SUBSISTEMA DE CONTROL DE GESTIÓN
COMPONENTE - INFORMACIÓN
ELEMENTO - SISTEMAS DE INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN CENTRAL DEL MUNICIPIO DE SANTIAGO DE CALI

Versión 1

Macroproceso: Gestión Tecnológica y de la Información
Proceso: Administración de Recursos de Tecnologías de Información y Comunicación

Septiembre 9 de 2010

CONTENIDO

pág

1. INTRODUCCIÓN

La información es considerada actualmente como el mayor tesoro de las empresas, es por ello que se debe tener muy presente cómo protegerla de todo tipo de ataques que le puedan hacer; bien sea ataques físicos o lógicos. Por esta razón es muy importante tener bien definidas políticas que permitan darle protección al Sistema de Información, a través de la protección tanto física como lógica de la red de comunicaciones.

La información constituye un activo que, como todos los demás activos comerciales importantes, es valioso para toda organización; por eso es necesario protegerlo de una manera apropiada. La seguridad de la información protege la información contra amenazas muy diversas, para asegurar la continuidad de las actividades de la entidad.

La información se presenta de diversas formas. Puede ser impresa o escrita sobre papel, almacenada en soportes electrónicos, transmitida por correo o utilizando medios electrónicos, expuesta sobre películas o hablada en conversaciones. Cualquiera sea la forma que tenga la información o los medios por los cuales es transmitida o almacenada, ella debe ser siempre protegida de manera apropiada.

Política de Seguridad de los Sistemas de Información de la Administración Central del Municipio de Santiago de Cali, contemplará tres (3) grandes políticas: Política de Seguridad Informática, Políticas Generales de Seguridad de los Sistemas de Información y la Política de Seguridad de la Información.

2. OBJETIVO

Establecer la política administrativa y proveer una guía respecto a la seguridad de los Sistemas de información de la Administración Central del Municipio de Santiago de Cali.

3. ALCANCE

La Política de Seguridad de los Sistemas de Información aplica para todos los usuario(a)s internos y externos de la Administración Central del Municipio de Santiago de Cali.

4 DEFINICIONES

ACCESIBILIDAD WEB. Este término hace referencia al acceso a la web sin importar el tipo de hardware o software utilizado por el usuario, el idioma o la ubicación geográfica del mismo. La Iniciativa de Accesibilidad Web busca permitir a cualquier tipo de persona tener acceso a las herramientas que ofrece la web por medio de diseños o estructuras que faciliten la navegación dentro de la Red.

ARCHIVO ELECTRONICO. Conjunto de documentos electrónicos, producidos y tratados archivísticamente, siguiendo la estructura orgánico funcional del productor, acumulados en un proceso natural, por una institución en el transcurso de su gestión.

ATAQUE CIBERNÉTICO. Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

BACKUP. Guardar en un medio extraíble (para poder guardarlo en lugar seguro) la información sensible referida a un sistema.

BASE DE DATOS. Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso.

BRECHA DE SEGURIDAD. Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

BUSCADOR. Servicio o programa que localiza páginas en Internet que contengan una serie de palabras o datos dados.

CALIDAD. Grado en el que un conjunto de características inherentes cumple con los requisitos.

CARTOGRAFÍA DIGITAL. La cartografía es la ciencia que se encarga del estudio y de la elaboración de los mapas geográficos, territoriales y de diferentes dimensiones lineales y demás. La Cartografía Digital comprende la utilización de métodos de automatización para producir dichos mapas. Es necesario recurrir a nuevas metodologías, técnicas y procesos que permitan la incorporación de las tecnologías digitales al proceso de producción cartográfica, dado que todos los avances que generen nuevo conocimiento en ésta área pueden considerarse investigación en producción cartográfica digital.

CERTIFICADO DIGITAL. Un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

CHAT. Es un anglicismo que usualmente se refiere a una comunicación escrita a través de Internet entre dos o más personas, que se realiza instantáneamente. Su espontaneidad expresada en la falta de convenciones o reglas gramaticales u ortográficas y en la tendencia de los usuario(a)s autodesignarse con pseudónimos o alias llamados nicknames, prueban la cercanía de este tipo de comunicación con la oralidad. En pocas palabras es una herramienta de comunicación sincrónica disponible para múltiples usuario(a)s, cuyo éxito ha llevado a identificarlo como el paradigma de la comunicación ciberespacial.

CIFRAR. Quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama descodificar ó descifrar. Los sistemas de ciframiento se llaman sistemas criptográficos.

CLIENTE. Organización, entidad o persona que recibe un producto y/o servicio. El término cliente incluye a los destinatarios, usuario(a)s o beneficiarios (DUB); los cuales pueden ser internos o externos a la entidad.

CMS (CONTENT MANAGEMENT SYSTEM). Poder conectarse a las bases de datos trajo como consecuencia que los sitios web empezaran a manejar grandes cantidades de información y números de páginas. Para lidiar con la complejidad cada vez mayor fueron ideados los Sistemas de manejo de Contenido mejor conocidos como "Portales". Estos sistemas están compuestos generalmente por herramientas de administración, bases de datos y las páginas que se publican. Muchos de estos portales pueden ser utilizados de forma gratuita debido a que tienen un esquema de licenciamiento público y son de código abierto lo que quiere decir que solo se incurre en los gastos del desarrollo y, eventualmente, infraestructura.

CONFIDENCIALIDAD. Se refiere a que la información solo puede ser conocida por individuos autorizados.

CONTENIDOS. Implican todas las formas de información o datos que se divulgan en la página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños, animaciones.

CONTROL DE ACCESO. El proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (mandatory access control – MAC), o definido por el usuario propietario del objeto (discretionary access control – DAC).

COOKIES. Las cookies son pequeños archivos de texto que son descargados automáticamente (si está permitido por las reglas de seguridad) al navegar en una página web específica.

CORREO ELECTRÓNICO. El correo electrónico (email, electronic mail) es el intercambio de mensajes almacenados en computadora por medio de las telecomunicaciones. Los mensajes de correo electrónico se codifican por lo general en formato de texto ASCII (American Standard Code for Information Interchange). Sin embargo, se pueden también enviar archivos en otros formatos, tales como imágenes gráficas y archivos de sonidos, los cuales son transferidos como archivos anexos en formato binario.

CRACKER. Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en

contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas. Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.

CRIPTOGRAFÍA DE LLAVE PÚBLICA. Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

CUENTA. Es un mecanismo de identificación asignado a un usuario. Este mecanismo debe ser único e intransferible, vigente durante el tiempo de vinculación del usuario con la Alcaldía, y debe estar sujeto a restricciones o políticas definidas para este fin.

DEMO. Es la abreviatura de demostración, implica que un programa puede ser libremente usado aunque usualmente con algunas limitaciones que van desde un funcionamiento parcial (es decir que no trabaja al 100%), hasta un funcionamiento limitado (es decir sólo por un período limitado de tiempo). El objetivo es introducir al usuario en la lógica y servicios del programa, para que este se de una idea de él y de acuerdo a ello decida, con conocimiento de causa, si se siente animado o no a adquirirlo o a usarlo plenamente.

DENIAL OF SERVICE (NEGACIÓN DE SERVICIOS) En seguridad informática, un ataque de denegación de servicio, también llamado ataque Dos (de las siglas en inglés *Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé

abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

DERECHOS DE PROPIEDAD INTELECTUAL. Hacen referencia a todos los derechos de propiedad de la información de La Administración Central del Municipio de Santiago de Cali o de cualquier persona que sea titular legítima, como: signos distintivos, marcas, lemas, enseñas, logos, nombres de dominio, derechos de autor, bases de datos, diseños, contenidos o cualquier otra obra o creación intelectual vinculada con el objeto, operación o desempeño del sitio WEB de La Administración Central del Municipio de Santiago de Cali.

DMS. (Document Management System - sistema de gestión de documentos). Sistema informático utilizado para rastrear y almacenar documentos electrónicos e imágenes de documentos en papel. Suele proporcionar el almacenamiento, la seguridad y las capacidades de recuperación e indexación del contenido.

DOCUMENTO. Información y su medio de soporte. Abarca tanto la información contenida en el documento en si, como las diferentes formas que estos podrían tener tales como los documentos escritos, los discos duros de computador, disquetes, CD, cintas de video, audio y afiches, entre otros.

EDUCACIÓN VIRTUAL. Es una oportunidad de aprendizaje que se acomoda al tiempo y necesidad del estudiante. La educación virtual facilita el manejo de la información y de los contenidos del tema que se quiere tratar y está mediada por las tecnologías de la información y la comunicación -las TIC- que proporcionan herramientas de aprendizaje más estimulantes y motivadoras que las tradicionales.

ENCRIPTACIÓN. (Cifrado, codificación). La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas.

ESTÁNDAR. Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación de las políticas: son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes que crear nuevas políticas.

FAQ. Sección en la que se recopilan las preguntas y respuestas más solicitadas por los visitantes o usuario(a)s de un sitio web.

FIREWALL. (Muro de Fuego - Cortafuego). Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

FORO. Es un servicio basado en el correo electrónico, mediante el cual se forman grupos de personas, con intereses comunes sobre temas específicos, que intercambian información respecto a los mismos a través de sus direcciones de correo. Cualquier mensaje enviado a la lista se distribuye automáticamente a todos los miembros de la misma lista o se publican en el sitio web.

GEOMÁTICA. Conjunto de tecnologías que optimizan la adquisición, procesamiento, análisis y generación tanto de productos como de servicios de información geográfica, los cuales son de gran importancia para el desarrollo sostenible de un territorio.

HTML. Es el pilar sobre el que se construyó la WWW. Es un lenguaje sencillo basado en marcas, que permite la creación de hipervínculos, facilitando la lectura no lineal y la búsqueda de información. Su sencillez y la gran cantidad de herramientas que facilitan su uso son unas de las razones que explican el rápido crecimiento de Internet y la generalización de su uso.

HACKER. El Hacker es una persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos

cifrados y las posibilidades de acceder a cualquier tipo de "información segura".

Su formación y las habilidades que poseen les dan una experticia mayor que les permite acceder a sistemas de información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

HARDWARE (LENGUAJE DE MARCAS DE HIPERTEXTO). Es un término genérico para todos los componentes físicos (que se pueden tocar) de la computadora, tales como discos, unidades de disco, monitor, teclado, ratón (mouse), impresora, placas, chips y demás periféricos. Se incluyen además aquellos componentes físicos que nos vemos, tales como dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, entre otros.

HTTP (HyperText Transfer Protocol). El Protocolo de Transmisión de Hipertexto es el estándar para el acceso a páginas publicadas en Internet.

INFORMACIÓN. Es un conjunto organizado de datos procesados que constituyen un mensaje sobre determinado tema. Puede existir en diferentes formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiera o los medios a través de los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

INFRAESTRUCTURA DE DATOS ESPACIALES (IDE). Es el conjunto "tecnologías, políticas, estándares y recursos humanos para adquirir, procesar, almacenar, distribuir y mejorar la utilización de la información geográfica". Al igual como las carreteras y autopistas facilitan el transporte vehicular, las IDE facilitan el transporte de información geoespacial. Las IDE promueven el desarrollo social, económico y ambiental del territorio.

INTERNET. Es un sistema mundial de redes de computadoras, integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos

apropiados, obtener información, efectuar transacciones, comunicarse y participar en toda gama de procesos públicos y privados puesto en dicha red.

INTRANET. Red de una organización que utiliza tecnologías y protocolos de Internet, pero que sólo está disponible para determinadas personas, por ejemplo para los empleados de una compañía. Una Intranet también recibe el nombre de red privada.

KERBEROS. Es un tipo de protocolo de autenticación - (authentication protocol). Un protocolo de autentificación (o autenticación) es un tipo de protocolo criptográfico que tiene el propósito de autentificar entidades que desean comunicarse de forma segura.

Los protocolos de autenticación se negocian inmediatamente después de determinar la calidad del vínculo y antes de negociar el nivel de red.

LOGIN. El login es el momento de autentificación al ingresar a un servicio o sistema.

MATERIAL NO PERMITIDO. Es la información que viola la normatividad. Encierra la transmisión, distribución o almacenamiento. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales.

MODELO ESTÁNDAR DE CONTROL INTERNO (MECI) para el Estado Colombiano 1000:2005. Proporciona la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación del proceso administrativo, y aunque promueve una estructura uniforme, se adapta a las necesidades específicas de cada entidad, a sus objetivos, estructura, tamaño, procesos y servicios que suministran.

MENSAJES DE DATOS. Es la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser entre otros, el intercambio electrónico de datos -EDI-, el correo electrónico, el telegrama, el télex o el telefax.

MODELO OPERATIVO POR PROCESOS. Metodología que permite gestionar la entidad como un todo, definir las actividades que generan valor, trabajar en equipo e identificar los recursos necesarios para su realización, orientando a la Administración Municipal hacia una organización por procesos, los cuales en su interacción, interdependencia y relación causa-efecto garantizan una ejecución eficiente, y el cumplimiento de sus objetivos.

MOTOR DE BÚSQUEDA. Es toda herramienta que sirve para buscar información. En Internet hace referencia a aquellos sitios que tienen herramientas que facilitan la búsqueda de información por la Red al recibir solicitudes y arrojar los respectivos resultados que se encuentren dentro de ésta. Algunos ejemplos con Google, Yahoo y Lycos, entre otros.

MULTIMEDIA. Sistema que utiliza de manera simultánea más de un medio de comunicación (texto, audio, video) en la presentación de la información.

NAVEGADOR O BROWSER. Es un programa que, a través de la web, permite visualizar hipertextos de datos o imágenes que estén en alguna computadora o en dispositivos conectados a la misma. La función primordial es la de poder acceder a páginas que se encuentran como hipervínculo en algún archivo. A esta acción de traslado de ubicación entre portales o sitios web se le denomina Navegación. En el mercado se ofrecen sin número de navegadores, pero los más utilizados son Internet Explorer, Mozilla Fireox y Netscape Navigator.

