DISTRITAL DE SALUD DE BOGOTÁ

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SDS

Documento Técnico
Versión 3.0

Septiembre de 2012

Cra. 32 No. 12-81
Tel.: 364 9090
www.saludcapital.gov.co
Info: Línea 195

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SALUD

CONTROL DE ACTUALIZACIONES

Código	Versión	Fecha	Resumen de cambios	Elaboró	Aprobó
	1.0	27/03/2011	Primera versión	Ing. Marco Robayo	Ing. Jairo Bahamón
	2.0	29/03/2012	Primera versión	Ing. John Triana	Ing. Jairo Bahamón
	3.0	04/09/2012	Primera versión	Ing. John Triana	Ing. Jairo Bahamón

Elaboró: Comité de Seguridad de la Información de la SDS

TABLA DE CONTENIDO

POLITICA DE SEGURIDAD DE LA INFORMACION DE LA SECRETARIA DISTRITAL DE SALUD

La política pública para el Distrito Capital en materia de salud, está orientada a reducir la desigualdad, la discriminación social, económica y cultural, por lo que se propone modificar las condiciones que restringen el acceso a condiciones de salud y nutrición adecuadas para su desarrollo integral, generando respuesta a las necesidades de la población, en lo individual, familiar y colectivo, mediante la implementación de un modelo de atención en salud que beneficie a toda la población sin distinciones; fundamentado lo anterior en la Estrategia de Atención Primaria en Salud [APS]; que integre la atención en salud, articulando las redes de servicios, garantizando la participación y el compromiso de todos los sectores y actores sociales.

El Plan de Salud del Distrito Capital (PSDC) es la apuesta política para la transformación de los procesos relacionados con la calidad de vida y la salud de los Bogotanos y se soporta en los postulados internacionales, nacionales y Distritales. Se soporta en los compromisos que se tienen como ciudad con su gente, con el país y con el mundo en la contribución que desde ciudad se hace para el cumplimiento de los objetivos del milenio, los cuales pretenden disminuir la pobreza, promover la educación y mejorar los indicadores de calidad de vida de la población, así como de la agenda de salud de las Américas, de las políticas sociales de Bogotá y se armoniza con el plan de desarrollo económico, social y de obras publicas 2012 -2016 " "Bogotá Humana".

El PSDC, propone mejorar las condiciones de salud a través de seis objetivos en el plan marco y cinco ejes estructurantes: aseguramiento, prestación y desarrollo de servicios, salud pública e intervenciones colectivas, vigilancia y control de riesgos profesionales, emergencias y desastres y promoción social.

Se busca optimizar la oportunidad, integridad, confidencialidad y consistencia de la información para la toma de decisiones de gestión en salud del distrito capital, facilitar los flujos de información y comunicaciones los niveles intrainterinstitucional, intersectorial y fortalecer la incorporación de las tecnologías a los procesos de salud en los territorios con énfasis en la promoción de la salud, la detección y la prevención de la enfermedad. Materializar un proceso tecnológico implica la búsqueda e implementación de herramientas que garanticen el acceso y la utilización de las tecnologías cumpliendo con parámetros mínimos de calidad y seguridad.

1. Política de seguridad

1.1. Introducción

La modernización del Estado y de las entidades del Estado, lleva implícito el uso de las tecnologías de la información y de la comunicación, en tal sentido el traslado de datos a través de la red, pueden verse afectados por pérdida, uso indebido, daño o alteración, siendo necesario generar mecanismos para garantizar su seguridad.

En el mismo sentido, el deterioro o indisponibilidad de los Sistemas de Información puede interrumpir el normal desarrollo de la operatividad, produciendo efectos negativos en la calidad del servicio y los beneficios que la entidad presta.

Por lo anterior, con este documento se busca establecer el marco normativo con relación a la seguridad de la información para los funcionarios de la Secretaria Distrital de Salud (SDS), describiendo lo que se espera de todo el personal que trabaja para la SDS y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos tecnológicos de la entidad en general, garantizando, la confidencialidad, integridad y disponibilidad de la información y sistemas de información. La Política de Seguridad refleja requerimientos de orden legal, ético y de mejores prácticas en el ejercicio de las actividades que se ejecutan a diario.

