ALCALDIA MUNICIPAL DE SINCELEJO

SECRETARÍA TIC

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

GESTIÓN INTEGRAL

2020

MANUAL DE SEGURIDAD DE LA INFORMACION

Este manual, tiene por objeto establecer las medidas de indo le técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la Alcaldía Municipal de Sincelejo.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

DISPOSICIONES GENERALES

2.1 Definiciones

La Estrategia Gobierno en Línea de la Alcaldía Municipal de Sincelejo, ha desarrollado las siguientes Políticas de Seguridad Informática, las cuales son un conjunto de normas enmarcadas en el ámbito jurídico y administrativo de las entidades. Estas normas inciden en la adquisición y el uso de los bienes y servicios informáticos, las cuales se deberán acatar por aquellas instancias que intervengan directa o indirectamente en ello.

2.1.1 ABD

Administrador de Base de Datos.

2.1.2 ATIC

Administradores de Tecnología de Información y de las Comunicaciones de la Alcaldía Municipal de Sincelejo son los responsables de la administración de los equipos de cómputo, sistemas de información y redes y comunicaciones. Su función es velar por todo lo relacionado con la utilización de equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

La Oficina de Informática actualmente está conformado por funcionarios idóneos, los cuales tienen a su cargo distintas funciones referentes al soporte y mantenimiento de la plataforma tecnológica, desarrollo de sistemas de información, administración de bases de datos, gestión de recursos de tecnología y administración de redes y comunicaciones; por esta razón ha sido necesario emitir políticas particulares para el conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos.

Los ATIC son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.
- Definir estrategias y objetivos a corto, mediano y largo plazo.
- Mantener la arquitectura tecnológica.
- Controlar la calidad del servicio brindado.
- Mantener el Inventario actualizado de los recursos informáticos.
- Velar por el cumplimiento de las políticas y procedimientos establecidos.
- Desarrollar, someter a revisión y divulgar (intranet, email, sitio web oficial) las Políticas de Seguridad.

2.1.3 Comité

Equipo integrado por Representante(s) de ATIC, los Jefes de área y personal administrativo de Las entidades (ocasionalmente) convocados para fines específicos como:

- Adquisiciones de Hardware y software
- Establecimiento de estándares de Las entidad tanto de hardware como de software.
- Establecimiento de la Arquitectura tecnológica de grupo.
- Capacitar a los empleados en lo relacionado con las Políticas de Seguridad.

2.1.4 Contraseña

Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

2.1.5 Centro de Comunicaciones

Oficina con equipos de cómputo, telecomunicaciones y servidores que prestan servicios a todas
Las Empresas con las características físicas y ambientales adecuadas para que los equipos alojados funcionen sin problema.

2.1.6 Gestor de Seguridad

Persona dotada de conocimientos técnicos, encargada de velar por la seguridad de la información, realizar auditorías de seguridad, elaborar documentos de seguridad como, políticas, normas; y de llevar un estricto control con la ayuda de los ATIC referente a los servicios prestados y niveles de seguridad aceptados para tales servicios.

2.1.7 Red

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos, donde siempre hay un receptor y un emisor. Nuestra red está Compuesta por medios de comunicación, equipos de cómputo, servidores, dispositivos de comunicación, telefonía y algunos periféricos.

2.1.8 Responsable de Activos

Personal del área administrativa, que velará por la seguridad y correcto funcionamiento de los activos informáticos, así como de la información procesada en éstos, dentro de sus respectivas áreas. Esta persona debe mantener el inventario físico al día, velar por que todos los activos tengan sus respectivas pólizas de seguros bajo los parámetros de ley.

2.1.9 Solución Antivirus
Recurso informático empleado para solucionar problemas causados por virus informáticos.

2.1.10 Usuario
Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por Alcaldía Municipal de Sincelejo tales como equipos de cómputo, sistemas de información, redes de telemática.

2.1.11 Virus informático
Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

2.2 Alcance
Esta política aplica a toda la entidad en el proceso de Tecnología de Información, a los empleados, contratistas, consultores, eventuales y otros empleados, incluyendo a todo el personal externo que cuenten con un equipo conectado a la Red; También a todo el equipo y servicios propietarios o arrendados que de alguna manera tengan que utilizar local o remotamente el uso de la Red o recursos tecnológicos de la Alcaldía Municipal de Sincelejo así como de los servicios e intercambio de archivos y programas de esta institución y la ciudadanía en general.

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% de la política.