NO REPUDIO. Este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

PÁGINA WEB. Una página de Internet o página web es un documento electrónico que contiene información específica de un tema en particular y que es almacenado en algún sistema de cómputo que se encuentre conectado a la red mundial de información denominada Internet, de tal forma que este documento pueda ser consultado por cualesquier persona que se conecte a esta red mundial de comunicaciones y que cuente con los permisos apropiados para hacerlo. Es la unidad básica del World Wide Web.

PARTE INTERESADA. Organización, persona o grupo que tenga un interés en el desempeño de una entidad. Ejemplo: Beneficiarios, servidores públicos y/o particulares que ejercen funciones públicas de una entidad, proveedores, sindicatos, entidades de control, veedurías ciudadanas o la sociedad en general.

PASSWORD. En informática, la palabra password significa contraseña, clave, key o llave.

PERSONAL AUTORIZADO. Son todas las personas que están autorizadas a utilizar los servicios ofrecidos por la red. Deben estar autorizados a hacer uso de estos servicios todos los servidor público y /o personal de la Alcaldía (de planta, ocasionales y externos autorizados).

PLATAFORMA TECNOLOGICA. Conjunto de elementos de hardware y software que sirven de base para el desarrollo y funcionamiento de los sistemas de información.

POLÍTICA. Declaración general de principios que presenta la posición de la Administración Central Municipal para un proceso definido. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir un número pequeño), deben ser apoyadas y aprobadas por la alta dirección, y deben ofrecer direccionamientos a toda la entidad o todos los procesos involucrados. Por definición las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

POLÍTICAS DE SEGURIDAD INFORMÁTICA. Una política de seguridad informática es una forma de comunicarse con el usuario (a)s, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

PORTAL. Es un nuevo término generalmente sinónimo de puerta o "punto de entrada" para un sitio de la World Wide Web, que es o pretende ser un importante punto de partida para los usuario(a)s cuando se conectan a la Red, o que los usuario(a)s tienden a visitar como un sitio fijo en su

navegación. Es el punto de partida para encontrar información, trámites o comunicaciones sobre un rango de temas o sobre un ramo.

PROCEDIMIENTO. Forma establecida para llevar a cabo una actividad o un proceso, en la cual se debe definir quién hace qué, dónde, cuándo, por qué y cómo.

PROCESO. Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados. Los elementos de entrada para un proceso son generalmente salidos de otros procesos. Los procesos de una entidad son, generalmente, planificados y puestos en práctica bajo condiciones controladas, para generar valor. Un proceso en el cual la conformidad del producto o servicio resultante no pueda ser fácil o económicamente verificada, se denomina habitualmente "proceso especial".

PRODUCTO. Resultado de un proceso o un conjunto de procesos.

PROVEEDOR. Organización o persona que proporciona un producto y/o servicio. Un proveedor puede ser interno o externo a la entidad y en una situación contractual, un proveedor puede denominarse (contratista).

PROXI. Tipo de servidor que lleva a cabo algunas funciones como representante de otros clientes (computadoras) en la red para incrementar el rendimiento de ciertas operaciones (por ejemplo, servir como caché de documentos y otros datos) o para servir como barrera de seguridad (por ejemplo, navegación anónima, o filtrado de los datos de entrada peligrosos). Los servidores proxy no permiten un tráfico directo entre las partes.

PUBLICAR. Hacer que un documento sea visible desde el Sitio web Institucional.

RECURSO INFORMÁTICO. Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

RED DE LA ALCALDIA. La red de la Alcaldía es el conjunto de instalaciones, infraestructura de telecomunicaciones y recursos informáticos, principalmente los provistos por el centro de cómputo además, de los de todas las

dependencias; que proveen todos los servicio a los usuarios de la red. En ocasiones mencionada como red de comunicaciones o simplemente red.

REDES. Incluye varios sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.

ROL. Es un conjunto de permisos que puede asignarse a un usuario que se registra en un administrador de sistemas. Normalmente, los roles se definen de modo que incluyan permisos que guarden cierta relación y suelen corresponderse con algún rol de la vida real.

SERVICIOS. Son las ayudas en línea que La Administración Central del Municipio de Santiago de Cali provee actualmente o que piensa proveer en el futuro a los usuario(a)s, por medio de esta página web, como Publicación de noticias o actividades propias de la gestión institucional; trámites en línea; consultas; foros y buzón de quejas y reclamos, entre otros.

SEGURIDAD INFORMÁTICA. La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

SISTEMA DE CONTROL INTERNO. Se entiende por control interno el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas y objetivos previstos.

SISTEMA DE DESARROLLO ADMINISTRATIVO. Es el conjunto de políticas, estrategias, metodologías, técnicas y mecanismos de carácter administrativo y organizacional para la gestión y manejo de los recursos humanos, técnicos, materiales, físicos y financieros de las entidades de la Administración Pública, orientado a fortalecer la capacidad administrativa y el desempeño institucional.

SISTEMA DE GESTIÓN DE LA CALIDAD. Herramienta de gestión sistemática y transparente que permite dirigir y evaluar el desempeño de la Administración Central Municipal, en términos de calidad y satisfacción social en la prestación de los servicios. Está enmarcado en los planes estratégicos y de desarrollo.

SISTEMA. Tradicionalmente un Sistema es entendido como la interrelación mutua que se establece entre los elementos que componen un todo y que conducen al logro de objetivos.

SISTEMAS DE GESTIÓN. Es el conjunto de actividades que, interrelacionadas y a través de acciones específicas, permiten definir e implementar los lineamientos generales y de operación de las entidades públicas. Para efectos de la Presente Norma Fundamental, se entenderá como Sistemas de Gestión los tres (3) Sistemas de la Administración Central Municipal que son: Sistema de Gestión de la Calidad, Sistema de Control Interno y Sistema de Desarrollo Administrativo.

SISTEMAS DE INFORMACIÓN. Están conformados por el conjunto de herramientas o instrumentos tecnológicos tales como bases de datos, aplicativos, entre otros que facilitan la captura, procesamiento, administración y distribución de datos e información, estos deben tener procedimientos diseñados, mecanismos de control implementados y deben estar a cargo de los responsables de los procesos, para garantizar el desarrollo de la gestión para el manejo de aspectos tales como inventarios, nómina, archivo, recursos físicos, procesos de contratación, entre otros. En otras palabras, por sistemas de información se entiende el conjunto de tecnologías informáticas construidas, los procedimientos diseñados y los mecanismos de control implementados y la asignación de personas responsables por la captura procesamiento, administración y distribución de datos e información.

SISTEMAS DE INFORMACIÓN GEOGRÁFICA (SIG). Es una integración organizada de hardware, software y datos geográficos diseñada para capturar, almacenar, manipular, analizar y desplegar en todas sus formas la información geográficamente referenciada con el fin de resolver problemas complejos de planificación y gestión.

SISTEMAS DE POSICIONAMIENTO GLOBAL (GPS). Es un sistema global de navegación por satélite (GNSS) que permite determinar en todo el mundo

la posición de un objeto, una persona, un vehículo o una nave, con una precisión hasta de centímetros. Aunque su invención se atribuye a los gobiernos francés y belga, el sistema fue desarrollado, instalado y actualmente operado por el Departamento de Defensa de los Estados Unidos. En la actualidad la Unión Europea trabaja en su propio sistema denominado GALILEO, y por otro lado Rusia tiene en funcionamiento el sistema llamado GLONASS.

SITIO WEB. Es un conjunto de archivos electrónicos y páginas Web referentes a un tema en particular, que incluye una página inicial de bienvenida, generalmente denominada Home page, con un nombre de dominio y dirección en Internet específicos. Estas direcciones son denominadas URL (por sus siglas en inglés Uniform Resource Locator) y obedecen a un sistema mundial de nomenclatura regido por el ICANN (Internet Corporation for Assigned Names and Numbers).

SOFTWARE. También conocido como programática o equipamiento lógico es el programa o conjunto de programas y aplicaciones que permiten la realización de las tareas de computación a las que se destina. Se trata del conjunto de instrucciones que permite la utilización del computador y puede cumplir diferentes funciones: • Administrar los recursos de cómputo. • Proporcionar las herramientas para optimizar estos recursos. • Actuar como intermediario entre el usuario y la información almacenada.

SPOOFING. En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Existen diferentes tipos dependiendo de la tecnología a la que nos refiramos, los cuales se describirán más adelante, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN (TIC). Conforman el conjunto de recursos necesarios para manipular la información y particularmente los ordenadores, programas informáticos y redes necesarias para convertirla, almacenarla, administrarla, transmitirla y

encontrarla. Se puede reagrupar según: Las redes, los terminales y los servicios.

USO INDEBIDO. Actividad o comportamiento conocida como mala o inapropiada.

USUARIO EXTERNO. Se refiere a los usuarios de la prestación del servicio o usuarios receptores del producto de la entidad. Pueden ser ciudadanos, entidades comunitarias, otras entidades del Estado o entidades privadas.

USUARIOS INTERNOS. Todas aquellas personas naturales que tienen algún tipo de vinculación contractual con la Administración Central del Municipio de Santiago de Cali.

VÍNCULO - LINK. Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor web a otro, cuando se navega por Internet.

VIRUS INFORMÁTICO. El virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diferentes medios extraíbles o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados.

WORLD WIDE WEB. Se refiere a la red de recursos accesibles en el Internet, usando el protocolo de transferencia de recursos Hypertext Transfer Protocolo (HTTP).

5. POLÍTICA DE SEGURIDAD INFORMÁTICA

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las entidades públicas y empresas privadas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan ha llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de las entidades públicas y empresas privadas.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a las entidades públicas y empresas privadas crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Una política de seguridad informática es una forma de comunicarse con el usuario (a)s, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización. No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los servidores públicos, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

5.1 PRINCIPIOS FUNDAMENTALES DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- **INTEGRIDAD.** Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema

informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información

- **CONFIDENCIALIDAD.** Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

- **DISPONIBILIDAD.** Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran. Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

- **NO REPUDIO.** Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. El servicio de Seguridad de No repudio o irrenunciabilidad está estandarizado en la ISO-7498-2.

    - No Repudio de origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros.

En éste caso la prueba la crea el propio emisor y la recibe el destinatario.

- No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

- **AUTENTICACIÓN.** La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

5.1.1 Qué se debe Proteger? Si no hubiese nada que proteger, la seguridad no tendría sentido; por tal motivo es muy relevante detallar de forma exhaustiva todo lo que necesita ser protegido. Todo lo que se debe proteger dentro de la entidad, implementando la Política de Seguridad Informática se describe a continuación:

- Datos: La información puede ser robada, destruida o modificada; lo que podría alterar el funcionamiento interno de la Alcaldía.

- Programas: Al igual que los datos, los programas deben ser protegidos, entre otras cosas porque son una forma de acceso a los datos.

- Hardware: Es muy importante proteger a los activos de la entidad, debido a sus altos costos y a que estos son los que contienen la información y permiten su intercambio.

- Imagen: No hay nada que produzca más desconfianza, que una entidad pública o privada que ha sido atacada o que ha sido usada como soporte para un ataque a una tercera persona. Por tanto, es importante que una entidad pública o privada mantenga una buena seguridad.

5.1.2 De Quien se debe Proteger? Se debe proteger de los intrusos que aprovechan las vulnerabilidades que hay en la red de la entidad para realizar diferentes ataques. Estos ataques pueden clasificarse en tres tipos:

- Desmantelamiento de sistemas: Suelen ser ataques de Denial of Service (Negación de Servicios). Estos ataques tienen como fin colapsar una o más máquinas.

- Robo de datos: La manera más normal de atacar para robar datos es conseguir una combinación de login/password de algún usuario.

- Intrusión: Estos ataques consiguen que el hacker tenga acceso remoto a otra máquina, y por tanto puede usar los recursos de esta. Normalmente se utilizan estas maquinas para lanzar ataques contra otras de una forma “camuflada”, y sin un riesgo claro para el atacante; una manera de hacerlo es cuando el atacante hace spoofing (direcciones suplantando la dirección de origen por otra totalmente diferente).

La única forma eficaz de protegerse de ellos es conseguir que sea tan difícil atacar el Sistema de Información que no les merezca la pena emplear tanto tiempo. Por esta razón es que se debe tener bien protegido el Sistema de Información en el ámbito físico y lógico; teniendo un buen sistema de informes, principalmente para que un ataque no pueda pasar desapercibido y para que se pueda rastrear al atacante. Este sistema debe ser exhaustivo, de tal forma que recoja la información de todo lo que pase en el sistema, y además debe ser difícil de modificar, para que no se pueda manipular fácilmente.

5.1.3 Cómo se debe Proteger? No existe una forma genérica para proteger los Sistemas de Información de cualquier ataque. Hay muchos factores a tener en cuenta, desde la importancia de los datos a proteger, hasta el presupuesto disponible para seguridad.

Como ya se mencionó anteriormente, es importante plantear la importancia de lo que se va a proteger, para hacerse una idea de los esfuerzos que están dispuestos a hacer los hackers para conseguir atacar los Sistemas de Información.

Es aconsejable tener un tipo “especial” de segmento, conocido como DMZ (De-Militarizad Zone), donde se suelen colocar los equipos de “riesgo”, como los servidores donde se encuentran los servicios que deben ser accesibles desde la zona Internet (servidores de www, correo, IRC...) o de sedes remotas. La razón por la cual es aconsejable esta zona es porque es una zona donde hay que permitir conexiones con el exterior (acceso externo), y no es recomendable que conviva con otros equipos que no necesitan tantos riesgos. Esta es la configuración más típica, con un firewall al que se conecta la subred segura, el DMZ e Internet (o el acceso externo), y se crean distintas políticas para cada acceso (Internet-Interno, DMZ-Interno, Interno-Externo...).

Además se puede añadir un servidor Proxy (de Web, de Telnet, de FTP...) para ofrecer distintos servicios con un nivel de seguridad mayor, ya que un Proxy analiza el tráfico de forma más detallista que un filtro, que sólo analiza tráfico como mucho a nivel de direcciones, puertos y protocolo de nivel 4.