Las medidas que se implementan no sólo son soluciones técnicas, sino también reflejan reglas claramente definidas, para dar el mejor uso a los recursos de TIC, por parte del usuario final de la plataforma tecnológica de la SDS.

Lo que se trata de demostrar es que se debe afrontar el tema de la seguridad de la información a nivel global y que debe constar de los siguientes elementos:

- Sensibilizar a los usuarios de la entidad acerca de los problemas de seguridad de la información.
- Seguridad lógica, es decir, la seguridad a nivel de los datos, en especial los datos de la entidad, las aplicaciones e incluso los sistemas operativos de la SDS.
- Seguridad en las telecomunicaciones: tecnologías de red, servidores de la entidad, redes de acceso, etc.
- Seguridad física, o la seguridad de infraestructuras materiales: asegurar centro de cómputo, centro de cableado, las estaciones de trabajo de los empleados, etc.

La política de seguridad comprende todas las reglas de seguridad que sigue la entidad, por lo tanto todas las personas que laboran en la SDS, deben conocer la política definida, ya que afecta a todos los usuarios del sistema.

1.2. Objetivo General

Garantizar que la plataforma tecnológica de la SDS (recursos de software, recursos de hardware, sistemas de información) se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto, acatando las normas y políticas de seguridad de la información.

1.2.1. Objetivos Específicos

- Garantizar que los datos estén libres de modificaciones no autorizadas “Integridad”.

- Asegurar que sólo los usuarios autorizados tengan acceso a los recursos que se intercambian “Confidencialidad”.
- Garantizar el correcto funcionamiento de los sistemas de información “Disponibilidad”.
- Garantizar de que no pueda negar una operación realizada “No repudio”.
- Asegurar que sólo los individuos autorizados tengan acceso a los recursos “Autenticación”.

1.3. Alcance

El propósito principal de los datos, recursos y servicios informáticos de la Secretaria Distrital de Salud es el de contribuir al cumplimiento de objetivos de la entidad, por ello, todas las personas (Funcionarios y Contratistas), que los utilicen deben estar de acuerdo y compartir este propósito. En efecto, se espera y así se exige, que, quien los utilice, actúe acorde con este propósito y lo haga con suma responsabilidad, incluyendo el cuidado físico de los mismos. Todos los usuarios de la plataforma tecnológica de la SDS, asumen la responsabilidad de conocer, entender y seguir todas las normas, políticas y procedimientos de seguridad de la información establecidos, cumpliendo con las directrices administrativas trazadas para tal fin.

La Dirección de Planeación y Sistemas (DPS), puede acceder e inspeccionar, sin necesidad de previo aviso, a todos los dispositivos informáticos propiedad de la Secretaría, conectados o no a la red y de los recursos de software, para los propósitos de resolución de problemas o para investigar violaciones a las políticas, normas y procedimientos definidos por la entidad.

2. Aspectos organizativos de la seguridad

La DPS, como administrador de la plataforma tecnológica y generador de la política general de seguridad de la información de la SDS, garantiza la adecuada gestión de la seguridad de la información procesada y/o que albergada por los sistemas y servicios contemplados en el alcance. Para desarrollar esta política, esta dirección bajo la gestión del Referente de Seguridad de la Información y con aval del Comité de Seguridad de la Información de la SDS, se compromete a:

- Llevar a cabo un análisis de riesgos que permita mantener una adecuada visión de los riesgos de seguridad de la información a los que están expuestos los activos y desarrollar las medidas necesarias para limitar y reducir dichos riesgos, definiendo las medidas de seguridad a establecer.

- Desarrollar una completa normativa de seguridad que regule las condiciones en las que la entidad, dentro del alcance establecido, debe desarrollar su actividad para respetar los requerimientos de seguridad de la información establecidos.

- Destinar los recursos y medios necesarios para desarrollar todas las medidas de seguridad que se determinen, manteniendo un adecuado balance entre costo y beneficio.

- Establecer un plan de formación y concientización en materia de seguridad de la información que ayude a todo el personal implicado a conocer y cumplir las medidas de seguridad establecidas y a participar de forma proactiva en la gestión de la seguridad de la información.