La elaboración de las Políticas de Seguridad está fundamentada bajo la norma ISO 27001, han sido planteadas, analizadas y revisadas con el fin de no contravenir con las garantías básicas de los usuarios, y no pretende ser una camisa de fuerza, y más bien muestra una buena forma de operar los sistemas con seguridad, respetando en todo momento estatutos y reglamentos internos de la entidad;

Esto aplicado a:

- Control de acceso (aplicaciones, base de datos, área del Centro de Cómputo, sedes filiales).

- Resguardo de la Información.
- Clasificación y control de activos.
- Gestión de las redes.
- Seguridad de la Información en los puestos de trabajo.
- Controles de Cambios.
- Protección contra intrusión en software en los sistemas de información.
- Monitoreo de la seguridad.
- Identificación y autenticación.
- Utilización de recursos de seguridad.
- Comunicaciones.
- Privacidad.

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% de la política.

2,3 Objetivos

Dotar de la información necesaria a los usuarios, empleados y directivos, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la Red, así como la información que es procesada y almacenada en estos.

Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la Alcaldía Municipal de Sincelejo.

Los objetivos que se desean alcanzar luego de implantar la Política de Seguridad son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de los ATIC.
- Compromiso de todo el personal de la Alcaldía Municipal de Sincelejo con el proceso de seguridad, agilizando la aplicación de los controles.
- Que la prestación del servicio de seguridad genere tranquilidad y agilidad en los procesos.
- Todos los empleados se convierten en interventores del sistema de seguridad.

2.4 Vigencia

La documentación presentada como Políticas de Seguridad entrará en vigencia desde el momento en que sean aprobadas por el Alcalde del municipio de Sincelejo. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de esta Institución o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

2.5 Notificaciones de violaciones de seguridad.

Todo empleado es responsable del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también notificar a su nivel jerárquico superior, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad.

Es de carácter obligatorio para todo el personal (Fijo o Contratado), la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito vía correo electrónico a los, quienes están en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.
Es obligatorio que el personal de la entidad conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación de la política.

2.6 Lineamientos para la adquisición de bienes informáticos.

Toda adquisición de tecnología informática se efectuará a través del Comité. Los ATIC, deberán planear las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomar en cuenta:

2.6.1 Precio.

Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.

2.6.2 Calidad.

Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

2.6.3 Experiencia.

Presencia en el mercado, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

2.6.4 Desarrollo Tecnológico.

Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

2.6.5 Estándares.

Toda adquisición se basa en los estándares, es decir la arquitectura de grupo empresarial establecida por el Comité. Esta arquitectura tiene una permanencia mínima de dos a cinco años.

2.6.6 Capacidades

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área. Para la adquisición de Hardware se tendrá en cuenta lo siguiente:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en sitio.
- Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por los ATIC.
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local. Los ATIC son los encargados de emitir periódicamente las especificaciones técnicas mínimas para su adquisición.
- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y en Las Empresas, corroborando que los suministros (tinta, cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Los equipos adquiridos deben contar con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, switch es y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.

- En lo que se refiere a los computadores personales, al vencer su garantía por adquisición, deberán contar con por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de repuestos.
- Todo proyecto de adquisición de bienes de tecnología, debe sujetarse al análisis, aprobación y autorización del Comité.

2.6.7 Software

En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente.

Para la adquisición de Software base y utilitarios, el Comité dará a conocer periódicamente las tendencias con tecnología de punta vigente, siendo la principal lista de productos autorizados la siguiente:

2.6.7.1 Sistemas Operativos

- MS-Windows
- Mac OS-X
- GNU (Versiones de Linux)

2.6.7.2 Bases de Datos

- MS-SQL
- MySQL

2.6.7.3 Lenguajes y herramientas de programación

- **PHP**: Nunca pretendió ser un lenguaje de programación, sino que fue creado con la intención de contar con un conjunto de herramientas para el mantenimiento de las páginas web.
- Java: Reconocido por su legibilidad y simplicidad, Java es uno de los lenguajes de programación más adoptados

- **C**: Creado entre 1969 y 1972 en los Laboratorios Bell, es uno de los más utilizados en el mundo.

- **C++**: Conocido por el nombre **"C Plus Plus"**, este lenguaje de programación orientado a objetos surge como una continuación y ampliación del C.

- **Pyhton**: Un lenguaje de programación multiplataforma y multiparadigma, que también es de propósito general.