Además, es necesario conocer los riesgos asociados a cada servicio que se permitan en los Sistemas de Información, para así añadir la seguridad que sea necesaria, bien en el propio firewall, o bien en los equipos finales. Puede ser necesario añadir un sistema de detección de intrusos para que monitorice el tráfico en busca de patrones conocidos de ataque, dependiendo de los servicios que se permitan.

Otro de los factores a tener en cuenta es que varios de los ataques comienzan desde dentro de los Sistemas de Información, bien por malicia de un usuario o por desconocimiento del mismo. Por eso es muy importante concienciar a todo el mundo de las cosas que se pueden y se deben hacer, y de cuales no (no ejecutar archivos descargados de páginas de poca confianza, vigilar los attachments de los e-mails, etc.), aquí radica la importancia del establecimiento de políticas de seguridad para los usuarios (usuarios con distintos privilegios en función de su cargo y de sus conocimientos en informática). Por tanto, también es importante añadir seguridad en los equipos finales, principalmente en los servidores, de los que depende gran parte del funcionamiento de los Sistemas de Información.

5.2 POLITICA DE ADMINISTRACION DE LA SEGURIDAD INFORMÁTICA

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las

mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en los Sistemas de Información conformados por el Portal Municipal, la Intranet ó los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el servidor público que la detecta, en forma inmediata y confidencial al Asesor de Informática y Telemática.

Los servidores públicos que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por la Asesoría de Informática y Telemática.

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, usb memory key, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

El Asesor de Informática y Telemática divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará al Alcalde o quien el ejecutivo delegue, los casos de incumplimiento con copia a la Dirección de Control Interno y Dirección de Control Interno Disciplinario.

5.3 RIESGOS DE LA RED EN LOS SISTEMAS DE INFORMACIÓN

Como ya se mencionó anteriormente uno de los principales problemas de inseguridad que se presentan es la interactividad e intercambio de información entre usuarios, donde se pueden presentar muchos huecos, si estos no están conscientes de la importancia de proteger sus equipos y su información.

Otro gran problema es el estar conectados a una red pública como Internet, que como ya se dijo anteriormente, esta no tiene en su estructura ningún mecanismo de seguridad, por lo tanto los servicios ofrecidos por esta tienen un alto grado de vulnerabilidad. Agregando las conexiones con sedes

remotas.

Adicionalmente se encuentran los problemas asociados con los servicios, debido a que estos presentan riesgos que ponen en peligro la seguridad de la red. A continuación se hace una breve descripción de los servicios más utilizados en la red de la Alcaldía y de sus posibles problemas, riesgos o debilidades que pueden presentar.

- Mail. Este es posiblemente uno de los servicios más utilizados en la red. El principal riesgo del correo radica en la difusión de gusanos que se difunden automáticamente utilizando la agenda de direcciones del usuario infectado.

A nivel de protocolos existen tres (3) distintos, POP, IMAP, para correo entrante del usuario y SMTP que se utiliza par el correo saliente.

  - POP: El más utilizado es el POP3, que corre en el puerto 110. Bajo este protocolo los login/password van en claro, lo cual es considerado una gran inseguridad para la integridad del correo. Además es común que los usuarios utilicen el mismo login/password para el correo que para el acceso al sistema, comprometiendo así la seguridad de la red. Por eso no se debe permitir acceso al servidor POP desde el exterior de la red. Para conexiones remotas, es recomendable adoptar una solución remota vía SSL (Secure Socket Layer) para garantizar la confidencialidad e integridad de la información que viaja por el correo.

  - IMAP: Muy similar a POP3, pero más seguro. Sin embargo es aconsejable tener presente las mismas consideraciones que el anterior en lo referente a los login/password de los usuarios y las conexiones remotas.

  - SMTP: Es el protocolo que transporta el mensaje. Sufre de problemas como el Mail basura y ataques de Denial of Service a través de las listas de distribución de correo (ataques como el mail bombing pueden colapsar a un usuario o incluso un servidor). En general no se debe permitir que el servidor SMTP envíe mensajes que no procedan de la subred, a no ser que el

servidor implemente sistemas de seguridad propios para evitar estos problemas (como limitar el tamaño máximo de mensajes, ser capaz de detectar bucles de mandado de mails).

- FTP. Como ya se conoce este servicio se utiliza para realizar transferencia de archivos, lo que puede ser un problema, en el caso de que se transmitan archivos maliciosos sin el conocimiento del usuario. Además, en el caso de tener un servidor de FTP, se debe restringir el acceso para que solo se pueda acceder a las áreas "publicas" y no se pueda entrar en las áreas de sistema.

Otro problema típico es el warezhousing, en el que se convierte un servidor de FTP "legal" en un depósito de piratería y material ilegal. Por eso hay que concienciar a todos los usuarios de la red tener cuidado y no aceptar los archivos que provengan de un usuario anónimo.

Adicionalmente, hay que tener presente que los datos del FTP van "en claro" (sin encriptar) y por tanto, en el caso de tener un servidor (o una parte de el) no-anónimo (con acceso restringido para usuario autorizados), no se debe permitir que tengan los mismos login/password que utilicen para otros servicios o para el acceso a la Red protegida.

A través de ataques FTP se pueden suplantar archivos normales (como el NotePad) por programas maliciosos (Troyanos y Back Orifice) de forma inadvertida para el usuario, de ahí la importancia de un sistema de detección de intrusos (IDS), puesto que un usuario que se conecte con un servidor de FTP malicioso podrá ser atacado sin que ningún Firewall de Filtrado lo detecte (existen Proxies con funcionalidades de IDS integradas).

Existen dos (2) modos de operación en el FTP, el activo y el pasivo, y tienen modos de funcionamiento muy distintos:

- Activo: Se usa el puerto de TCP número veintiuno (21) para los comandos, y el TCP veinte (20) para los datos (en el servidor). En el cliente se selecciona un puerto temporal (1024-65535) para los datos y se le comunica al servidor, el cual inicia una conexión en ese puerto.

Esto es bueno para un servidor tras un firewall, ya que sólo necesita habilitar

el puerto veinte (20) y veintiuno (21), mientras que es bastante malo para un cliente tras un firewall, porque hay que permitir que “cualquiera” inicie conexiones TCP en los puertos temporales.

Además, si el Firewall hace masquerading (oculta todas las direcciones IP internas con la suya propia) este modo no funciona, porque el firewall no es capaz de determinar qué cliente es el que ha hecho la petición FTP, puesto que el servidor inicia una conexión con la IP del Firewall en un puerto temporal que le ha comunicado el cliente (y el firewall no sabe cual es).

Existe una tecnología llamada “Adaptative Firewalling” que consigue resolver el problema del masquerading con el FTP activo, pero que no resuelve el hecho de tener que permitir cualquier conexión en el rango temporal.

  - Pasivo: El puerto TCP veintiuno (21) es el encargado de los comandos, y no se usa el puerto TCP veinte (20), el servidor escoge un puerto del rango temporal y se lo comunica al cliente. Posteriormente el cliente abre una conexión a ese puerto en el servidor, por lo que es fácil dar soporte a clientes tras el firewall ya que es el que inicia ambas conexiones, mientras que si se tiene un servidor tenemos el mismo problema que antes con el cliente y se deben abrir los puertos del 1024 a 65535.

- Telnef. Este servicio permite el control remoto de un equipo, en modo consola a través del puerto TCP veintitrés (23). Es un servicio inseguro porque no utiliza encriptación, e incluso los login/password van en claro, por lo que la información no viaja protegida desamparando la seguridad de la misma. Se debe permitir, como mucho hacia fuera (sentido Intranet - Internet), siempre teniendo en cuenta que no se deben usar los mismos login/password que se usan en la Intranet. Se puede usar Telnet junto con Kerberos, que le aporta la seguridad.

En su lugar de telnet es mejor utilizar Ssh (conocido como Telnet Seguro). Ssh corre en el puerto de TCP veintidós (22), y utiliza encriptación para transmitir la información, lo que le confiere un grado de seguridad bastante alto. De hecho, los ataques contra Ssh se basan en ataques criptográficos para romper la codificación y convertirlo en un Telnet “normal”.

Ssh es muy seguro para conexiones máquina-máquina y máquina-red, pero puede no ser suficientemente seguro para conexiones red-red, por lo que se recomienda en este último supuesto el uso de VPN (Redes Privadas Virtuales) que proporcionan un mecanismo de seguridad mucho mayor.

- HTTP. Normalmente corre en el por el puerto ochenta (80), aunque pueden encontrarse servidores que utilicen otros puertos como por ejemplo, el puerto 8080. Este servicio es el más usado en Internet, y paradójicamente es el que más problemas da. Este servicio no provee por si mismo ningún tipo de autenticación ni de encriptación, por lo que de por si, es una fuente potencial de problemas. Adicionalmente, el protocolo HTTP permite, además de transmitir información, la transmisión y ejecución de programas a través del navegador de Internet.

Existe una forma de ofrecer un servicio seguro de HTTP, mediante la utilización de SSL (Secure Socket Layer). Este protocolo permite la autenticación de cliente, servidor o de ambos, por medio de una autoridad de certificados (30 de confianza). Además, permite una comunicación segura a través del firmado (MAC usando MD5 o SHA-1) y encriptación de los datos (DES, Triple DES, RC4, RC2 e IDEA).

El principal problema de habilitar HTTP (sin SSL) a través del firewall, es que si un usuario teóricamente protegido visita una página con código “malicioso”, el firewall no será capaz de defenderse, puesto que ha sido el usuario el que ha conectado voluntariamente con el hacker. La única forma de parar ese tipo de ataques es mediante un IDS (Intrusion Detection System) integrado en el Firewall (ya sea de filtrado o de Proxy, aunque es común que los Proxy lo tengan), que analizan el tráfico en busca de patrones de ataque conocidos. Este sistema puede detener la mayoría de ataques, pero no es capaz de detener los ataques “a medida”, aquellos hechos por los profesionales.

Este no es el único problema. Existen numerosas grietas e inseguridades en la implementación de JavaScript, Java y ActiveX para navegadores, que pueden ser aprovechadas para iniciar un ataque contra una máquina, aunque continuamente salen plug-ins para disminuir estos defectos. Entre los problemas más conocidos se encuentran:

- Frame Spoofing: La URL parece correcta, pero en realidad la conexión se realiza a otro sitio, que además puede tener la misma apariencia que la pagina deseada.

- Buffer OverFlow: Este ataque se basa en el hecho de que el Buffer del Navegador esta justo encima del de instrucciones, por lo que si se ve sobrepasado, se escribe en este, y se ejecutan instrucciones.

- Back Orifice: Posiblemente el ataque más común de todos, permite un control remoto de la máquina. Se transmite vía HTTP, y solo se puede detectar con un IDS. Es más peligroso en máquinas Windows o Machintosh porque no detectan procesos en BackGround.

Para evitar la mayoría de debilidades, es muy importante tener un navegador seguro, por lo que es recomendable el uso de Mozilla antes que Explorer o Netscape. También se recomienda evitar el uso de agentes de correo integrados con el navegador puesto que suelen ser más vulnerables que los programas específicos de correo. También es recomendable es uso de SSL.

- DNS. Es un servicio fundamental para el funcionamiento de la red, y por tanto debe ser permitido a través del firewall de una manera o de otra, bien para que los usuarios hagan peticiones DNS o para que el servidor interno haga peticiones a su DNS superior. Por esta razón es necesario que se controle mucho las peticiones DNS, y que sólo se permitan las justas y necesarias), para evitar “fugas” de información. Además, el servicio sufre de debilidades propias como ataques de Buffer Overflow (para atacar a un servidor poco protegido) y Denial of Service. Otro de los ataques conocidos contra DNS, y posiblemente el más peligroso consiste en hacer una falsa respuesta a una petición DNS (capturando el paquete de petición y creando uno a medida), de tal forma que el usuario inicia una conexión con una IP que no es la que el quería.

Entre las soluciones, se encuentra la de utilizar direcciones IP estáticas y evitar en la medida de lo posible las peticiones DNS.

- Ofros Servicios. En el momento de habilitar un servicio, es de gran

importancia conocer cómo funciona, y si es seguro o no. Por lo que es conveniente testear la seguridad de un programa antes de permitir que se instale en la red y comprometa la seguridad de esta. Por otro lado, el servicio debe abrir un único puerto, para minimizar el riesgo, y en caso de que pueda abrir gran cantidad de ellos, se debe fijar estáticamente a un único puerto.

- Afaques a IP. Los ataques basados en IP utilizan las direcciones y la fragmentación/reensamblado como arma ofensiva. Las prácticas más comunes consisten en el “Spoofing”, el “Strict and Loose Service Routing” y los ataques de “TearDrop”.

    - Spoofing: Se basa en direcciones suplantando la dirección de origen por otra totalmente diferente y así, aparentar ser quien no es.

    - Strict Routing: Al igual que el Spoofing, se basa en las direcciones. Consigue forzar el encaminamiento a través de un determinado camino, para conseguir distintos efectos, desde que el trafico viaje por la vía mas insegura, hasta que el trafico pase por algún equipo bajo control del hacker, lo que le permitirá extraer trafico de la red.

    - TearDrop: Los ataques de este tipo se basan en el mecanismo de reensamblado/solapamiento de fragmentos.

- Ataques a TCP. Entre los ataques mas conocidos de TCP están el “Land Attack”, el “HiJacking” y los “Denial of Service” basados en Checksums.

    - Land Attack: Crea un paquete con la dirección de origen y destino iguales a la de la máquina a ataque. Esto crea un bucle infinito en la conexión, que acaba por colapsar la máquina

    - HiJacking: Es el secuestro de una conexión, filtrándola comunicación entre dos (2) usuarios a través del atacante. Esto se consigue a través del HandShake, procedimiento que se usa al iniciar una conexión TCP para negociar parámetros y establecer una conexión.

- Denial of Service: Consiste en bombardear a la victima con paquetes TCP con un Checksum incorrecto, hasta que se colapse. Se puede detener con un IDS capaz de detectar esta situación anómala.

- Ataques a UDP. Los ataques UDP más comunes son el TearDrop y el ataque de fraggle, una variante del tipo Denial of Service.