- Desarrollar todas las medidas necesarias para garantizar la adecuada gestión de los incidentes de seguridad que puedan producirse, y que permitan la resolución tanto de las incidencias menores como de las situaciones que puedan poner en riesgo la continuidad de las actividades contempladas.

- Impulsar y velar por el desarrollo, cumplimiento y mantenimiento del Plan de Continuidad de Negocio (PCN) de la SDS como máxima responsable del mismo. La Dirección entiende el PCN de la SDS, como un proceso de carácter cíclico y continuo, con responsables y responsabilidades asignadas, y con procedimientos técnicos y organizativos, definidos y auditables.

- Definir e implantar un Proceso de Continuidad orientado a proteger los servicios y procesos de TIC de la entidad.

- Propiciar y facilitar la participación y asunción de responsabilidades de los empleados y colaboradores en la preparación, implantación, mantenimiento y ejecución del PCN de la SDS.

Las políticas de seguridad general para la Secretaría, prevalecen sobre los requerimientos individuales y cualquier eventualidad de excepción a los mismos deberá ser analizada. En caso de ser necesario se llevará al “Comité de seguridad” quien definirá o no su aplicación.

El comité de seguridad de la información de la SDS, establece los procedimientos y formas de actuación necesarias para garantizar el correcto desarrollo de esta política, que se plasman en un sistema de seguridad, documentado y conocido por todo el personal de la SDS, y que cumple los requisitos establecidos en la norma ISO/IEC 27001.

De la misma manera la DPS, como generador de la política general de seguridad de la información, implementa las siguientes políticas generales:

- La DPS, es el único autorizado para ingresar a la red de la SDS, nuevos recursos y sistemas informáticos (Software, hardware, seguridad, equipos de red etc). Esta

Dirección será la responsable de coordinar la reparación y mantenimiento de equipos, las reparaciones y/o ampliaciones de estos equipos no pueden ser hechas o contratadas por ningún usuario diferente a la DPS.

- La administración de toda la plataforma tecnológica de la SDS, es responsabilidad de la DPS.

- A criterio de la DPS, aquellos equipos, sistemas, software utilitario que puedan calificarse como riesgosos para la entidad o para los datos que tiene la entidad, o para los sistemas o los servicios de TIC, serán desconectados de la red, sin aviso previo.
- Toda persona que use o acceda a los recursos o servicios de TIC de la SDS, deberá utilizarlo para los fines destinados a contribuir al cumplimiento de los objetivos de la Secretaria Distrital de Salud, para el cumplimiento de esta política, se obliga a todo el personal (Funcionarios y Contratistas), a solicitar autorización previa por parte del jefe inmediato.

- Todo el personal de la Secretaría, (Funcionarios y Contratistas) será responsable civil y penalmente, por la mala utilización de la información reservada.

- Los dispositivos y sistemas conectados a la Red en todo momento, deben contar con las licencias de software, conforme a las leyes que regulan la materia.

- Todos los PC, que se conecten en red interna de la SDS, deberán tener instalado en forma permanente y actualizada un antivirus activo.

- El uso o conexión a los recursos y servicios de TI de la Red de la SDS, implica el total conocimiento y aceptación de las normas y políticas que regulan el uso de estos recursos, al ingresar a la Red, el usuario asume toda responsabilidad legal que surja de una violación a estas políticas.

- Cada usuario, deberá velar por el cumplimiento de las políticas permanentes de resguardo de la información a su cargo y de su dependencia (donde labora), estipulando mecanismos y tiempos para la realización de copias de respaldo de su estación de trabajo, controlando la efectividad de este procedimiento.

- La información que reside en cada PC o medio de almacenamiento auxiliar (Diskette, CD, USB, Disco externo etc.) es responsabilidad de cada usuario**.**

3. Clasificación y control de activos

Inventario y nivel de protección de los activos.

3.1. Activos de Información

Definición: Recurso de información que tiene valor para la entidad.

3.1.1. Políticas de seguridad de activos de información.

Objetivo de Control: Proveer dirección y soporte a la administración para la seguridad de información.