- **C#**: También llamado **"C Sharp"**, es una evolución del C y C++ que se destaca por su sencillez y modernidad.

- **Visual Basic. NET**: Es visto como uno de los lenguajes más amigables para los que recién comienzan, sobre todo a comparación de C#.

- **JavaScript**: Es un lenguaje de programación que puede ser utilizado para crear programas que luego son acoplados a una página web o dentro de programas más grandes. Podemos ver funcionando este lenguaje en servicios como el chat, calculadoras, buscadores de información y un sin fin de utilidades más.

- **Perl**: Es un lenguaje de propósito general que sirve prácticamente para todo, como puede ser la generación y tratamiento de ficheros, para analizar datos y textos, y muchas otras cosas más.

- **Assembly language** (ASL): (lenguaje ensamblador) Se trata de un lenguaje de programación de bajo nivel utilizado para interactuar con hardware informático.

2.6.7.4 Utilitarios de oficina

- Microsoft Office 365
- Oppen Office
- Readers para PDF

2.6.7.5 Programas antivirus

- Kaspersky antivirus

2.6.7.6 Correo electrónico

- Outlook de Office 365

2.6.7.7 Navegadores de Internet

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Opera

2.7 Licenciamiento

- Todos los productos de Software que 5se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.
- Los ATIC promoverán y propiciarán que la adquisición de software de dominio público o free que provenga de sitios oficiales y seguros.

2.8 Bases de datos

Para la operación del software de red en caso de manejar los datos institucionales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- Toda la información de la Alcaldía municipal de Sincelejo deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.

- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.

- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los CD, DVD, Discos externo y Servidores de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Google Drive) o en medios de almacenamiento alternos.

- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados.

- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).
- Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

2.9 Frecuencia de evaluación de las políticas.

Se evaluarán las políticas del presente documento, con una frecuencia anual por el Comité de SGSI.
Las políticas serán evaluadas por los ATIC con una frecuencia semestral.

3 POLÍTICAS DE SEGURIDAD FISICA

3.1 Acceso Físico

La Alcaldía Municipal de Sincelejo tiene un área que funciona como centro de telecomunicaciones donde se ubican los sistemas de telecomunicaciones y servidores, por lo tanto:

- Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

- El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante la permanencia del mismo.

- Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable de la Oficina de Sistemas o con permiso de los ATIC.

- Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

- El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo, el Superior responsable, los ATIC o personal de Servicios generales debidamente autorizado, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del área Administrativa y al personal de seguridad del edificio en caso que requiera salida del mismo.

3.2 Protección Física

3.2.1 Rack de Comunicaciones.

El Rack de Comunicaciones deberá

- Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.
- Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado.
- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- Aire acondicionado. Mantener la temperatura a 21 grados centígrados.
- Asignar un técnico para que realice un control diario temperatura y aires acondicionados y llevar un registro de estos controles.
- Respaldo de energía redundante.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

- Contar con algún esquema que asegure la continuidad del servicio.
- Tener Control de humedad
- Prevención y/o detección de incendios
- Sistemas de extinción.
- Contar por lo menos con dos extintores de incendio adecuado y cercano al Rack de
- Comunicaciones.

3.2.2 Infraestructura

Las dependencias deberán considerar los estándares vigentes de cableado estructurado y/o medios de transmisión inalámbrica durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.
El resguardo de los equipos de cómputo deberá quedar bajo La Oficina de Informática, contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

3.3 Instalaciones de equipos de cómputo

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- El Área de Tecnología, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de la red de Voz y Datos.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

3.4 Control

- Los ATIC deben llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.

- Los encargados de La Oficina de Sistemas son los responsables de organizar al

personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

- El Área de Recursos Humanos deberá reportar a los ATIC cuando un usuario deje de laborar o de tener una relación con La Alcaldía municipal de Sincelejo con el fin de retirarle las credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.

- El usuario, en caso de retiro, deberá tramitar ante La Oficina de Informática el paz y salvo correspondiente.

3.5 Respaldos

- Las Bases de Datos serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.

- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Cloud) que permita tener contingencia y continuidad de procesos.

- Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; y en las unidades de almacenamiento asignadas por La Institución o en "La Nube" (Google Drive), deberá realizar una sincronización continua de la información importante de la Alcaldía Municipal de Sincelejo, Los respaldos serán responsabilidad absoluta de los usuarios.

- Los ATIC no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

3.6 Recursos de los usuarios

3.6.1 Uso

- Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y Red de la Alcaldía de Sincelejo, de acuerdo con las políticas que en este documento se mencionan.