- Ataques a ARP. El principal problema del ARP (Address Resolution Protocol) es que no tiene estado, por lo que si se recibe un Reply, no se sabe si hubo un request, lo cual se puede utilizar para fines maliciosos.

- Afaques a IGMP (Infernef Group Managemenf Profocol). Se usa para crear Grupos Multicast, donde una serie de máquinas están adscritas a una dirección Multicast, de forma que se pueden comunicar entre si de una forma más eficiente. Se puede usar de forma maliciosa, para convertir Multicast en Broadcast (añadiendo toda la subred al grupo), y así poder hacer ataques de Denial of Service de forma más eficiente.

También se suelen utilizar ataques de Buffer Overflow (sobrepasar el buffer de la aplicación y escribir en el área de instrucciones, para así conseguir ejecutar programas de forma inadvertida) en sesiones Multicast (ataque múltiple).

Como recomendación, lo mejor es desactivarlo a menos que sea imprescindible para la red, en cuyo caso será necesario añadir seguridad a nivel Multicast, principalmente para evitar la modificación no autorizada de los grupos.

- Afaques a ICMP (Infernef Confrol Message Profocol). Este protocolo se usa, como su nombre indica, para tareas de control y administración de la red. Entre las aplicaciones más conocidas están el ping (que se usa para probar la conectividad con otras maquinas) y el traceroute (que se usa para conocer la ruta que sigue el paquete para ir a un destino). Entre los ataques mas conocidos, están el “Ping of Death”, los Denial of Service y una variante del “cache poisoning”.

5.3.1 Equipos de Seguridad Informática Los equipos de seguridad juegan un papel muy importante en el manejo de la seguridad, pues de estos depende en gran medida en nivel de seguridad que se quiera lograr. Entre los equipos de seguridad más destacados se encuentran los siguientes:

5.3.1.1 Firewall Para el firewall existen dos (2) alternativas, este puede ser tipo software o tipo hardware; su principal diferencia radica en el costo y en el nivel de seguridad que este ofrece.

- Firewall Tipo Hardware. Los más costosos son los firewall de este tipo, pero recompensando esto, estos producen una conmutación más rápida que un equipo software, y además proporcionan un nivel de seguridad muy alto; brindando la opción de mejorarlo con nuevos y más modernos sistemas, gracias a las continuas actualizaciones On-Line.

- Firewall Tipo Software. Los firewalls de este tipo ofrecen un nivel de seguridad menor que los firewall tipo hardware, no son capaces de manejar enormes caudales de conexión (como los Hardware de gama alta); sin embargo son de un precio menor, pues solo se paga el software de seguridad y se instala en una máquina disponible. Adicionalmente este tipo de firewall requiere de un gran esfuerzo para su configuración.

5.3.1.2 Proxy Este juega un papel muy importante, debido a que es por este por donde entran y sale información bien sea, de clientes locales o internos o posibles clientes virtuales (como por ejemplo, instituciones financieras, clientes remotos, etc.); por ello en el proxy se debe tener configurado políticas bien definidas para garantizar la integridad y seguridad de la información, y así, proteger el servidor o servidores donde se encuentran alojados los datos a los cuales van a acceder los clientes.

Adicionalmente, es necesario monitorear la red y su funcionamiento para que no lleguen a los archivos protegidos. El proxy cumple la función de ser un servidor de consulta, por esta razón es aconsejable colocar una copia de los archivos para consulta, para que no sean afectados los archivos originales con que opera la Alcaldía.

5.3.1.3 Servidores Otro de los puntos críticos de una red son los servidores (Web, FTP, Correo, etc.), ya que es necesario permitir el acceso a ellos desde y hacia Internet. Además, si un Servidor es vulnerable, ningún Firewall será capaz de protegerlo, ya que el ataque tendrá una apariencia de ser una conexión normal, y pasaría impunemente por el filtro. Estos ataques van desde el simple Denial of Service, hasta el acceso privilegiado a la configuración/recursos del servidor.

Por esta razón, además del firewall, hay que destinar recursos a proteger los servidores, instalando programas seguros y estables (por ejemplo, personal firewall), que no ofrezcan facilidades a la hora de atacar y que permita el establecimientos de políticas de acceso más restringidas para ellos. Existen dos alternativas de aplicaciones, libres y propietarias. Las aplicaciones libres suelen ofrecer mejores resultados que las propietarias, ya que están en continua evaluación y corrigen las debilidades más rápidamente que las aplicaciones propietarias, por eso es recomendable su utilización.

Adicional a esto es recomendable el establecimiento de la DMZ (De-Militarized Zone) o red perimetral, donde se colocan los servidores con los servicios que requieren de mayor fiabilidad y que tienen acceso restringido, para garantizar que el servidor es accedido sólo para el servicio que ofrece, pues se tendrían unas políticas diferentes para ellos. Esto es debido a que los servidores son los que más riesgo corre y tienen necesidades distintas de las de los usuarios finales. De esta forma, se le agrega seguridad a los servidores y además, se separan físicamente los servidores de los usuarios; en el caso de perder el control de un servidor no se compromete la seguridad de los usuarios finales.

5.3.1.4 Aplicaciones de Usuario Otro punto a considerar a la hora de querer tener una red segura, son las aplicaciones de los usuarios; estas juegan un papel importante, debido a que hay algunas aplicaciones más sensibles que otras a determinados ataques que no puede detener un firewall, dependiendo del tipo de aplicación, principalmente las que no tienen el sistema de detección de intrusos y las que no bloquean dichos ataques; por esta razón las aplicaciones que se utilicen deben de ser lo más estable y seguras posibles.

Los navegadores Web son los más sensibles a los ataques de red, ya que el

protocolo HTTP permite transportar programas además de datos. Además, algunos navegadores (como Internet Explorer y Netscape) tienen un problema de Buffer Overflow, pudiendo ejecutar programas sin el conocimiento del usuario (Windows y Machintosh no detectan procesos en segundo plano). Se recomienda usar navegadores seguros, como Mozilla, e instalar el Java Plug-in, para disminuir muchos de los problemas que provoca el uso de JavaScript.

6. POLÍTICAS GENERALES DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Las políticas que se nombran a continuación servirán como observación, y en ningún momento pretenden formarse como normas absolutas. Todos los actos que se consideren como violaciones a las normatividades vigentes (Leyes de la República de Colombia, Normatividad interna de la Alcaldía de Santiago de Cali, y/o cualquier otra disposición debidamente establecida en el ámbito jurídico), y que no se mencionen expresamente en este documento, deberán ser prohibidos.

Todos los servidores públicos que hagan uso de los servicios que ofrecen los Sistemas de información de la Alcaldía deberán conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo no debe exonerar a la persona de las responsabilidades asignadas.

La Asesoría de Informática y Telemática, debe comprometerse a publicar y difundir las políticas, una vez estas sean aceptadas y aprobadas por el líder del proceso y adoptadas mediante acto administrativo; para garantizar el conocimiento de las mismas por parte de todos los usuarios de los Sistemas de información de la Alcaldía.

6.1 POLITICA DE SEGURIDAD FISICA

La Seguridad Física consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo;

implementados para proteger el hardware y medios de almacenamiento de datos. A continuación se establecen los lineamentos generales para su cumplimento

6.1.1 Acceso y Protección La Administración Central del Municipio de Santiago de Cali deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que se consideren críticas. El sistema de seguridad conservará un historial completo de todas las personas externas que ingresen a la Centro de Cómputo, para efectos de seguridad, control, estadísticas, registro, etc. A continuación se dictan los lineamientos establecidos para su implementación en la Administración Central Municipal:

- Los usuario(a)s visitantes de la oficina de la Asesoría de Informática y Telemática de la Administración Central del Municipio de Santiago de Cali, deben ser acompañados durante todo el tiempo por un servidor público de la misma. Esto significa que se requiere de un acompañante tan pronto como un usuario(a) visitante entra a esta área y hasta que este mismo usuario(a) visitante sale del área controlada. Todos los usuarios (a)s visitantes requieren un acompañante incluyendo clientes, antiguos empleados, miembros de la familia del servidor público.

- Siempre que un servidor público se dé cuenta que un usuario(a) visitante no acompañado se encuentra dentro de áreas restringidas de la oficina de la Asesoría de Informática y Telemática de la Administración Central del Municipio de Santiago de Cali, el usuario(a) visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

- Los particulares en general, entre ellos, los familiares de los servidores públicos, no están autorizados para utilizar los recursos informáticos de la Administración Central del Municipio de Santiago de Cali.

6.1.1.1 Sistemas de Circuito Cerrado de Televisión El principal objetivo del sistema de Circuito Cerrado de Televisión es el de servir como extensión

de los ojos del operador de turno y de esta forma ser el medio por excelencia para verificar y registrar en medio digital los acontecimientos rutinarios y de excepción. Mediante su sistema de detección de movimiento digital y aprovechando la capacidad IR (luz Infrarroja para visión nocturna) de algunas cámaras, deberá alertar al operador sobre cualquier acción en zonas restringidas.

Los criterios para el diseño del Sistema de de Circuito Cerrado de Televisión, deberá contemplar los siguientes requerimientos:

- Las cámaras fijas se dispondrán de tal forma que cumplan, como mínimo, con las siguientes funciones:
  - Vigilancia de todos los accesos a las áreas del Centro de Cómputo.
  - Vigilancia de pasillos de oficinas.
  - Vigilancia de áreas críticas, como ingresos a Oficina de Informática y Telemática.
  - Cubrimiento en los puntos fijos de ascensores y escaleras.
  - Vigilancia en la mayoría de salidas e ingresos con control de acceso.
  - Cubrimiento diurno y nocturno de todos los puntos anteriores.
- Para estos efectos, se ubican cámaras fijas interiores con capacidad para visión nocturna.
- Para el monitoreo y la grabación de todos los movimientos registrados por las cámaras, se instaló, en el Centro de Computo, equipos de grabación, control y monitoreo de las señales de las cámaras. Estos equipos son los siguientes:
  - Videograbadoras digitales: Las videograbadoras permitirán almacenar y reproducir las señales de cada una de las cámaras, de forma digital.

- Monitores LCD en número tal que permitan visualizar fácilmente la totalidad de las cámaras en forma secuencial y/o simultánea.

- Equipos para interactuar con los demás sistemas electrónicos en la medida de lo posible utilizando señales digitales dentro de un PC estándar.

- La imagen de las cámaras a través de cable trenzado multipar (UTP), en vez del tradicional coaxial. Con esto se evita al máximo las interferencias ocurridas en la señal de video. El cable UTP permite, igualmente, mayores distancias entre las cámaras y los equipos de control y una mayor flexibilidad de la red de CCTV, al facilitar la instalación futura de nuevas cámaras sin tener que cablear directamente desde el Cuarto de Control, ya que se podrán utilizar los pares libres de los cables UTP existentes en todo el complejo para transmitir las nuevas señales de video. De igual forma, el cable UTP permitirá migrar fácilmente, en un futuro, y si así lo requiere la Centro de Cómputo, a tecnología IP.

6.1.1.2 Sistema Contra Intrusión El objetivo principal del Sistema de Intrusión es el de detectar con la suficiente anticipación una posible violación del perímetro o zona interior restringida y asegurada, y alertar a los operadores de turno del cuarto de control. Las señales de alarma se enrutan a una unidad de control que analiza los estados y toma la decisión de entrar en estado de alarma o no. El sistema debe interactuar con el computador central de control, y avisar en la pantalla a través de una señal gráfica y audible el sitio exacto del evento de excepción. Este sistema puede ser parte del sistema de control de accesos.

6.1.1.2.1 Sistema de Control de Acceso y Sistema de Detección de Intrusión Los distintos dispositivos que envían o reciben información de los Controladores Locales y Expansores en los Cuartos de Interconexión de Acceso (Lectoras de Proximidad, Lectoras de Activos, Barras Antipánico, Sensores Infrarrojos PIR, Pulsadores de Emergencia, Contactos Magnéticos, entre otros), lo hacen a través de cable UTP de 4 Pares. Cada dispositivo se cablea de forma independiente a dichos Controladores, para de esta forma conocer exactamente el lugar donde ocurra un evento. Los Electroimanes

reciben la señal de alimentación de los Controladores Locales de Acceso a través de cable Dúplex 18AWG.

6.1.1.2.2 Alarmas Contra Intrusión Para la mayoría de las puertas de las áreas de Centro de Cómputo se utiliza contactos magnéticos para detectar el estado de las mismas y enviar la correspondiente señal de alarma. Por lo tanto, estos contactos serán ubicados, ante todo, en las puertas con control de acceso, en los cuartos técnicos, en las puertas de ingreso principal, en las puertas de las oficinas, en las puertas de ingreso de un área principal a otra, en las puertas que dan hacia las salidas de evacuación y las escaleras de emergencia, etc.

De igual forma, se instalaron sensores infrarrojos de movimiento de personas (PIR) en los puntos susceptibles de intrusión desde el exterior de las áreas del Centro de Computo y en los puntos donde se requiera alta seguridad, como son los cuartos técnicos y la oficina de sistemas y de administración de la Oficina de Informática y Telemática.

Todos los elementos de alarma contra intrusión (contactos magnéticos, sensores infrarrojos, pulsadores de emergencia) son manejados por expansores de entradas supervisadas que irán acoplados a los paneles del sistema de control de acceso, en los distintos cuartos de interconexión. Cada dispositivo de alarma será ubicado en una (1) zona del expansor, con el fin de conocer el sitio exacto donde se presentó la señal de alarma, y como las entradas del expansor son supervisadas cada elemento deberá contar con resistencia de fin de línea, para poder detectar intentos de sabotaje. Las señales de alarma serán recibidas por los operarios del Cuarto de Control, por medio de avisos visibles y sonoros del software principal en el PC de integración.

6.1.1.3 Paneles de Control de Acceso Se trata de equipos de procesamiento de datos locales que se encargarán de analizar la información capturada por las lectoras, los contactos magnéticos y las barras antipánico asignados a ellos con el propósito de autorizar, negar, enviar alguna señal de alarma o control para bloquear o liberar puertas, dispositivos electromecánicos controlables, etc. Trabajan bajo el principio de control distribuido, con lo cual se comunican con otros controladores para compartir información y pueden ser autónomos a la operación del PC de control.