Protección y respaldo de la información

- Se deberá preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad y Disponibilidad de la información de la institución.
- La información de la institución deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite.
- La institución deberá identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información sean adecuadas.
- Los niveles de protección y clasificación establecidos para la información de la institución deberán ser mantenidos en todo momento. (Acceso, toma de respaldo, backup, transporte, recuperación, otros). Por lo tanto se deben mantener los controles y medidas establecidas para esto.
- Los usuarios de la institución son responsables de alojar la información que necesita ser respaldada en los lugares establecidos para ello.
- Los usuarios respaldarán y protegerán, con medidas que eviten accesos de personas no autorizadas, aquellos activos digitales de información que estén almacenados en elementos de TI de uso personal, que les hayan sido asignados. Se deberán preservar los lineamientos de acuerdo a la sensibilidad y nivel de clasificación de seguridad.
- Los usuarios son responsables de aplicar los controles para la protección de la información según su nivel de clasificación. Así mismo deberán alertar a la DPS cuando un activo digital de información requiera medidas especiales de protección.

3.2. Activos de software

Definición: Los Activos de Software se pueden aplicar a prácticamente cualquier aspecto del entorno de TI en una organización, pero sobre todo a aquellos que tienen que ver con la gestión de licencias de software e inventario de activos. Entre sus ventajas destacan su capacidad para gestionar de manera coherente los documentos de prueba de licencia, Los distintos modelos de licencia, Las distintas plataformas de software, Los medios de instalación y copias de distribución de los

productos, Las versiones y ediciones, Todo el software instalado, Listas detalladas de versiones, parches y actualizaciones, Las licencias, Los contratos, Medios de distribución, tanto físicos como electrónicos.

3.2.1. Políticas de seguridad de activos de software.

Objetivo de Control: Proveer dirección y soporte a la administración para la seguridad activos de software.

- Los medios, documentos o licencias de software deben están custodiados por un referente y almacenados en caja fuerte.
- La gestión y/o administración de las licencias de software deben ser de responsabilidad de la Dirección de Planeación y Sistemas.
- Se debe contar con un directorio (DML) para almacenar los medios magnéticos para la instalación de software licenciado por la SDS.

4. Seguridad ligada al personal

Reducir riesgos de errores humanos, robos, fraudes o mal uso de los recursos.

4.1. Derechos y obligaciones de los funcionarios de la SDS

- El propósito principal, de los datos, recursos y servicios informáticos, es el de contribuir al cumplimiento de objetivos de la Secretaria Distrital de Salud, por ello, todas las personas (Funcionarios y Contratistas), que los utilicen deben estar de acuerdo y compartir este propósito. En efecto, se espera y así se exige, que, quien los utilice, actúe acorde con este propósito y lo haga con suma responsabilidad, incluyendo el cuidado físico de los mismos. Los Usuarios asumen la responsabilidad de conocer, entender y seguir los procedimientos administrativos, establecidos cumpliendo con las directrices administrativas trazadas para tal fin.

- Sin perjuicio de las normas Constitucionales, legales y reglamentarias que regulan la materia, cada Usuario asume individual y solidariamente, toda responsabilidad derivada de los daños y perjuicios que el mal de las TIC y de la información puedan hacer.

- Cada funcionario debe almacenar la información relevante para la entidad en la carpeta asignada a los usuarios (H: Home Directory) y a la cual la DPS le hace backup dentro del esquema definido**.**

- Cada Jefe de dependencia (Secretaría, Subsecretaría, Oficina, Dirección, grupo) es el responsable de solicitar y cancelar ante la DPS los recursos de hardware, software o servicios que requiera el funcionario o contratista a su cargo: Computador, impresora, cuenta de red, correo electrónico, claves, sistemas de información, Home directory "H:", acceso a carpetas (privada o públicas de cada dependencia)

- Es responsabilidad del Jefe inmediato de un Usuario, solicitar formalmente a la DPS, los perfiles de usuario con sus privilegios, de acuerdo con el tipo de información que se requiera operar, así como retirar solicitar su cancelación cuando ya no los estime conveniente o necesarios.

- Cada usuario, al momento de retirarse de la Secretaría, o cuando no lo requiera, deberá solicitar a la mesa de servicios de TIC, la cancelación dela cuentas de red, correo electrónico y demás permisos que tenga a su cargo, de no hacerlo, el jefe inmediato, lo podrá solicitar.

