Alcaldía de Medellín
ISVIMED
Instituto Social de Vivienda y Hábitat de Medellín

Políticas de Seguridad de la Información

ELABORADO POR	REVISADO POR	APROBADO POR
Carlos Gómez Valencia Profesional Esp. Juan F. Gonzalez Ochoa. Contratista.	Verónica Arias Garcés Subdirector Administrativo y Financiero.	Verónica Arias Garcés Subdirector Administrativo y Financiero.

Introducción

La política general de seguridad de la información de la institución es una declaración de la conducta, ética y responsabilidad adoptada por la organización, con el fin de proveer un ambiente seguro en el manejo de la información propia, de clientes y de terceras personas.

La institución ha establecido las presentes políticas de seguridad de la información, en donde se definen los lineamientos principales para el establecimiento de la gestión de seguridad de la información, con el fin de establecer una cultura de seguridad de la información en todos los procesos de la entidad ya que esta debe siempre estar protegida en forma adecuada.

Objetivo

Determinar los parámetros generales para que la información que se maneja en la Institución bien sea, propia, en custodia, o compartida con terceros que cumpla con los siguientes criterios:

1. Sea protegida contra modificaciones no autorizadas, realizadas con o sin intención.
2. Sea accedida y usada sólo por aquellos que tienen una necesidad legítima, para la realización de las funciones propias de su cargo en la institución.
3. Esté disponible cuando sea requerida y sea utilizada exclusivamente para los propósitos para los cuales fue obtenida.

Objetivos Específicos

Fundamentar el desarrollo, implantación, mantenimiento y cumplimiento de la Seguridad de la información por medio de un Sistema de Gestión de Seguridad que la despliegue.

Confidencialidad: Que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Que se salvaguarde la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad: Que se asegure la validez de la información en tiempo, forma y distribución. Asimismo, se garantice el origen de la información, validando el emisor para evitar la suplantación.

Auditabilidad: Que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: Consiste en asegurar que un documento sólo se realice una vez, que sea único y no existan múltiples replicas, a menos que se especifique lo contrario.

No repudio: Garantizar que toda comunicación que se envié o se reciba llegue al destinatario final.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la Institución.

Confiabilidad: Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

ALCANCE

Estas políticas deben ser conocidas y cumplidas tanto por funcionarios de la entidad, como por los contratistas que apoyan la gestión y que utilicen la información generada y custodiada y por quienes hagan uso de los servicios tecnológicos de la Entidad.

Controles a Implementar

- ✓ Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.

- ✓ Dotar de seguridad toda la información confidencial que se maneja en los equipos y redes de la entidad.

- ✓ Dotar a sus terminales, equipos de cómputo y redes locales, de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de los usuarios y de sus operaciones.

- ✓ Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales e instrumentos para la realización de operaciones. En desarrollo de lo anterior, la entidad deberá establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.

- ✓ Tener en operación sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad. Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.

- ✓ Llevar el registro de las actividades adelantadas sobre los dispositivos finales a cargo de la entidad, usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.

Procedimientos

Gestión de Seguridad y Riesgos Informáticos

Este procedimiento inicia con la identificación de las necesidades de seguridad y mitigación de riesgos, y finaliza con la evaluación de las actividades y la toma de acciones pertinentes.

Gestión de soporte de los Recursos Tecnológicos e Informáticos

Proporcionar, mantener, proteger y optimizar mediante soporte técnico, los recursos tecnológicos e informáticos necesarios para el buen funcionamiento en las diferentes dependencias de la administración de la institución.

Este procedimiento inicia con la identificación de las necesidades de entrega o soporte de recursos tecnológicos e informáticos y finaliza con la evaluación de las actividades y la toma de acciones pertinentes.

Políticas

Politica 1: Política de Seguridad de la información

Su objetivo es Proteger los recursos de información del Instituto y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Mantener la Política de Seguridad de la entidad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Los funcionarios del Instituto son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la entidad, y por la Ley, a fin de protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la

información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Responsables de hacer cumplir la política de seguridad de la información en la Institución.

El Líder del **Proceso de Talento Humano** o quién desempeñe esas funciones, cumplirá la función de: notificar a todo el personal que ingresa, de sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información, y de todas las normas, procedimientos y prácticas que de ella surjan. (Inducción).

Asimismo, tendrá a su cargo la notificación de la presente política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

El Líder del **Proceso de Recursos Tecnológicos o Área de Informática** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Institución. Por otra parte, tendrá la función de velar por el cumplimiento del contrato de mantenimiento de sistemas, que contemple la inclusión de medidas de seguridad en todas las fases.

El Líder del **Proceso de Gestión Jurídica** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Institución con sus funcionarios y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.

El Líder del **Proceso de Control Interno**, es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan. La información generada por cada funcionario debe ser institucional y no de uso personal.

Politica 2: Acceso para agentes externos que garantiza la seguridad de la información.

Su objetivo es mantener la seguridad de la información y de los activos de información de la Institución cuando sean accesados por terceros. Debe controlarse permanentemente el acceso de terceros a los dispositivos de tratamiento de información de la entidad.