6.1.1.4 Infraestructura para las Redes Electrónicas A partir del diseño de los sistemas descritos arriba, se especifico la ubicación de las bandejas, ductos, cableado y demás elementos pasivos. Para cada sistema, el cableado sería el siguiente:

6.1.1.4.1 Circuito Cerrado de Televisión En el presente proyecto se utilizo cable UTP (trenzado multipar) para transmitir la señal de video de las cámaras. En el Centro de Cómputo se hizo el ordenamiento y la interconexión de los cables UTP provenientes de las cámaras por medio de Patch Panels, Patch Cords y gabinetes.

Para llevar la alimentación a dichas cámaras se utilizará cable tríplex 18AWG.

6.1.1.4.2 Sistema de Control de Acceso y Sistema de Detección de Intrusión Los distintos dispositivos que envían o reciben información de los Controladores Locales y Expansores en los Cuartos de Interconexión de Acceso (Lectoras de Proximidad, Lectoras de Activos, Barras Antipánico, Sensores Infrarrojos PIR, Pulsadores de Emergencia, Contactos Magnéticos, entre otros), lo hacen a través de cable UTP de 4 Pares. Cada dispositivo se cablea de forma independiente a dichos Controladores, para de esta forma conocer exactamente el lugar donde ocurra un evento.

Los Electroimanes reciben la señal de alimentación de los Controladores Locales de Acceso a través de cable Dúplex 18AWG.

6.1.2 Equipos Se entenderá como equipos aquellos elementos tales como: los computadores portátiles, módems y equipos de comunicación y cómputo de propiedad de la Administración Central del Municipio de Santiago de Cali.

- El ingreso ó salida (del centro de cómputo así como de la oficina de la Asesoría de Informática y Telemática) de cualquier equipo deberá ser registrado en un formato, elaborado previamente para dicho fin.

- Se debe revisar y actualizar periódicamente (cada seis meses) los derechos de acceso a las áreas protegidas.

- Además de la puerta de salida del edifico, se debe establecer otro punto de chequeo para detectar el retiro no autorizado de equipos; del cual los trabajadores no estén al tanto.

- Antes de retirar cualquier equipo, se debe contar con la autorización de la dirección pertinente.

- Todos los computadores portátiles, módems y equipos de comunicación y cómputo de propiedad de la Administración Central del Municipio de Santiago de Cali, deben registrar su ingreso y salida y no deben abandonar el edificio a menos que esté acompañado por la autorización respectiva y la validación de supervisión del responsable de su administración.

- Los equipos de microcomputadores (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

- Los servidores públicos se comprometen a NO utilizar a la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que generen caídas de la energía.

- Al retirar un equipo, el encargado debe garantizar la seguridad del equipo de igual forma que si estuviera dentro de las instalaciones.

- En el formato de retiro de equipos debe estar el compromiso que debe adquirir la persona, que va a retirar el equipo.

- A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de video, audio u otro tipo de equipamiento que registre información.

- Los equipos de computo deben contener o incorporar identificadores electrónicos internos que permitan alertar de su ingreso y salida de las instalaciones de la Administración Central Municipal

6.1.3 Centro de Cómputo Los centros de cómputo o centro de proceso de datos, data center, son habitaciones en donde hay múltiples computadoras para un fin específico. Las computadoras en los centros de cómputos suelen estar conectadas entre sí a través de una red informática y entre otros centros de cómputos dentro de la organización.
Existen centros de cómputos que deben cumplir ciertos estándares con el fin de cumplir correctamente sus objetivos. Por ejemplo un objetivo puede ser que las computadoras deban estar encendidas las veinticuatro (24) horas del día y, por lo tanto, se les debe garantizar electricidad y refrigeración constantes. A continuación se establecen los siguientes lineamientos:

- Los centros de cómputo o áreas que la Administración Central del Municipio de Santiago de Cali considere criticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

- Todo usuario(a) interno que se encuentre dentro de la entidad deberá portar su identificación en lugar visible.

- En los centros de cómputo o áreas que la Administración Central del Municipio de Santiago de Cali considere criticas deberán existir elementos de control de incendio, inundación y alarmas.

- Los centros de computo o áreas que la Administración Central del Municipio de Santiago de Cali considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas

- Los relojes de los equipos de cómputo deben estar sincronizados, para garantizar que los registros realizados para cualquier eventualidad tengan ese nivel de coincidencia, al momento de realizar una auditoría.

- Procurar que todos los dispositivos de Inter conectividad (servidores, switches, enrutadores, etc.) de mayor importancia se encuentren dentro del centro de cómputo.

- Permitir el acceso al centro de cómputo sólo a personal autorizado, y contar con un registro de entradas y salidas de visitantes.

- Se prohíbe el consumo de bebidas y comida dentro del centro de cómputo.

- Se debe supervisar constantemente las condiciones ambientales para evitar que se vean afectados los equipos dentro del centro de cómputo.

- Proveer a los equipos de fuentes de energía permanentes (como UPS, alimentaciones múltiples, etc.).

- Se recomienda que los sistemas de agua y desagüe se encuentren a niveles inferiores al Centro de Cómputo. Se verificará periódicamente el estado de las griferías y cañerías a fin de evitar posibles inundaciones.

- Es recomendable contar con servicio de aire acondicionado, evitando que esté próximo a material inflamable, asimismo contará con las instrucciones de operación visibles.

- Verificar que el aire acondicionado esté alimentado con agua refrigerada de un suministro confiable.

- Asegurar que las tomas de aire de los equipos se encuentren ubicados en zonas no susceptibles de ser obstruidas.

- Capacitar al personal en el uso y mantenimiento del equipo contra incendio.

- Evitar que las paredes, pisos y techos contengan material inflamable, recomendándose instalar equipos de alarma detectores de humo.

- Para combatir los incendios producidos por equipos eléctricos se deben utilizar extintores, hechos preferentemente de bióxido de carbono, productos químicos secos y liquido vaporizado.

6.1.3.1 Salidas de Emergencia En las salidas de emergencia se ubicarán Barras Antipánico para la apertura de las mismas. Estas Barras, al ser

tocadas durante cierto tiempo, permitirán la liberación de los electroimanes de dichas puertas; paralelamente, emiten una señal de alarma local, y envían una alarma al Cuarto de Control.

6.1.3.2 Elementos de Control Principales En el Centro de Cómputo se tiene una unidad de proceso de información que permite centralizar y actualizar la información que se ingrese de nuevos usuarios del sistema, usuarios excluidos, permisos y niveles de autoridad. De la misma forma permite generar informes para ser impresos sobre: 1) Eventos, 2) Tipos de permisos, 3) Alarmas, 4) Ingresos forzados, 5) Tarjeta habitantes, 6) Por puertas, 7) Por operador, entre otros. Esta unidad constará de un PC principal de control de acceso e integración, y del software respectivo. De igual forma, si la marca propuesta por el proponente lo requiere, se tendrá un panel principal de control de accesos que recibirá y manejará la información de los distintos paneles de acceso ubicados en los Cuartos de Interconexión.

El software permite igualmente la integración con los demás subsistemas del presente diseño (Circuito Cerrado de Televisión y Detección de Intrusión), y permitirá una integración futura con otros sistemas electrónicos (Detección de Incendios, Automatización de Edificios, etc.).

6.1.4 Cuarto de Cableado El cuarto de cableado es por donde el sistema del cableado estructurado debe permitir la distribución del servicio de datos desde el cuarto de cableado más cercano hasta los puestos de trabajo de los usuarios.

Para el soporte físico del cableado a ser distribuido horizontalmente en cada piso se debe utilizar una tubería principal que recorrerá cada una de las plantas a lo largo de éstas y se harán derivaciones para llevar los cables hasta cada uno de los tabiques y mobiliarios, empleando canaletas plásticas con sus accesorios para las áreas visibles y para el interior de las oficinas, terminando cada canaleta en una caja con su respectivo wallplate.

- Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

- Se deben crear áreas seguras para albergar los equipos, preferiblemente cuartos aparte con requisitos de seguridad mínimos.

- Permitir el acceso sólo a personal autorizado.

- Si el encargado necesita salir, debe dejar cerrado con llave el cuarto.
- La Asesoría de Informática y Telemática debe tener una copia de todos los centros de cableado de cada dependencia.

6.1.5 Gabinetes ó Rack Cerrados y Abiertos

- Estas van principalmente dirigidas a aquellos gabinetes que no se encuentran dentro de un cuarto de cableado. De igual manera, es importante que los gabinetes que sí se encuentran dentro de un cuarto cableado, procuren cumplir con estos requisitos mínimos.

- Tener los gabinetes siempre cerrados con llave.

- Designar un encargado de las llaves de los gabinetes, así como un encargado de las copias de las llaves.

- Procurar ubicar los gabinetes en un sitio donde reciban la mejor ventilación posible; o por lo menos dotarlos de un extractor, para evitar que los equipos se recalienten. Aplica tanto para rack cerrados como para abiertos.

- Hacer mantenimiento periódico de los gabinetes. Aplica tanto para rack cerrados como para abiertos.

6.1.6 Controles Generales - Inventario de Equipos

- Llevar a cabo un registro de los equipos activos más importantes dentro de la alcaldía. Este registro debe contener la siguiente información:

    - Código del equipo.

    - Descripción detallada de la configuración del equipo.

    - Responsable del equipo.

- Ubicación del equipo.
- Fecha de adquisición.
- Proveedor.
- Tiempo de garantía.
- Software instalado del equipo.
- Mantenimientos realizados.

- Al ingreso de un nuevo equipo se le debe realizar su registro respectivo para que este quede incluido dentro del inventario de equipos activos.
- Identificar al encargado respectivo de cada equipo, así como identificar su localización.
- Mantener un inventario de equipos activos asociado a cada sistema de información existente dentro de la alcaldía
- Llevar a cabo un registro de los equipos de suministro eléctrico y aire acondicionado. Este registro debe contener la siguiente información:
  - Código del equipo.
  - Descripción detallada de la configuración del equipo.
  - Responsable del equipo.
  - Ubicación del equipo.
  - Fecha de adquisición.
  - Proveedor.

- Tiempo de garantía.
- Referencia de fábrica del equipo.
- Mantenimientos realizados.

6.1.7 Mantenimiento y Aseguramiento de Equipos

- Mantener los equipos según las recomendaciones del proveedor, en cuanto a condiciones naturales y especificaciones técnicas.
- Llevar un registro (bitácora) sobre cuándo y qué tipo de mantenimiento se le ha realizado a cada equipo, así como de las medidas preventivas y correctivas que se les haya llevado a cabo.
- Planeación de capacidad de equipos: las demandas de la capacidad deben estar supervisadas, y deben hacer proyecciones para requisitos a futuro, esto para asegurar procesos adecuados y espacio de almacenamiento disponible. Para esto se debe supervisar en los servidores críticos lo siguiente: espacio en disco duro, RAM, CPU.

6.1.8 Manejo de Recursos de Información

- Llevar un inventario detallado y actualizado que incluya discriminadamente: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, información archivada. Indicando en cada caso, fecha de adquisición y fecha en que fue archivada (según el caso).
- La información detallada anteriormente debe ser recopilada y almacenada por el encargado de cada dependencia, quien a su vez debe remitir una copia de dicha información a la oficina asesoría informática y telemática, en donde se acopiará la información al respecto, de todas las dependencias.

6.1.9 Manejo de Software

- Llevar un inventario detallado y actualizado del software que se maneja. Para facilitar esta tarea se recomienda que cada jefe de sistemas de cada dependencia lleve su propio registro y dé a conocer este documento a la oficina de informática y telemática.

- Cada encargado de sistema debe asegurarse de que los equipos a su cargo solo tengan instalado software legalizado.

- Cada que se realice una compra, instalación o desinstalación de software, se debe reflejar en el inventario. A demás debe existir un procedimiento de autorización en donde se considere lo siguiente:

- Las nuevas instalaciones deben ser adecuadamente aprobadas por los encargados de sistemas, autorizando su propósito y uso. La aprobación también debe obtenerse del director de la oficina de informática y telemática, a fin de garantizar que se cumplen todas las políticas y requerimientos de seguridad pertinentes.

- Cuando corresponda, debe verificarse el hardware y software para garantizar que son compatibles con los componentes de otros sistemas.
  Nota: Puede ser necesaria la comprobación de categorías para ciertas conexiones.

- Deben ser autorizados el uso de las instalaciones personales de procesamiento de información, para el procesamiento de información de la empresa, y los controles necesarios.

- El uso de instalaciones personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades y en consecuencia debe ser evaluado y autorizado.

- Debe existir una persona responsable del inventario del software, que siempre debe estar actualizando y detallando los equipos donde se encuentra instalado.

- Las licencias deben estar inventariadas y custodiadas.

- Se debe advertir a los usuarios de las sanciones legales que implica el instalar software ilegal.

6.1.10 Administración de Proyectos

- Crear y liderar mecanismos de difusión e intercambio de conocimientos y experiencias en materia informática y de telecomunicaciones entre las dependencias.

- Establecer normas y estándares para lograr el desarrollo armónico y coordinado de proyectos de informática y telecomunicaciones con las dependencias y verificar su cumplimiento.

6.1.11 Plan de Respaldo

- Llevar una documentación de procedimientos de operación: en caso de que algún equipo cese sus operaciones normales por cualquier motivo, las bitácoras respectivas deben permitir solucionar los problemas, con tiempos de respuesta estimados según la situación que se presente. Esta es una medida de respaldo para levantar de nuevo el funcionamiento normal de la red en el menor tiempo posible, en caso de que se presenten fallas.

- El Comité Tecnológico Operativo - CTO de la Administración Central Municipal, velará por el cumplimiento de las normas y las políticas de seguridad de los equipos y medios de procesamiento de la información, el cual se recomienda que esté presidido por el Asesor de Informática y Telemática o su delegado.