- Es obligación del jefe inmediato, informar previamente a los usuarios que utilizan un aplicativo, cuál información está clasificada como confidencial y qué medidas de seguridad se deben tener para el manejo y disposición de datos e información.

- Para todo funcionario no está permitido compartir claves de usuarios o de aplicativos. El nombre de usuario y la clave de acceso asignados a un funcionario, son personales e intransferibles. No se permite la utilización de ningún usuario anónimo. La autorización de acceso a los recursos es exclusiva al usuario al que le fue asignada y no es transferible ni heredable a otros usuarios o dispositivos.

- Ningún funcionario podrá hacer utilización de cualquier recurso informático de la Red de la SDS, con propósitos comerciales en beneficio del Usuario y/o de terceros.

- Para todo funcionario no está permitido la utilización de cualquier recurso informático de la Red de una manera que viole cualquier norma Nacional o Internacional.

- Ningún funcionario está autorizado a realizar instalaciones de hardware y/o software sin la autorización de la DPS.

- No se autoriza a ningún funcionario permitir a personal externo acceder a recursos informáticos con su usuario y clave personal**.**

5. Seguridad física y del entorno

Evitar accesos no autorizados, violación, daños o perturbaciones a las instalaciones y a los datos.

5.1. Seguridad de áreas

5.1.1. Controles físicos de entrada.

- Cualquier persona “interna o externa”, que ingresa a la entidad con equipos de cómputo portátiles o de escritorio, debe realizar el respectivo registro de los equipos en los puestos de vigilancia.

5.1.2. Seguridad centro de cómputo

- No se permite el ingreso al área de especialistas del centro de cómputo a personal no autorizado.

- El personal autorizado a ingresar al área de especialistas del centro de computo y que tiene su puesto de trabajo en esa área no podrá atender o hacer ingresar usuarios o personal no autorizado al interior de la misma.

- El ingreso de personal externo (proveedores, consultores, directivos etc.), se registrara en el formato de control de ingreso y debe realizarse con el acompañamiento de uno de los administradores.

5.1.3. Seguridad centros de cableado.

- A los centros de cableado solo podrá ingresar (previo aviso a la sala de control): el referente de seguridad, el administrador de la red y el personal del centro de control y monitoreo de la entidad.

- El ingreso de personal externo (proveedores, consultores, directivos etc.), debe realizarse con el acompañamiento de una de las personas autorizadas.

6. Gestión de comunicaciones y operaciones

Asegurar la operación correcta y segura de los recursos de tratamiento de información.

6.1.1. Gestión de la seguridad en red.

- Todos los requerimientos sobre compra, arriendo, préstamo, donación etc. de cualquier tipo de equipo o elemento tecnológico, deberá canalizarse en forma oportuna a través de la DPS, quien revisará su pertinencia,

conveniencia, compatibilidad, disponibilidad de recursos y procederá a conceptuar y/o a la provisión correspondiente.

- No se permite realizar conexiones no autorizadas a la red, tanto alámbrica como inalámbrica.

- No está permitido que un funcionario de la SDS, prive o intente privar a otros usuarios de la utilización y/o acceso a recursos informáticos de la Red que estén autorizados.

- No se permite a ningún funcionario penetrar o intentar penetrar sin autorización, la seguridad de cualquier comunicación de la red.

- Cualquier trabajo de adición de puntos de red en el cableado estructurado de la SDS, deberá tener el apoyo técnico y acompañamiento de la Dirección de Planeación y Sistemas con el fin de garantizar el cumplimiento del estándar establecido e implementado por la entidad, en donde se especifican las condiciones y características del cableado a instalar.

6.1.2. Gestión de la seguridad en el sistema de mensajería.

- El correo electrónico es para la SDS un medio de comunicación institucional, formal y está sujeto a las disposiciones nacionales e internacionales vigentes y como tal debe dársele un buen uso.

- No se puede utilizar el correo electrónico o sistema de mensajería, para enviar contenido abusivo, ofensivo, obsceno, subversivo o saturar los canales de comunicaciones, o el envío "cadenas", y otros esquemas que pueden causar tráfico excesivo en la red o cargar los sistemas informáticos.