Cuando se requiera acceso de terceros, se debe realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que sean pertinentes. Estas medidas de control deberían definirse y aceptarse en un contrato.

Para mitigar el riesgo de acceso por terceros: se debe tener un inventario de las conexiones de red y flujos de información significativos con las respectivas ubicaciones, reportes de ingresos fallidos, reporte de ingresos sin identificar, reportes de amenazas, ataques bloqueados. (Los reportes anteriores son generados por la Consola de Antivirus – Firewall -IDS) Así mismo, se debe evaluar los riesgos y revisar los controles de seguridad de información existentes respecto a los requerimientos legales.

Los usuarios terceros tendrán acceso a los recursos informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el jefe inmediato o supervisor. En todo caso deberán firmar el acuerdo de buen uso de los recursos informáticos. La conexión entre sistemas internos de la entidad, y otros de terceros debe ser aprobada y certificada por el proceso de Recursos Tecnológicos con el fin de no comprometer la seguridad de la información interna de la entidad.

Responsables de hacer cumplir la política de acceso para agentes externos que garantiza la seguridad de la información en la Institución.

El líder del **proceso de recursos tecnológicos o área de Informática** capacitará al personal de la entidad en materia de seguridad de la información y coordinará la interacción con organismos especializados. Asimismo, junto con los funcionarios que generan la información, analizará el riesgo de los accesos de terceros a la información de la entidad y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

El Líder del **proceso de recursos tecnológicos o área de Informática** cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios, cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de

la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

Los **líderes de cada proceso** cumplirán la función de informar y autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

El líder de **Control Interno** será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

Política 3: Gestión de activos de Información.

Su objetivo es alcanzar y mantener una protección adecuada de los activos de la Institución, además garantizar que los activos de información reciban un apropiado nivel de protección. Al igual que los activos a terceros que se encuentren dentro de la infraestructura.

La entidad debe tener conocimiento preciso sobre los activos que posee, tales como:

- ✓ Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
- ✓ Recursos de software: software de aplicaciones, sistemas operativos, publicación de contenidos, etc.
- ✓ Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos externos, etc.-).
- ✓ Otros equipos: UPS

Todos los activos deben estar justificados y deben ser asignados a un funcionario.

Se deberían identificar a los responsables de cada uno de los activos y asignarles la responsabilidad de notificar acerca de algún inconveniente.

Responsables de hacer cumplir la política de Gestión de Activos en la Institución.

El líder de **Infraestructura**, el líder del **proceso de Recursos Tecnológicos o área de informátic**a y con ayuda del encargado del almacén, deberá construir un inventario actualizado de activos de información, mostrando los funcionarios y sus equipos asignados con especificación y detalle de los mismos (ubicación, número

de serie, estado, etc). El uso de códigos de barra facilita la identificación de los activos.

Política 4: Política para los aspirantes a cargos y/o contratos con la Institución.

Su objetivo es asegurar que los futuros funcionarios, contratistas y usuarios de terceras partes, entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo y/o contrato. (Inducción) Los contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberán firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad de la información en la Institución.

El comité de contratación de la Institución, es el responsable de vigilar y hacer cumplir los lineamientos expresados en los contratos, conforme a la ley y a las políticas de seguridad.

Política 4.1: Política para los funcionarios y/o contratistas activos de la Institución.

Su objetivo es asegurar que los funcionarios, contratistas y terceras personas activas en la entidad, estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben definir las responsabilidades de la dirección para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de la Institución.

Todos los empleados, los contratistas y los terceros que desempeñen funciones en la entidad, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación / inducción.

El líder del **proceso de talento humano** será el encargado de coordinar las acciones de capacitación que surjan de la presente Política, comunicar los cambios y actualizaciones que se realicen en las mismas.

El líder del **proceso de control interno** en una periodicidad de doce meses deberá revisar el material correspondiente a capacitaciones, políticas, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento, así mismo se hará una auditoria interna para determinar el cumplimiento de las políticas.

Política 4.2: Política para los funcionarios y/o contratistas que dejan o cambian de cargo en la Institución

Su objetivo es asegurar que los funcionarios, contratistas y terceras personas que salgan de la entidad o cambien de cargo lo hagan de manera organizada y segura con respecto a los activos informáticos, documentos y lineamientos de ley. Se deben establecer las responsabilidades para asegurar que la salida de la entidad del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo, entrega del cargo con todos los activos informáticos (software, documentos corporativos, equipamiento, dispositivos de computación, etc.) y se eliminen todos los derechos de acceso.

Después de que el funcionario deja de prestar sus servicios a la entidad, se compromete entregar toda la información respectiva de su trabajo realizado documental (archivos de gestión) electrónica almacenada en el equipo de cómputo o en el correo electrónico corporativo. Una vez retirado el funcionario de la Institución debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios que detecten el mal uso de la información está en la obligación de reportar el hecho al grupo de control interno.