    - El Comité Tecnológico Operativo - CTO de la Administración Central Municipal deberá promover la seguridad dentro de la entidad, mediante un adecuado compromiso y una apropiada reasignación de recursos. Además deberá cumplir con las siguientes acciones:

        - Revisar y aprobar la política y las responsabilidades generales en materia de seguridad de la información.

- Monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes.

- Revisar y monitorear los incidentes relativos a la seguridad.

- Aprobar las principales iniciativas para incrementar la seguridad de la información.

6.1.12 Respaldo de Información Esencial Respaldar la información significa copiar el contenido lógico del sistema informático a un medio que sea confiable, este fuera de línea (es decir en un lugar seguro) y que la forma de recuperación sea rápida y eficiente.

- Tener copias de seguridad actualizadas con frecuencia, en un medio que sea confiable, y minimice las probabilidades de error.

- Contar con un plan de recuperación rápido y eficiente; para así probar la confiabilidad del sistema de respaldo, no sólo para respaldar sino también para recuperar.

- Probar los sistemas de Backup regularmente, para asegurarse de que sí se podría hacer una restauración dentro del marco de tiempo asignado para la recuperación.

- Los métodos para realizar copias de seguridad deben garantizar la reconstrucción de los archivos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

- Definir mecanismos de comprobación de las copias de seguridad; puede ser restaurando parte de la copia o la copia completa.

- Procurar que las copias de seguridad se realicen de forma automática por medio de un programa de copia, y según la configuración de éste, se podrá realizar un día concreto, diariamente, semanalmente, mensualmente, a una hora concreta, cuando el sistema esté inactivo, etc. Esto según sean las necesidades del sistema.

- Debe existir un responsable de la supervisión del proceso de copias de seguridad, su almacenamiento, e incluso de verificar que las copias se hayan realizado correctamente y funcionen. Adicional a esto debe hacer una verificación periódica a cerca del conocimiento de los usuarios de red, en cuanto a la realización de copias de seguridad.

6.1.13 Administración de Medios de Almacenamiento Removibles

- Almacenar estos medios en un lugar seguro, tan pronto se haya terminado de hacer el respaldo del equipo.
- Evitar la reutilización de medios magnéticos, pues estos cuentan con un período de vida útil.
- Si un medio ya no es requerido, este debe ser destruido y desechado con seguridad.
- Las documentaciones de los sistemas y cintas de Backup deben estar protegidas contra el acceso no autorizado.
- La eliminación cualquier activo de información sensible debe ser registrada, con el fin de mantener una pista de auditoría.
- Para el almacenamiento de las copias de respaldo se deben llenar por cada copia una plantilla que contenga como mínimo la siguiente información:
    - Numeración del medio magnético
    - Contenido
    - Fecha de compra
    - Fecha de ultima utilización (de escritura o lectura)

- Tiempo de vida útil

6.1.14 Sistema Eléctrico

- Disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

- Deberá disponerse de un polo a tierra, conectado al sistema eléctrico que alimenta los equipos. Asimismo se debe etiquetar el cableado, las extensiones y los tableros de distribución eléctrica.
- Asegurar un suministro de energía eléctrica de voltaje estable con la ayuda de sistemas de estabilización de voltaje, supresores de picos y unidades de potencia contra cortes fluidos (UPS).

- Evitar los cableados sueltos o dispersos, éstos deberán entubarse.

- Planes de respuesta a emergencias y recuperación ante desastres.

  - Contar con un plan de contingencia, que contenga las estrategias adecuadas para hacer frente a los desastres. Entre el área de informática y las demás áreas, se deben establecer acuerdos acerca de las condiciones bajo las cuales el plan de contingencia ha de ser activado, considerándose la duración probable de la falta de servicio, y la pérdida (total o parcial) de la capacidad de procesamiento en las instalaciones.

  - Seleccionar organizaciones afines a la Institución y establecer con una o más de ellas convenios de mutuo apoyo, para los casos de desastres que inhabiliten el procesamiento de información. El principal criterio será la confiabilidad sin dejar de lado los límites que deben existir en el intercambio de información de seguridad, para garantizar que no se divulgue información confidencial, perteneciente a la Alcaldía, o entre personas no autorizadas, también habrá que analizar la capacidad del centro de cómputo para efectuar el servicio recíproco.

6.1.15 Autenticación y Seguridad en la Red

- Identificar los problemas referentes a la red y servicios, para así establecer las normas y procedimientos para el uso de los servicios de red.

- Se debe exigir la autenticación de usuarios para las conexiones externas.

- Controlar el acceso a los puertos de diagnóstico con algún mecanismo de seguridad.

- Se deben introducir controles en la red para separar grupos de servicios de información y usuarios. Segmentar la red.

- La capacidad de conexión de los usuarios debe estar limitada al segmento de la red al que pertenece.

- Las redes segmentadas deben tener controles de enrutamiento para asegurar y controlar el acceso de los usuarios que se haya establecido.

- Se debe exigir una descripción clara de las cualidades de seguridad de todos los servicios usados por la red (acceso Internet).

- Para las aplicaciones de alto riesgo, se debe manejar límites en el tiempo de conexión.

- Se debe monitorear y registrar los eventos presentados; es necesario para respaldar futuros controles de acceso.

- Para el establecimiento de las contraseñas se deben seguir los siguientes lineamientos:

    - Capacitar al personal de la Alcaldía, sobre como crear y cambiar las contraseñas.

    - Establecer un tiempo para la caducidad de las contraseñas de entre treinta (30) y sesenta (60) días.

- Las contraseñas deben tener un mínimo de ocho (8) caracteres. Entre mayor longitud, mejor. Es conveniente que contenga alternativamente letras mayúsculas y minúsculas, números y caracteres especiales.

- Cambiar de Clave de Acceso cada tres (3) meses. Aunque lo ideal es hacerlo mensualmente.

- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
- Deben ser fáciles de recordar para no verse obligado a escribirlas. No se debe anotar con exhibición pública y menos pegarla en el monitor o escritorio.

6.1.16 Seguridad de los Equipos - Protección contra: Virus, Gusanos, Troyanos y Malware Los equipos se deben proteger de los virus, los cuales se pueden clasificar en función de múltiples características y criterios: según su origen, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se esconden, los daños que causan, el sistema operativo o la plataforma tecnológica que atacan, etc. Existen varios tipos de virus, según su funcionalidad cómo se describen a continuación:

- Virus residentes. La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

- Virus de acción directa. Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

- Virus de sobreescritura. Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan

un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

- Virus de boot o de arranque. Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador.

- Virus de macro. El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros: documentos de Word (ficheros con extensión DOC), hojas de cálculo de Excel (ficheros con extensión XLS), bases de datos de Access (ficheros con extensión MDB), presentaciones de PowerPoint (ficheros con extensión PPS), ficheros de Corel Draw, etc. Las macros son micro - programas asociados a un fichero, que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas.

- Virus de enlace o directorio. Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

- Virus encriptados. Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran o encriptan a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

- Virus polimórficos. Son virus que en cada infección que realizan se cifran o encriptan de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

- Virus multipartites. Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

- Virus de Fichero. Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

- Virus de FAT. La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador.

Lineamientos a tener en cuenta para la protección de los equipos informáticos de la Administración Central Municipal.

- Los equipos deben contar con programas antivirus instalados y estar en operación, no desactivados; que permitan eliminar cualquier virus de este y/o de otros medios. Este debe permitir la actualización de manera frecuente.

- Procurar que el antivirus cuente con soporte técnico, resolución urgente de nuevos virus y servicios de alerta.

- El antivirus debe permitir la eliminación o detección de virus de distintos dispositivos como discos duros, floppy, etc.

- Los administradores de sistemas con frecuencia deben monitorear la operación de estos programas para asegurarse que los usuarios no los han desactivado o, mejor aún, los usuarios deben estar impedidos de hacerlo.

- Tener cuidado al operar los programas ejecutables si no están seguros de que han sido enviados por una fuente conocida y confiable.

- Mantener el equipo actualizado con los últimos parches disponibles. Para facilitar esta tarea, Microsoft pone a disposición de los usuarios servicios como http://windowsupdate.microsoft.com. Este servicio debe ser lanzado a demanda por parte del usuario.

- Para instalar un nuevo programa o archivo en la red, se debe instalar primero en un equipo no conectado a la red y comprobarlo con el software de detección de virus.

- Se deben adoptar controles de detección y prevención contra Software malicioso.
- Instalar un Firewall de Software / Hardware o cualquier sistema seguro para controlar los puertos del sistema.

6.2 POLÍTICA SEGURIDAD DE LAS COMUNICACIONES

Esta política tiene como objeto definir la normativa de seguridad de la red de comunicaciones de la Administración Central Municipal de Santiago de Cali que garantice la confidencialidad, integridad y disponibilidad de la información en los usos requeridos por sus usuarios tanto internos como externos. A continuación se establecen los lineamentos generales para su cumplimento

- Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Administración Central del Municipio de Santiago de Cali, deberán ser consideradas y tratadas como información confidencial.

- La red de amplia cobertura geográfica a nivel nacional e internacional debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

- Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Administración Central del Municipio de Santiago de Cali, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de ciframiento y verificación de datos,

detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuario(a) s.

- Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.

- Los computadores de la Administración Central del Municipio de Santiago de Cali se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización de la Asesoría de Informática y Telemática.
- Toda información secreta y/o confidencial que se transmita por las redes de comunicación, incluyendo el Portal Municipal, deberá estar cifrada

6.3 POLÍTICAS DE MANEJO Y CONTROL DE LOS SISTEMAS DE INFORMACIÓN

La Administración Central del Municipio de Santiago de Cali, se esmera en facilitar el acceso a sus servidores públicos, sin distingo de cargo o nivel a fuentes de información internas y externas y a proveer un ambiente que fomente la difusión del conocimiento, el proceso de creación y los esfuerzos de colaboración, dentro de la misión institucional y de servicio público.

La Administración Central es proveedora de los medios de acceso a la vasta y creciente cantidad de información disponible a través de medios de información con que cuenta.

El acceso a los sistemas de información en la Administración Central del Municipio de Santiago de Cali, es un privilegio y no un derecho, y por ello debe ser tratado de manera responsable, mesurada y acorde a sus funciones, por todos los usuarios de dichos sistemas.

Deberes de todos los usuarios.

- Actuar honesta y responsablemente.

- Cada usuario es responsable y deberá respetar la integridad de las instalaciones físicas y sus métodos de control.

- Respetar los derechos de otros usuarios.

- Respetar toda licencia pertinente y acuerdo contractual que esté relacionado con los sistemas de información de la Administración Central.

- Actuar de acuerdo con los lineamientos expuestos en éstas política, la normatividad municipal y las Leyes Nacionales pertinentes.

- Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

- Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

- El usuario es el encargado de asegurarse de que sus archivos cuenten con las protecciones necesarias de escritura, lectura y ejecución.

- Es deber del usuario revisar que lo que vaya a introducir en la red o en su computador no esté infectado de virus o Software malicioso.

- La información contenida en los diferentes medios extraíbles también puede contener virus. Los usuarios deberán explorar estos medios antes de copiar o abrir archivos o antes de utilizarlos para iniciar el sistema.

- Es deber de los usuarios informarse acerca de los virus y cómo se difunden normalmente. Aprender las señales comunes de los virus: mensajes extraños que aparecen en la pantalla, rendimiento deficiente del sistema, datos perdidos e imposibilidad de tener

acceso al disco duro. Si advierte algunos de estos problemas en el equipo, debe ejecutar inmediatamente el software de detección de virus para reducir las posibilidades de perder datos.

- Es responsabilidad del usuario realizar el respaldo (Backup) de su información.

- Los usuarios deberán habilitar el bloqueo de pantalla automático luego de un período de inactividad (no inferior a diez (10) minutos).

- En caso de notar un mal funcionamiento en el sistema o algún otro problema, los usuarios deberán dirigirse primero al encargado de sistemas de su respectiva dependencia. Si este no puede resolver el problema, entonces deberán dirigirse a la oficina de informática y telemática.

- Los usuarios deben habilitar el método de autenticación por contraseña para el ingreso a sus equipos.

- Los usuarios deben cambiar sus contraseñas periódicamente, y procurar que estas estén compuestas por letras, números y otros caracteres.

- El usuario se compromete a hacer uso diligente de las contraseñas de acceso y mantener en secreto las mismas.

- El usuario se debe comprometer a comunicar a la oficina de informática la pérdida o robo de contraseñas de acceso en el menor tiempo posible para proceder a su desactivación.

- Si no es necesario, no utilizar los mismos login/password que utilicen para otros servicios o para el acceso a la Red protegida.

- Usar Claves de Acceso que no estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc.

- Solicitar al jefe o encargado de sistema de la dependencia la actualización en forma permanente los últimos parches de los sistemas operativos. Para facilitar esta tarea, Microsoft pone a disposición de los usuarios servicios como http://windowsupdate.microsoft.com. Este servicio debe ser lanzado a demanda por parte del usuario.

- Los únicos autorizados parar realizar instalación y desinstalación de programas, así como cambios de configuración en el sistema operativo, son los encargados de sistemas de cada dependencia; estas acciones deben estar regidas por un procedimiento para hacerlo. Esto con el fin de evitar malas configuraciones y deficiencias en el sistema operativo.

- Es responsabilidad del usuario realizar la limpieza externa del equipo a su cargo.

- La información sensible o confidencial, una vez impresa, debe ser retirada de la impresora inmediatamente.

- El equipo debe protegerse con cubiertas plásticas especiales al finalizar el día.

- Cada usuario es responsable de apagar los equipos de oficina que estén a su cargo al finalizar la jornada de trabajo.

- El uso del ID y contraseña es personal e intransferible.

- Todo buzón de correo es personal e intransferible y su seguridad depende de la privacidad con que el usuario proteja su clave de acceso. Es responsabilidad exclusiva del usuario, preservar cuidadosamente la seguridad de su clave de acceso.

- En caso de que el usuario conozca o sospeche del uso indebido de su ID y/o contraseña por terceros, deberá informar de esta situación a la oficina de informática y telemática al respecto.