- No se puede utilizar el correo electrónico o sistema de mensajería para generar, guardar o transportar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo, lesivo al buen nombre y honor de la SDS, o cualquiera persona, propagandas comerciales, cadenas, difusión de actividades lucrativas en general, ni para actividad no administrativa o de servicio, proselitismo político.

7. Control de accesos a los sistemas de información

Evitar accesos no autorizados a los sistemas de información (de usuarios, computadores, redes, etc.)

7.1.1. Requisitos para el control de acceso.

- Todos los usuarios que acceden a recursos de TIC de la red interna de la SDS, requieren de una única e intransferible identidad, normalmente un

nombre de usuario para una única persona, y un nombre de máquina para un PC. Esta identidad se usa para representar un usuario o dispositivo en el ambiente informático de la red. La DPS proporcionará este identificador como parte del proceso de autorización. Todas las acciones realizadas bajo los auspicios de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular del identificador.

7.1.2. Gestión de acceso de usuarios

- La DPS debe garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los servicios de red de la SDS y a los sistemas de información.
- La asignación de cuenta de usuario es responsabilidad de la DPS, previa solicitud formal del director, supervisor o jefe inmediato del funcionario o contratista.
- Es responsabilidad del director, supervisor o jefe inmediato, informar la des habilitación de la cuenta de usuario por motivo de la no permanencia del funcionario en la entidad o por no necesitar dichos recursos.
- La DPS debe aplicar el control de deshabilitar la cuenta de usuario por inactividad mayor a treinta (30) días calendario.
- No se podrá eliminar ninguna cuenta de usuario en un tiempo no menor a dos (2) años.

7.1.3. Responsabilidad de los usuarios.

- No está permitido a terceros, el ingreso a los recursos tecnológicos de la Secretaria Distrital de Salud sin autorización previa del Jefe inmediato o el supervisor del contrato.

7.1.4. Control de acceso a la red.

- El mal uso de la identidad de un usuario o un dispositivo constituye falsificación o falsedad. Sin perjuicio de las acciones legales, toda acción que involucre acceso desautorizado, impropio o el mal uso de recursos informáticos de la red interna de la SDS, está sujeta a sanciones disciplinarias o legales pertinentes.

7.1.5. Control de accesos al sistema operativo.

- No se permite alterar la configuración del software de los equipos, Sistema Operativo, Motores de Base de Datos, Herramientas de Desarrollo, Utilitarios del Sistema, Software de Comunicaciones de un PC o de la Red, sin previa autorización de La DPS.

- En las estaciones de usuario final se tendrán como estándar dos usuarios genéricos como administradores locales (Admins del dominio – G – Operadores de la red), no se podrán adicionar y/o configurar usuarios con privilegios de administración local. Ante una solicitud de adicionar a la maquina un usuario de la red con privilegios de administración local, esta solicitud deberá ser enviada previamente por el jefe inmediato y escalada al Referente de Seguridad de la Información, quien evaluará y analizará si el usuario, dentro de las actividades propias de sus funciones, requiere este perfil o nivel de permisos.

7.1.6. Control de acceso a aplicaciones e información.

- A todo funcionario y proveedor de servicios de la SDS, no está permitido el uso no autorizado de cuentas de red y de computadores u otras formas de acceso a los recursos informáticos.

- Los dispositivos y sistemas conectados a la Red deben, en todo momento, estar por completo de conformidad con las licencias de software adquiridas y disponibles en la SDS.

7.1.7. Control de acceso a computación móvil (Wireless).

- La red inalámbrica de la SDS usa el estándar 802.11a/b/g. Por lo tanto las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar.

- En la entidad se definen cuatro (4) redes inalámbricas, cada una con propósito especifico:
  1. SDS-LC, (Local) corresponde a usuarios internos “funcionarios” que se conectaran a la red autenticándose ante el dominio de la entidad, aplicándole así todas las políticas y directivas institucionales definidas en el Directorio Activo,
  2. SDS-IO, (invitado ocasional) corresponde a usuarios externos que se autenticaran ante el controlador de la red inalámbrica, no tendrán acceso a la red interna, solo tendrán salida a internet y la navegación será controlada por las políticas de la entidad,
  3. SDS-IP, (Invitado permanente) corresponde a usuarios invitados permanentes los cuales poseen dispositivos móviles y necesitan estar conectados permanentemente a Internet,
  4. WIFI-VOZ, corresponde a la red de voz inalámbrica de la entidad.