- Los usuarios deberán solicitar apoyo la oficina de informática ante cualquier duda en el manejo de los recursos de cómputo de la Alcaldía municipal de Sincelejo.

- El correo electrónico no se deberá usar para envío de material no institucional o innecesario.

3.6.2 Derechos de Autor

- Todo software desarrollado internamente en la Alcaldía municipal de Sincelejo por funcionarios o contratistas, automáticamente pasara a ser parte de los activos de software de la Alcaldía municipal de Sincelejo.

- Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los usuarios deberán firmar un documento donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

- Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la Alcaldía municipal de Sincelejo bajo ninguna circunstancia sin la autorización escrita de la Oficina de informática.

- No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que la Alcaldía municipal de Sincelejo posee una licencia que cubre dicha instalación.

- No está autorizada la descarga de Internet de programas informáticos no autorizados por la Administración de TIC de la Alcaldía municipal de Sincelejo.

- No se tolerará que un empleado realice copias no autorizadas de programas informáticos.

- No se tolerará que un empleado cargue o descargue programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos para utilizar sistemas de peer-to-peer (P2P- Ej. Kazaa) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.

- No se tolerará un empleado realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

- Si se descubre que un empleado ha copiado programas informáticos o música en forma ilegal, este puede ser sancionado, suspendido.

- Si se descubre que un empleado ha copiado programas informáticos en forma ilegal para dárselos a un tercero, también puede ser sancionado, suspendido o despedido.

- Si un usuario desea utilizar programas informáticos autorizados por la Alcaldía municipal de Sincelejo en su hogar, debe consultar con los ATIC para asegurarse de que ese uso esté permitido por la licencia del editor.

- El personal encargado de soporte de Tecnología revisará las computadoras constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si se poseen licencias para cada una de las copias de los programas informáticos instalados.

- Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.

- Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

- Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión.

- No se permite la duplicación ilegal de programas informáticos.

- Los empleados que realicen, adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo a las circunstancias. Dichas sanciones pueden incluir suspensiones y despidos justificados.

4 POLÍTICAS DE SEGURIDAD LOGICA.

4.1 Red

- Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de la entidad, entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes.

- El Área de TIC no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

- No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de Alcaldía municipal de Sincelejo.

- El uso de analizadores de red es permitido única y exclusivamente por los ATIC para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.

- No se permitirá el uso de analizadores para monitorear o censar redes ajenas a la Alcaldía municipal de Sincelejo y no se deberán realizar análisis de la Red desde equipos externos a la entidad.

4.2 Servidores

4.2.1 figuración, instalación y funcionamiento

- Los ATIC tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

- La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de los ATIC.

- El Acceso Remoto a los Servidores o a cualquier Pc de la red interna de la Alcaldía municipal de Sincelejo solo será uso de los ATIC bajo estricta necesidad laboral.

- Si por motivos técnicos es necesario detener algún servidor o servicio, es necesario informar con anterioridad a los usuarios directamente afectados dentro

de la red de esta entidad.

- Todo mantenimiento técnico de hardware o software que se quiera hacer a los servidores, debe planearse en horarios de mínima congestión o solicitud de los servicios que este preste.

- Durante la configuración de los servidores, los ATIC deben genera las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

- Los servidores que proporcionen servicios a través de la red e Internet deberán:

  a. Funcionar 24 horas del día los 365 días del año.
  b. Recibir mantenimiento preventivo mínimo dos veces al año.
  c. Recibir mantenimiento semestral que incluya depuración de Bases de Datos.
  d. Recibir mantenimiento anual que incluya la revisión de su configuración.
  e. Ser monitoreados por los ATIC.

- La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

  a. Diariamente, información crítica.
  b. Semanalmente, los documentos web.
  c. Mensualmente, configuración del servidor y Bases de datos.
  d. Los servicios de Internet sólo podrán proveerse a través de los servidores autorizados por los ATIC.

4.2.2 Electrónico

- Los ATIC se encargarán de asignar las cuentas a los usuarios para el uso de correo electrónico institucional en los servidores propios que administra bajo el dominio @sincelejo.gov.co.

- Para efecto de asignarle su cuenta de correo al usuario, el área de Recursos Humanos deberá llenar una solicitud en formato establecido para tal fin y entregarlo al área de Tecnología, con su firma o la del Jefe del área.