- Depurar periódicamente el contenido de los buzones en el correo para evitar que los mensajes permanezcan en el un tiempo excesivo que conduzca a la congestión o el bloqueo del mismo.

- Mantener copias de respaldo de sus carpetas de mensajes de correo más relevantes en su computador personal. En consecuencia se entenderá, que el contenido del buzón de correo está integrado únicamente por archivos "en tránsito" y no almacenados permanentemente allí.

- Si dado el caso el usuario no requiere más de los servicios de correo electrónico, debe informar al encargado de sistemas de la dependencia correspondiente para hacer la respectiva cancelación de la cuenta de correo.

El incumplimiento de esta política puede resultar en la negación de acceso a los sistemas de información de la Administración Central o a otras acciones disciplinarias enmarcadas en la LEY 734 de Febrero 5 de 2002 "Por la cual se expide el Código Disciplinario Único"

6.3.1 POLITICAS DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

6.3.1.1 Uso Permitido Los sistemas de información de la Administración Central son primordialmente para uso de asuntos estrictamente oficiales. El uso personal de cualquier sistema de información para acceder, descargar, transmitir, distribuir o almacenar material o información distinta a la requerida para el normal desempeño de sus funciones está enteramente prohibido y sujeto a sanciones desde el punto de vista disciplinario y penal.

El uso de los recursos de sistemas de información o equipo que tenga como objetivo cualquier tipo de ganancia económica personal para cualquier usuario está prohibido.

6.3.1.2 Acceso Está prohibido el acceso no autorizado a los sistemas de información de la Administración Central. Nadie debe usar la identificación, identidad o contraseña de otro usuario, y de la misma manera ninguno debe dar a conocer su contraseña o identificación, excepto en casos que faciliten la reparación o el mantenimiento de algún servicio o equipo y en este caso

debe dar a conocer estos datos única y exclusivamente a miembros Oficina Asesora de Telemática e Informática de la Administración Central.

6.3.1.2.1 Seguridad Frente al Acceso por parte de Terceros El acceso a las instalaciones de procesamiento de información por parte de terceros debe ser controlado. Cuando se permita dicho acceso, debe realizarse una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control.

- Tipos de acceso: la evaluación de riesgos debe diferenciar acceso físico (oficinas, sala de computo, armarios), y acceso lógico (bases de datos, sistemas de información); puesto que los riesgos existentes en el acceso a través de una conexión de red, son diferentes de los riegos existentes relativos al acceso físico.

- Justificaciones para el acceso: dentro de la evaluación de riesgos se debe analizar el motivo que va a generar dicho acceso. Ya que el acceso puede realizarse por distintas razones, por ejemplo, socios con riesgos compartidos (join ventures) quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos. Otro ejemplo es el personal de mantenimiento, quienes necesitan eventualmente ingresar a la sala de cómputo.

- Contratistas in situ: las personas que sean ubicadas in situ por un periodo de tiempo determinado según contrato (pasantes académicos, personal de limpieza), deben firmar un documento de confidencialidad o de no divulgación por un tiempo definido.

- Personal vital para el funcionamiento: el personal encargado de realizar funciones de gran importancia para el buen funcionamiento del sistema de información (administradores de red, administradores de seguridad informática), debe ser contratado como personal de planta, puesto que estas personas tienen acceso a la red de manera irrestricta, y lo ideal es que se cuente con este personal de manera permanente para evitar inestabilidad en la seguridad.

- Cuando un usuario termina su relación laboral o contractual con la Administración Central, sus identificaciones y contraseñas para todos los sistemas de información, deberán ser entregadas para efectos de

paz y salvo y descargo; las claves serán entonces deshabilitadas inmediatamente.

6.3.1.2.2 Cesión de Privilegios

- La Asesoría de Informática y Telemática es la única autorizada para conceder acceso a los servicios y/o recursos de la red de la Alcaldía, o de dar esta facultad a un usuario con previa autorización presentada por escrito.

- Ningún usuario de la red de comunicaciones está facultado para conceder acceso a los servicios y/o recursos de la red a terceros.

- Todos los usuarios con recursos de la red bajo su responsabilidad, sólo deben hacer uso de los mismos en beneficio institucional, deberán velar por la protección física de los bienes, y acogerse a las presentes políticas y normativas asociadas a las mismas.

6.3.1.3 Uso Indebido de Sistemas de Información Se consideran como mal uso de los sistemas de información las siguientes actuaciones:

- Mutilar físicamente, alterar o extraviar el contenido o información de expedientes físicos y electrónicos.

- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.

- Acceder sin la debida autorización, mediante computadores, software, información o redes de la Administración Central, a recursos externos o que pertenezcan a la Administración Central.

- Interferir sin autorización el acceso a otros usuarios a los recursos de los sistemas de información.

- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.

- Utilizar los sistemas de información para propósitos ilegales o no autorizados.

- Enviar cualquier comunicación electrónica fraudulenta.

- Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente sin la autorización escrita del propietario del software.

- Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.

- Usar las comunicaciones electrónicas para acosar o amenazar a los usuarios de la Administración Central o externos.

- Usar las comunicaciones electrónicas para revelar información privada sin el permiso explícito de la Administración Central.
- Leer la información o archivos de otros usuarios sin su permiso.

- Cualquier tipo de deshonestidad por parte de los servidores públicos.

- Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.

- Usar las comunicaciones electrónicas para adueñarse del trabajo de otros individuos, o de alguna manera apropiarse de trabajo ajeno.

- Monitorear las comunicaciones electrónicas para obtener o fabricar datos de investigación, sin la autorización de la oficina asesora de informática y telemática.

- Lanzar cualquier tipo de virus, gusano, o programa de computador hostil o destructivo.

- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Administración Central.

- Transportar o almacenar material con derechos de propiedad o material nocivo usando las redes de la Administración Central.

- Violar cualquier Ley o regulación nacional respecto al uso de sistemas de información.

- Uso de programas de Reingeniería Inversa (programas de descompilan los ejecutables y los convierten a código fuente).

- Uso de programas que capturan paquetes en la red (Sniffers).

- Uso de programas que capturan los que se digitan por el teclado (KeyLoggers).

- No se permitirá el almacenamiento de archivos de música y videos comerciales en los equipos de cómputo pertenecientes a la Administración Central. Salvo los casos en que estos sean requeridos para funciones relacionadas con el ámbito laboral.
- Los usuarios no deben abrir los computadores, impresoras, reguladores de voltaje etc., para retirar o instalar partes.

- No deben colocarse elementos como plantas, bebidas o alimentos sobre los equipos, ni bloquear las rejillas de ventilación.

- Las computadoras personales, terminales e impresoras no deben dejarse conectadas cuando están desatendidas y estas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso.

- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.

- No se debe confiar en los archivos gratuitos que se descargan de sitios Web desconocidos, ya que son una potencial vía de propagación de virus.

- No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos, tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.

- No utilizar la cuenta para el envío o reenvío de mensajes SPAM o HOAX (falsas alarmas asociadas a virus o fallos de seguridad), o con contenido que pueda resultar ofensivo o dañino para otros usuarios (virus, pornografía), o que sea contrario a las políticas y normas institucionales.

- Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.

- No enviar, contestar o redirigir mensajes de correo que constituyan cadenas.

- Envío de material ofensivo o de contenidos difamatorios.
- Transmisión de información de terceros sin previa autorización de la autoridad competente.

- Distribución no autorizada o copia de software sin licencia.

- Acoso informático y/o electrónico a cualquier miembro usuario de la red.

- Difusión de información de carácter comercial o cualquier otra forma que represente un lucro para la persona que lo origina, o la procura.

- Envío de mensajes hoaxes (falsas alarmas asociadas a virus o fallos de seguridad).

- Difusión de contenidos asociados a proselitismo político, religioso o racial.

- Difusión de material obsceno o que incite a la violencia.

- Cualquier tipo de uso catalogado como infracción informática (hacking, cracking, snooping, probing, entre otros).

- Se prohíbe cualquier tipo de acción o comportamiento que vaya en contra de la seguridad física y/o lógica de los recursos asociados a la red de la Alcaldía. Dichos comportamientos podrán acarrear sanciones institucionales, civiles y/o penales, y no se encuentran limitados a los siguientes:

    - Acceso, uso, puesta a prueba, o exploración no autorizada de los servidores, dispositivos o aplicaciones comprometidas en la prestación de los servicios de la red de la Alcaldía.

    - Bombardeo de correo (uso de mail bombers), inundación de tráfico (TCP Syn Flooding), intentos de denegación de servicio y/o difusión de virus, troyanos o cualquier otro tipo de software malicioso a usuarios, redes y/o servidores de la red, o de cualquier otra red de Internet.

    - Realizar cualquier tipo de suplantación mediante información falsa a nivel de direcciones MAC, encabezados IP o TCP, y/o encabezados a nivel de datos de protocolos de aplicación.

    - Activación, sin previa autorización, de programas que consuman de manera no controlada tiempo de procesamiento en servidores institucionales y de ancho de banda.

    - Cambios en las configuraciones de hardware o software de la red, que puedan ocasionar inestabilidad o caídas en el rendimiento de la red, o de otros recursos comprometidos en la prestación de servicios a través de la misma.

6.3.1.4 Privacidad

6.3.1.4.1 La Privacidad de los Usuarios no está Garantizada Cuando los sistemas de información de la Administración Central funcionan correctamente, un usuario puede considerar los datos que genere como información privada de tipo laboral, a menos que el autor de los datos realice alguna acción para revelarlo a otros. Los usuarios deben estar conscientes

sin embargo, de que ningún sistema de información es completamente seguro, que personas dentro y fuera de la institución pueden encontrar formas de tener acceso a la información. De acuerdo con esto, la Administración Central implementara todos los recursos, herramientas y acciones encaminadas a proveer un entorno de privacidad de los sistemas de información, pero no puede, y no garantiza la privacidad de la información de los usuarios, quienes deben estar conscientes de ello permanentemente.

La Administración Central Municipal se reserva el derecho de investigar, acceder o monitorear con fines de control, los espacios, perfiles e información oficial asignada a los usuarios.

6.3.1.4.2 Reparación y Mantenimiento de Equipos Los usuarios deben saber que ocasionalmente el personal técnico de la Oficina Asesora de Informática y Telemática o su delegado en las Dependencias tiene la autoridad para acceder archivos individuales o datos cada vez que deban realizar un mantenimiento, reparación o chequeo de equipos de computación. Sin embargo el personal técnico no puede exceder su autoridad en ninguna de estas eventualidades para usar esta información para propósitos diferentes a los de mantenimiento o reparación.

6.3.1.4.3 Respuesta al Uso Indebido de Computadores y Sistemas de Información Cuando por alguna causa razonable determinada por el servidor público responsable del proceso o el personal técnico de la Oficina Asesora de Informática y Telemática o quien haga sus veces, considere que algún tipo de uso indebido se ha presentado como se describe en el numeral 6.3.1.3 de este documento, la Administración Central puede acceder cualquier cuenta, datos, archivos, o servicio de información perteneciente a los involucrados en el incidente, para investigar y proceder a solicitar a los organismos de control correspondiente aplicar las sanciones respectivas.

Todos los miembros del personal técnico de la Oficina Asesora de Informática y Telemática están en la obligación de monitorear constantemente los sistemas de información de la Administración Central a través de los medios correspondientes para responder oportunamente a cualquier acción que atente contra la integridad, disponibilidad, seguridad, o desempeño correcto de los mismos mediante la negación, restricción de acceso a usuarios o sistemas, aislamiento o desconexión de equipos o servicios.

Los incidentes deben ser informados al servidor público responsable del proceso o quien haga sus veces con la mayor cantidad de evidencia posible, para tomar las medidas correspondientes.

6.3.1.4.4 Acceso a la Información de los Servidores Públicos en lo Referente a los Procesos al Interior de la Administración Central Municipal Los servidores públicos de la Administración Central llevaran a cabo sus procesos con los sistemas de información de la misma. Cada servidor público controla el acceso a información particular almacenada en los sistemas de información. Sin embargo, si un servidor público no estuviere disponible, se encontrare incapacitado o se negare a proveer información necesaria para llevar a cabo cualquier proceso de la Administración Central, previa autorización por parte del servidor público responsable del proceso, el personal técnico de la Oficina Asesora de Informática y Telemática o quien haga sus veces, puede tener acceso a estos archivos, datos, o partes individuales de los sistemas de información.

6.3.1.5 Mensaje de Datos

6.3.1.5.1 Aplicabilidad Todas las políticas incluidas en este documento son aplicables al mensaje de datos. El mensaje de datos debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los destinatarios colectivos y los foros de discusión. Las Leyes de derechos de autor y licencias de software también aplican para el mensaje de datos.

6.3.1.5.2 Retención del Mensaje de Datos Los mensajes de datos deben ser borrados una vez que la información contenida en ellos ya no sea de utilidad. Cuando se envían comunicaciones por mensaje de datos estas son guardadas en un backup con propósitos de recuperación en caso de fallos. El resguardo de esta información en los backups no excederá un período de quince (15) días, por lo que la responsabilidad del resguardo de datos contenidos en los mensajes es responsabilidad de cada usuario.

6.3.1.6 Portal Municipal El servidor público responsable del proceso, el personal técnico de la Oficina Asesora de Informática y Telemática o quien haga sus veces, garantizará que el portal esté disponible para la publicación de la información de carácter oficial.

Los estándares para los contenidos considerados como oficiales de la Administración Central, serán establecidos por el servidor público responsable del proceso adscrito a la Oficina Asesora de Comunicaciones según los lineamientos establecidos en la Tercera Política de Dirección. Apertura y Visibilidad de la Comunicación con los Usuarios, del Plan de Comunicaciones Organizacional e Informativa de la Administración Central.

6.3.2 POLITICAS DE SEGURIDAD EN LA ADMINISTRACION DE USUARIOS DE LOS SISTEMAS DE INFORMACIÓN Se espera que los usuarios de la Red de la Alcaldía de Santiago de Cali, hagan uso de la misma y de todos los servicios que esta ofrece de forma respetuosa, cortés y con responsabilidad, con el fin de no vulnerar los derechos de los demás usuarios de la Red. Los usuarios deben tener conocimiento básico de cómo funciona una red e Internet, además, de los tipos de uso vistos como aceptados y los tipos de uso que deben evitarse. Todas las personas que hagan uso de los servicios que ofrece la Red de la Alcaldía deberán conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo no debe de exonerar a la persona de las responsabilidades asignadas.