- Los equipos externos, “entiéndase por cualquier equipo de computo portátil que ingresa a la SDS por parte de proveedores, visitantes o equipos personales de funcionarios y/o contratistas, que no son de

propiedad de la entidad y no están como equipos miembros del dominio", no podrán ser conectados a ninguno de los puertos de la red LAN de la entidad y cualquier intención de conexión será tomado como un intento de acceso no autorizado. Estos equipos solo se podrán conectar inalámbricamente a la red llamada "SDS-IO", que fue creada para prestarles el servicio de navegación hacia internet sin tener acceso a la red interna de la SDS.

- No está permitida la instalación de dispositivos inalámbricos que brinden acceso inalámbrico a la red sin la debida autorización de la DPS.

- La SDS no controla ni es responsable del contenido y veracidad de la información que se transporta en la red interna, en consecuencia los usuarios son responsables por la utilización el servicio de manera apropiada.

- Los usuarios de la red interna, de la SDS son responsables de la seguridad de la información en las transacciones que envíen por la Red Inalámbrica. Por tanto se recomienda que utilicen aplicaciones seguras (secure shell, https, etc.).

- La SDS en conocimiento que las redes inalámbricas son fundamentalmente inseguras, en virtud de que el envío de la información se realiza por un medio compartido, por consiguiente recomienda abstenerse de realizar transacciones bancarias o similares, ya que no es posible por dicho medio garantizar la seguridad de las transmisiones.

- Todo funcionario y/o usuario debe abstenerse de publicar o pasar a terceros no autorizados por la SDS, las claves e información de acceso a la red o de obtenerlas o decodificarlas en caso de que no se les proporcione directamente por la entidad.

- No está permitido el uso de la red interna, con fines de lucro o propósitos comerciales que no estén directamente relacionados con asuntos que la propia entidad autorice, difunda y solicite.

- No se permite descargar servicios de difusión o broadcast, tales como audio y video.

- No está permitido usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.

- No está permitido extender el servicio de acceso a la red interna a más equipos por medio de conexiones a la red inalámbrica no autorizadas

para éste fin (ej: por medio de NAT, túneles, conexión compartida a internet, etc.) y/o extender el alcance de la red por medio de cualquier dispositivo físico o lógico (tales como antenas o repetidores) más allá de la superficie o límite físico de la entidad.

- No se autoriza obtener acceso a cualquier recurso computacional, sistema o sitio de telecomunicaciones a los que no le está permitido acceder.
- No se permite realizar actividades de rastreo, ataques de negación de servicio, difusión de virus, spyware o programas considerados dañinos o inapropiados o cualquier otra actividad informática ilícita.

- La DPS se reserva el derecho de controlar o negar el acceso al servicio de la red interna de la SDS a aquellas personas que no cumplan con los requisitos de uso establecidos en esta política.

- La DPS se reserva el derecho de permitir o negar la instalación del correo electrónico Outlook en Equipos móviles.

Cualquier funcionario y/o usuario de la SDS que viole estas políticas estará sujeto a las sanciones disciplinarias, sin perjuicio de las acciones legales que se puedan tomar en su contra.

8. Desarrollo y mantenimiento de sistemas

Garantizar que la seguridad está incorporada dentro de los sistemas de información, con el fin de evitar pérdidas, modificaciones, mal uso.

8.1. Especificaciones y requisitos para la adquisición desarrollo y mantenimiento de sistemas de información.

- Todo desarrollo, cambio, actualización, compra, mejora o implantación de Software deberá solicitarse oportunamente a través de la Dirección de Planeación y Sistemas.

- No está permitida la creación de archivos de copias de seguridad en los servidores que son accesibles desde redes externas.

- Para la publicación de páginas web de la entidad, se debe restringir o eliminar el acceso a directorios sensibles que contengan información como bases de datos o paginas de administración.

- Para la publicación de páginas web de la entidad, se debe implementar certificados de cifrados de seguridad SSL de encriptación robusta.