- La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

- Para mayor seguridad, es obligatorio cambiar la contraseña en un plazo no mayor a 24 horas luego de ingresar por primera vez.

- La longitud mínima de las contraseñas será igual o superior a ocho (8) caracteres. Se recomienda usar por lo menos un carácter numérico y una letra mayúscula.

- En caso de olvidar la clave, dirigirse ante el administrador del correo electrónico de la entidad.

4.2.3 Bases de Datos

- El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

- El Administrador de la Base de Datos es el encargado de asignar las cuentas y establecer roles a los usuarios para tal uso.

- Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

- En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

4.3 Recursos de Cómputo

4.3.1 Seguridad de cómputo

- Los ATIC son los encargados de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

- Los ATIC deben mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

- Los ATIC son los únicos autorizados para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

4.3.2 Soporte Técnico

El Soporte Técnico se hará bajo las atribuciones y/o responsabilidades siguientes:

- Podrá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.

- Deberán realizar respaldos periódicos de la información de los equipos de cómputo, siempre y cuando se cuente con dispositivos de respaldo y se haga solicitud por parte del responsable del pc.

- Deben actualizar la información de los recursos de cómputo cada vez que adquiera e instale equipos o software.

- Deben registrar cada máquina en el inventario de control de equipos de cómputo y red de la Alcaldía municipal de Sincelejo.

- Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

- Reportar a la Administración los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

4.3.3 Renovación de equipos

- Los ATIC deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

- Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de Tecnología a fin de que se seleccione el equipo adecuado. Sin el visto bueno del área de TIC no podrá liberarse una orden de compra.

4.4 Uso de Servicios de Red

4.4.1 Oficinas y Sedes

Se definirá los servicios de Internet a ofrecer a los usuarios y serán los ATIC quienes otorguen la configuración.

Se podrá utilizar la infraestructura de la Red para proveer servicios a los usuarios externos y/o visitas previa autorización los ATIC.

Los ATIC son los responsables de la administración de contraseñas y deberán guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.

No se asignaran equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en la Alcaldía de Sincelejo, excepto por orden expresa del jefe del área tratada.

Los ATIC son los únicos autorizado para asignar las cuentas a los usuarios.

Los ATIC podrán aislar cualquier servidor de red, notificando a las dependencias y áreas de la entidad, en las condiciones siguientes:

a. Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
b. Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
c. Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
d. Si se detectan accesos no autorizados que comprometan la integridad de la información.
e. Si se viola las políticas de uso de los servidores.
f. Si se reporta un tráfico adicional que comprometa a la red de Empresas externas.

4.4.2 Usuarios

4.4.2.1 Acceso

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por la administración municipal.

4.4.2.2 Responsabilidades Personales

- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre que sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco del equipo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

4.4.2.3 Uso Apropiado de los Recursos.

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

4.4.2.3.1 Queda Prohibido

- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del software o de los estándares de los recursos informáticos propios de la Alcaldía municipal de Sincelejo.

- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.

- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos de propiedad de la Alcaldía municipal de Sincelejo, a menos que atente contra la seguridad, disponibilidad y accequibilidad de los activos de información de esta entidad, en tal caso dirigirse a la oficina de Informática.

- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y en especial, las referidas a propiedad intelectual y control de virus.

4.5 Antivirus

4.5.1 Antivirus de la Red

Todos los equipos de cómputo de la Alcaldía municipal de Sincelejo deben tener instalada una Solución Antivirus con actualización automática desde Internet.

Cuando el usuario requiera hacer uso de discos, UBS, en sus computadoras, éstos deben ser rastreados por la solución antivirus.

4.5.2 Responsabilidad de los ATIC

Los ATIC serán responsables de:

Instalar la Solución Antivirus en las computadoras de la Alcaldía municipal de Sincelejo.

Solucionar contingencias presentadas ante el surgimiento de virus que la solución no se haya detectado automáticamente.

Los ATIC aislarán el equipo o red, en las condiciones siguientes:

a. Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros equipos y redes.

b. Si el usuario viola las políticas antivirus.

4.5.3 Cobertura

La solución de Antivirus debe tener cobertura a los siguientes sistemas operativos:

- Microsoft: Windows XP/ VISTA / 7 /8/10 en versiones 32 y 64 bits.
- Apple: Mac OS X 10.4/10.5/10.6/10.7/10.8

5 SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles.
Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Los ATIC implementarán soluciones lógicas y físicas que garanticen la protección de la información de la Alcaldía municipal de Sincelejo de posibles ataques internos o externos, las cuales deben:

- Rechazar conexiones a servicios comprometidos.
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de

dispositivos de red cuentas de usuarios internos.