6.3.2.1 Administrador de Usuarios Establece cómo deben ser utilizadas las claves de ingreso a los Sistemas de información de la Administración Central. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas. El administrador de Usuarios es quien tendrá referencia a las pistas o registros de los sucesos relativos a la operación de los usuarios de los Sistemas de Información Administración Central entre otras.

6.3.2.2 Rol de Usuario Los Sistemas de Información de la Administración Central, deberán contar con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos; permitir la asignación a cada usuario de posibles y diferentes roles y permitir un rol de usuario para la administración de los mismos.

6.3.2.3 Protección para Usuarios Externos Como medida de protección a los sistemas de información se define que para entidades externas (Es decir usuarios que no laboren directamente con la Administración Central), se puede otorgar un máximo de dos (2) usuarios.

Para Usuarios Externos se exige el carnet de identificación o cedula de ciudadanía y solo se permitirán y entregarán usuarios de consultas.

6.3.2.4 Protección para Usuarios Internos Para los usuarios internos se tendrán las siguientes consideraciones:

- Cada persona podrá tener uno y solo un usuario, exceptuando a los usuarios administradores, quienes normalmente trabajarán utilizando el usuario sin privilegios y en casos específicos asumirán el rol de administrador.

- Si el usuario ha cometido voluntaria o involuntariamente errores que vulneren la seguridad de los sistemas de información, el servidor público responsable del proceso, el personal técnico de la Oficina Asesora de Informática y Telemática o quien haga sus veces, realizará un análisis y tendrá la libre autoridad para mantener o inhabilitar al usuario.

- Todo servidor público que salga a vacaciones o tenga un permiso por más de tres (3) días, debe informar al administrador de usuarios de su ausencia o salida a vacaciones para que así mismo proceda a bloquearlo hasta nueva orden. El usuario no se borrará, solo se cambiará su clave y se restituirá cuando se reintegre de su periodo de ausencia.

6.3.2.5 Cuenta de Usuario para Acceder a los Sistemas de Información de la Administración Central Municipal Se debe garantizar el correcto uso de los servicios ofrecidos por la red, el usuario de la misma, debe tener una cuenta cuya asignación debe estar dirigida por los siguientes criterios:

- Una cuenta se debe asignar única y exclusivamente a los servidores públicos de la Alcaldía, que laboren en cualquiera de las dependencias.

- La cuenta debe solicitarse mediante una comunicación escrita, dirigida a la Oficina Asesora de Informática y Telemática. En dicha comunicación se debe detallar el nombre, documento de identidad y dependencia donde labora la persona a la cual se le va asignar la cuenta.

- La entrega de la solicitud no garantiza la apertura de la cuenta, antes ésta es analizada por los encargados de la oficina de Informática y Telemática, quienes decidirán si esta es o no abierta. Una garantía para la apertura de la cuenta es que la solicitud venga firmada por el jefe de sistemas de la dependencia correspondiente.

- La vigencia de la cuenta estará determinada por el tiempo de vinculación del usuario con la Alcaldía.

- La notificación de la asignación de la cuenta de usuario, junto con la información de la misma (nombre de usuario, contraseña provisional, solicitud de cambio de la contraseña provisional), debe ser enviada por los encargados de la apertura de la cuenta, al jefe de sistemas de la dependencia correspondiente.
- La cuenta una vez asignada, debe ser de uso personal e intransferible por parte del usuario.

- Si se requiere solicitar una cuenta de usuario para manejo de correo corporativo, se debe diligenciar el Formulario de Solicitud de Correo Corporativo que aparece publicado en la Intranet dentro del Portal Municipal

6.3.2.6 Seguridad del Usuario

- Al momento de realizar una contratación se debe verificar la información presentada por el aspirante al puesto, incluyendo las aptitudes académicas y profesionales alegadas.

- Si el aspirante aplica para un cargo de gran responsabilidad (manejo de información financiera o altamente confidencial), se debe llevar a cabo una verificación de crédito.

- Para casos de contratación a supernumerarios y personal temporal a través de una persona jurídica, el contrato celebrado debe especificar claramente las responsabilidades de la agencia por la selección y los procedimientos de notificación que ésta debe seguir.

- Exigir a los servidores públicos firmar acuerdos de confidencialidad o de no-acceso, como parte de sus condiciones iniciales de empleo.

- Incluir en el acuerdo, tanto la seguridad de los equipos activos como de la información.

- Al finalizar el empleo, y si es pertinente, exigir que estas responsabilidades continúen por un período definido.

6.3.2.7 Capacitación de Usuarios

- Informar a todos los servidores públicos (cuando sea relevante), acerca de las actualizaciones en cuanto a seguridad informática y establecimiento de políticas.

- Crear conciencia en los usuarios, en cuanto a divulgación de claves de acceso, abandono y mantenimiento de equipos, así como manipulación de la información.

- Ilustrar a los usuarios cómo construir una contraseña segura, y que esta debe ser cambiada periódicamente.

- Educar a los usuarios acerca de las distintas amenazas de las pueden ser víctimas (virus, malware, etc.), y como defenderse de éstas. A demás de los riesgos de perdida de información existentes en el manejo de la información.

- Solicitar a los usuarios de los servicios informáticos, advertir y reportar sobre cualquier irregularidad o debilidad que pueda significar una amenaza para los sistemas y servicios.

- Enseñar a los administradores de programas, responsables de Informática y personal de seguridad en Tecnologías de la Información fundamentos de seguridad, administración de riesgos y planes de contingencia.

- Procurar que, al menos anualmente, todos los servidores públicos que utilicen Tecnologías de la Información adquieran conocimientos de seguridad informática.

- Brindarle a los usuarios capacitación en temas referentes al uso de la red y sus servicios, manejo de archivos y del correo.

- Capacitar a los usuarios a cerca de cómo garantizar el buen uso de los equipos, y ejercer los controles necesarios.

- Capacitar a los servidores públicos cada seis (6) meses, en cuanto a las funciones que debe realizar de acuerdo al cargo que realiza. Esto para prevenir que existan personas nuevas o antiguas, que desconozcan parcialmente las tareas que se deben realizar.

6.3.2.8 Derechos de los Usuarios Tanto los encargados de sistemas como los usuarios de red tienen el derecho de conocer las políticas de seguridad informáticas referidas en este documento. Los derechos a que tiene el usuario son los siguientes:

- Los cambios efectuados a nivel operativo, de responsabilidades, o, en las políticas de seguridad deben ser notificadas al personal.

- Los cambios mencionados anteriormente se deben hacer teniendo en cuenta: evaluación del posible impacto de dichos cambios, el procedimiento de aprobación formal de los cambios propuestos, los procedimientos que identifican las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto a los mismos.

- Debe entregarse a los usuarios un detalle escrito de sus derechos de acceso a red.

- Los usuarios internos pueden utilizar los recursos de la red con las limitantes consignadas en el punto de usos inaceptables.

- Los usuarios dispondrán de pleno acceso a los recursos de la red, de acuerdo a lo consignado en el presente documento y en las normativas asociadas a este.

- A los usuarios externos se les faculta a utilizar únicamente los recursos que se les asigne por parte de la Asesoría de Informática y Telemática y/o el proyecto al cual estén inscritos.

- Los usuarios gozan de la privacidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad de la red de la Alcaldía.

- Los usuarios podrán acceder a Internet, cobijados bajo las políticas implementadas mediante firewall y proxy diseñadas por la Asesoría de Informática y Telemática para brindar seguridad a la red de comunicaciones y hacer un buen uso del ancho de banda.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Administración Central Municipal de Santiago de Cali, busca evitar que las amenazas latentes en el entorno, puedan acceder, manipular o deteriorar la información producida por los procesos de la organización y disminuir la posible pérdida de información.

- En caso que nos proporcione información personal, la Administración Central del Municipio de Santiago de Cali protegerá estos datos y no los revelará a terceros, a menos que así se lo hayamos comunicado previamente; previa autorización del usuario(a) ó que estemos requeridos por Ley a hacerlo.

- Nuestros sistemas están dotados de programas destinados a proteger la confidencialidad de la información en ellos contenida y se han implementado los procedimientos destinados a mantenerla. Permanentemente realizamos revisiones a nuestros sistemas,

procedimientos y mecanismos de control, a objeto de reducir los riesgos de cualquier acceso no autorizado.

- La Administración Central del Municipio de Santiago de Cali dará cumplimiento a las normas legales de protección de datos personales, así como a las disposiciones reglamentarias que regulen esta materia. Asimismo, la entidad se encuentra sometida a la regulación y fiscalización de sus actividades por parte de los Organismos de Control Estatal.

- La Administración Central del Municipio de Santiago de Cali procura asegurar que la información ofrecida en su Portal Municipal sea completa, exacta y actualizada. Por ello, se hace responsable por la integridad, exactitud, veracidad o vigencia de la misma.

- La Administración Central del Municipio de Santiago de Cali ha empleado todos los sistemas y medidas técnicas a su alcance para evitar la pérdida, mal uso, alteración, acceso no autorizado y sustracción de los datos facilitados por el Usuario(a). No obstante, el usuario(a) debe ser consciente de que las medidas de seguridad en Internet no son inexpugnables.
- La información del usuario(a) almacenada en los servidores o en el Portal Municipal de la Administración Central del Municipio de Santiago de Cali, se conserva en el entorno más seguro posible. Entre otras medidas de seguridad física y tecnológica, se dispone de medidas de protección como por ejemplo: un control de 'cortafuegos' dirigido a controlar el acceso a los servidores del sitio web desde el exterior.

- La Administración Central del Municipio de Santiago de Cali no vende, cede, ni transmite de modo alguna información personal de sus usuario(a) s a terceros. Los datos personales de los usuario(a) s objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del usuario(a) titular de los datos.

- La Administración Central del Municipio de Santiago de Cali ha adoptado las medidas y niveles de seguridad de protección de los

datos personales exigidos por la Ley 1273 de 2009 “de la protección de la información y de los datos”. Los datos personales recabados a través del Portal Municipal son objeto de tratamiento automatizado y se incorporan a ficheros titularidad del Portal Municipal, siendo su Administrador, responsable de los expresados ficheros.

- Los datos personales de los usuario(a) s que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

- Cuando se recaben datos personales de los usuario(a)s se deberá informar previamente a sus titulares en forma expresa y clara la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios, la existencia del archivo, registro, banco de datos, y la identidad y domicilio de su responsable; el carácter obligatorio o facultativo de las respuestas; las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos y la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.
- Los datos personales de los usuario(a) s que se recojan podrán ser tratados en la medida en que haya mediado el consentimiento libre, expreso e informado del titular de los datos.

- Cuando se recabe información, la misma debe mantenerse fiel al principio de finalidad, que implica que la información ha sido entregada con una sola finalidad y bajo ella se puede utilizar.

- El usuario(a) titular de los datos tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos y que estos sean rectificados y actualizados, cuando corresponda.

- El usuario(a) titular de los datos tiene derecho a solicitar, cuando corresponda, la supresión del dato caduco para evitar quedar prisionero de su pasado.

8. DOCUMENTOS DE REFERENCIA

- LEY 43 del 29/oct/1913 “Provee a la conservación de ciertos documentos oficiales”.

- LEY 87 del 29/nov/1993 “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones”.

- LEY 489 del 29/dic/1998 “Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones”.

- LEY 527 del 18/ago/1999 “Por medio de la cual se definen y reglamentan el acceso y su de los mensajes de datos, del comercio electrónico y de las firmas digitales”

- LEY 734 del 05/feb/2002 “Por la cual se expide el Código Disciplinario Único”.

- LEY 850 del 18/nov/2003 “Por medio del cual se reglamentan las veedurías ciudadanas”.

- LEY 872 del 30/dic/2003 “Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios”.

- LEY 909 del 23/sep/2004 “Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones”, y sus Decretos Reglamentarios, y demás normas aplicables a los Servidores Públicos.

- LEY 1273 del 05/ene/2009 “Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado

"de la protección de la información y de los datos"·y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- Decreto Nacional N°1537 del 06/jul/2001 “Por el cual se reglamenta parcialmente la LEY 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado”.

- Decreto Nacional 2170 del 30/sep/2002 “Por el cual se reglamenta la LEY 80 de 1993, se modifica el Decreto 855 de 1994 y se dictan otras disposiciones en aplicación de la LEY 527 de 1999”

- Decreto Nacional N°4110 del 09/dic/2004 “Por el cual se reglamenta la LEY 872 de 2003 y se adopta la Norma Técnica de Calidad en la Gestión Pública - NTCGP 1000 – 2004”.

- Decreto Nacional N°1599 del 20/may/2005 “Por el cual se adopta el Modelo Estándar de Control Interno MECI 1000:2005”.

- Decreto Nacional N° 3622 del 10/oct/2005 “Por el cual se adoptan las políticas de desarrollo administrativo y se reglamenta el capítulo cuarto de la LEY 489 de 1998 en lo referente al Sistema de Desarrollo Administrativo”.

- Decreto Nacional N° 4485 del 18/nov/2009 “Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública”.

- Modelo de Comunicación Pública, Organizacional e Informativa para entidades del Estado. Casals y Asociados. Marzo 2004.

- Norma NTC-ISO/IEC 27001:2005 Sistema de Gestión de Seguridad de Información.

- ISO 7498-2 Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture

Elaborado por: Equipo del DAPM y CTO	Cargo: No Aplica	Fecha: 09/sep/2010	Firma
Revisado por: Réinelo Rodríguez Lemus	Cargo: Asesor de Informática y Telemática	Fecha: 09/sep/2010	Firma
Aprobado por: María Grace Figueroa Ruiz	Cargo: Directora Departamento Administrativo de Planeación Municipal	Fecha: 09/sep/2010	Firma