8.2. Seguridad sistemas de información y de datos de los mismos.

- El referente del ambiente de producción de un sistema de información, es el jefe de grupo o de dependencia, y por ningún motivo, funcionarios diferentes a los asignados por él, tendrán acceso a la información y/o aplicativos que reposen en este ambiente. Así mismo, será el encargado de aprobar formalmente los cambios o nuevas implantaciones, módulos o nuevos procedimientos.

9. Gestión de incidentes

Gestionar los incidentes que afectan la seguridad de la información, teniendo en cuenta técnicas y clasificación de incidentes, no se permite a todo funcionario de la SDS hacer y usar:

- La utilización de técnicas y/o herramientas de “Hacking”.
- La ingeniería inversa, cracking o descriptación de contraseñas.
- El escaneo de puertos de TCP/IP.
- La sustitución de usuarios o Hacking.
- La sustitución de paquetes IP, también conocida como IP spoofing
- La utilización de analizadores de protocolos o scanners de tráfico de red.
- Grabadoras de teclas o Key Loggers
- Hardware para ataques de Tempesting.
- Herramientas de denegación de servicio.
- Utilización de identificadores de usuarios ajenos a la Secretaría
- Hacer ingeniería social.
- El uso de computadoras como gateways o routers a otra red o como servidor de acceso remoto, se requiere en todo caso autorización previa y expresa de la DPS.
- Crear, utilizar o distribuir programas como virus, troyanos, key loggers etc., que puedan causar daño a datos, archivos, aplicaciones, funcionamientos de los sistemas o alteren el funcionamientos de la red.
- Capturar, desencriptar, difundir contraseñas y/o protocolos de comunicaciones.
- Inspeccionar, modificar o copiar programas o datos sin la autorización del jefe inmediato o que atenten contra las normas legales y reglamentarias vigentes sobre utilización de software y/o propiedad intelectual.
- Utilizar cualquier correo electrónico o sistema de mensajería, para enviar contenido abusivo, ofensivo, obsceno, subversivo o saturar los canales de comunicaciones, o el envío "cadenas de cartas", y otros esquemas que pueden causar tráfico excesivo en la red o cargar los sistemas informáticos.
- Utilización de cualquier recurso informático de la Red para generar, guardar o transportar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo, lesivo al buen nombre y honor de la S.D.S., o cualquiera persona, propagandas comerciales, cadenas, difusión de actividades

lucrativas en general, ni para actividad no administrativa o de servicio, proselitismo político.

- Alterar el software o la configuración del hardware de cualquier equipo o computador o agregar cualquier dispositivo o sistema a la red sin el permiso correspondiente.
- Utilización de software comercial que no esté licenciado, ya sea texto, imágenes gráficas, o grabaciones de audio o video.
- Utilización de la Red para ganar o intentar ganar el acceso desautorizado a los recursos de información locales o remotos.
- Posesión o utilización de cualquier software o hardware que pueda comprometer la seguridad de la red y/o de cualquier recurso informático de la Red.
- Los usuarios en cuyos dispositivos de almacenamiento, discos, home directory (H:), carpetas pública o privadas de las dependencias, se encuentre software no autorizado, archivos de música, videos, fotografías no institucionales, se les procederá a borrar dichos archivos sin previo aviso, y la DPS podrá dirigir estos hallazgos a la dependencia competente para que se proceda a dar curso a las investigaciones a que dieran lugar.
- Las copias de seguridad o backup de la información que no se encuentren respaldado en el esquema de backup será asumido por el usuario quien es el único responsable.

10. Gestión de continuidad del negocio

Reaccionar a la interrupción de las actividades del negocio y proteger sus procesos críticos frente a fallas, ataques o desastres.

10.1. Administración de la plataforma de red.

- Durante los periodos en que la administración de la plataforma Tecnológica de la SDS, este cedida a un tercero y/o bajo la figura de Outsourcing, la firma encargada creara una cuenta administradora del Dominio, llamada “usersds” que solo será conocida por personal de la entidad para realizar tareas propias de monitoreo y verificación de la gestión del tercero. Esta cuenta será también verificada y monitoreada. Con esta cuenta el personal de la SDS podrá ingresar, monitorear y revisar cualquier componente de la plataforma tecnológica de la SDS sin previo aviso al proveedor.