5.1 Firewall

La solución de seguridad perimetral debe ser controlada con un Firewall que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.

Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.

Los ATIC establecerán las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.

El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.

El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

5.2 Redes Privadas Virtuales (VPN)

Los usuarios móviles y remotos de la Alcaldía municipal de Sincelejo, podrán tener acceso al a red interna privada cuando se encuentren fuera de la entidad alrededor del mundo en cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por la Oficina de Informática.

Los ATIC serán los encargados de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

5.3 Conectividad a Internet

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de la Alcaldía municipal de Sincelejo tienen las mismas responsabilidades en cuanto al uso de Internet.

El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall y Proxy incorporado en la misma.

Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

5.4 Red Inalámbrica (WIFI)

5.5.1 Acceso a Funcionarios de la Alcaldía municipal de Sincelejo:

La red inalámbrica (WIFI) de la Alcaldía municipal de Sincelejo es un servicio que permite a los usuarios conectarse sin la necesidad de algún tipo de cableado.

La Red inalámbrica le permitirá utilizar los servicios de Red en las zonas de cobertura (Hot Spot), donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, Tablet, Celulares, etc.) con capacidad de conexión Wireless.

Los ATIC, son los encargados de la administración, habilitación y/o bajas de usuarios en la red inalámbrica de red Wifi de la Alcaldía municipal de Sincelejo.

5.5.1.1 Identificación y activación

Para hacer uso de la red inalámbrica (WIFI), el solicitante necesariamente deberá ser Funcionario o Invitado de la Alcaldía municipal de Sincelejo.

Como primer paso para hacer uso de este servicio, los ATIC deben de registrar los usuarios que deseen la prestación del servicio a la red inalámbrica.

Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos de comunicación.

Los Dispositivos de conexión Inalámbrica destinados a los invitados, deben emplear autenticación tipo WPA2-AUTO-PSK para lo cual los nombres de usuarios y contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los usuarios.

5.5.1.2 Seguridad

A pesar de que se han establecido sistemas de encriptación de datos mediante el uso de medidas de seguridad, NO SE RECOMIENDA hacer uso de tarjetas de crédito para compras.

Los ATIC determinarán las medidas pertinentes de seguridad para usar las redes inalámbricas.

Los ATIC se reservan el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red. No se deben realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal.

No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica (Sniffer). Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.

Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a los ATIC para su respectiva baja del equipo de la red inalámbrica.

5.5.1.3 Tecnología

La red inalámbrica de Alcaldía Municipal de Sincelejo usa el estándar B02.11b/g/n con cifrado WPA2. Por lo tanto las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi de este estándar y soportar los requerimientos descritos.

Caso contrario se debe realizar algunas actualizaciones previas de tratarse de computador portátil.

A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA en ninguna forma el acceso desde cualquier punto fuera de cobertura de los equipos de conexión Inalámbrica de la Alcaldía Municipal de Sincelejo.

Sólo será soportado el protocolo TCP/IPV.4 en la red inalámbrica.

La Oficina de Informática se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios de Alcaldía Municipal de Sincelejo.

No se permiten la operación ni instalación de "puntos de acceso" (Access points) conectados a la red cableada de Alcaldía Municipal de Sincelejo sin la debida autorización por parte los ATIC.

No se permite configurar las tarjetas inalámbricas como "puntos de acceso o redes Ad Hoc" o la configuración de equipos como servidores adicionales.

5.5.1.4 Restricciones/prohibiciones de acceso a Internet

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (Peer to Peer).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
- Uso de JUEGOS "on líne" en la red.

5.5.1.5 Excepciones

- Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.
- En caso de eventos, cursos, talleres, conferencias, etc., se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.
- En el caso de estos eventos las restricciones para acceder podrán ser "anuladas" temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

6 PLAN DE CONTINGENCIAS INFORMATICAS

Los ATIC crearán para los departamentos un plan de contingencias info6rmáticas que incluya al menos los siguientes puntos:

- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

7 ACTUALIZACIONES DE LA POLITICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la Alcaldía municipal de Sincelejo se reserva el derecho a modificar esta política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los usuarios de esta institución.

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de la Política de Seguridad más reciente.

7.1 Disposiciones

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión. Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo del Comité; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

La falta de conocimiento de las normas aquí descritas por parte de los usuarios no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.