Los funcionarios que dejen el cargo deberán hacer entrega del mismo al jefe inmediato, de igual forma, a quien corresponda deberán hacer la entrega de los bienes asignados a su nombre.

Política 5: Gestión de la provisión de servicios por terceros en la Institución

Su objetivo es Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio por terceros.

Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los contratos. La entidad mantendrá control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte.

La entidad debe verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros. La gestión de cambios en servicios provistos por terceros deberá ir inmersa y especificada en cada contrato, con el fin de asegurar el cumplimiento del mismo.

Política 6: Protección contra el código malicioso y descargables en la institución

Su objetivo es proteger la integridad del software y la información. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, gusanos, bombas lógicas, etc.

Los funcionarios de la Entidad, deben estar al tanto de los peligros de los códigos maliciosos. El **líder de recursos tecnológicos o área de Informática** debe introducir controles para evitar, detectar y eliminar los códigos maliciosos. (Antivirus, Servidor de Dominio y Firewall).

Dichos controles, deben establecer políticas y procedimientos formales que contemplen las siguientes acciones:

a) Prohibir la instalación y uso de software no autorizado por la entidad (Derecho de Propiedad Intelectual del Software).

b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde redes externas, o por cualquier otro medio señalando las medidas de protección a tomar.

c) Instalar y actualizar periódicamente software de detección y reparación de virus, actualización de base de datos de firma de virus, examinando computadoras y medios informáticos, como medida preventiva y rutinaria.

d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles.

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la entidad, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas, en especial, realizar revisión y análisis de logs.

f) Bloquear todas las descargas de software y música, con el propósito de mantener los equipos protegidos contra las amenazas de la red.

g) Concientizar a los funcionarios de la entidad para borrar archivos temporales, cookies, y registros de navegación web.

Política 7: Copias de seguridad y respaldo de la información de servidores en la Institución.

Su objetivo es mantener la integridad, disponibilidad de la información y los medios de procesamiento de la misma.

La información que es soportada por la infraestructura de tecnología informática de la institución deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad. Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

El almacenamiento de la información deberá realizarse internamente en la entidad, esto de acuerdo con la importancia de la información para la operación de la Institución.

El proceso de Recursos Tecnológicos o área de informática será el encargado del respaldo de la información así mismo como del plan (tiempos, personal, recursos) y de la metodología a utilizar para llevarlo a cabo.

- ✓ Se debe definir un esquema de respaldos y copias de seguridad back-ups, que permita tener acceso a la información en el momento que sea requerida.
- ✓ Garantizar un nivel de resguardo, seguridad física y ambiental de la información según las normas aplicadas en la entidad.
- ✓ Realizar pruebas periódicas a los medios y/o dispositivos de respaldo garantizando su eficacia y cumplimiento de los tiempos de recuperación de las operaciones.
- ✓ De ser posible contar con un respaldo extramural, en caso de algún incidente que afecte las instalaciones, este deberá ser actualizado de

manera constante (mínimo se debe contar con una actualización semanal estos tiempos depende de la importancia de la información para la continuidad de la operación de la institución), o adquirir almacenamiento en la nube para el desarrollo de esta tarea.

Política 8: Gestión de la seguridad de las redes en la Institución.

Su objetivo es asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, requiere la consideración del flujo de datos, acciones legales, monitoreo y protección. También se pueden requerir controles adicionales para proteger la información confidencial que se transmite a través de red de la entidad.

El líder del **proceso de recursos tecnológicos o área de Informática** definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la entidad, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de la red, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
- Se deberán implementar controles para evitar comunicación entre equipos de la red, si se requiere de dicha comunicación solo el proceso de recursos tecnológicos podrá dar dicha autorización.

La entidad cuenta con un firewall propio para filtrar la red contra posibles ataques o amenazas.

Política 9: Intercambio de información en la institución

Su objetivo es mantener la seguridad de la información y del software que se intercambian dentro de la entidad o con cualquier ente externo.

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información que se va a intercambiar.

Es por ello, que se deberán, establecer procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

- ✓ Protección de la información intercambiada de la intercepción, copiado, modificación.
- ✓ Detección y protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas.
- ✓ Definición del uso aceptable de las instalaciones de comunicación electrónicas.
- ✓ Acuerdos con terceros, contratista y cualquier otro usuario de no comprometer a la entidad a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación epistolar, etc. (Cumplimiento Contractual).
- ✓ Instrucción y capacitación del personal sobre las precauciones que deben tomar a la hora de transmitir información de la entidad.

Política 10: Control de accesos en la Institución

Sus objetivos son:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la Institución y otras redes públicas o privadas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Todos los funcionarios de la Institución deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas (Practicantes, funcionarios por contrato) ajenas a la entidad deberán tener autorización dada por el líder del proceso donde desempeñará sus funciones que indique la información sobre la cual puede tener acceso.

Todas las prerrogativas para el uso de los sistemas de información de la entidad deben terminar inmediatamente después de que el trabajador cese de prestar sus servicios a la entidad.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la entidad.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución y manejado de acuerdo a su clasificación como incidente o problema.

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los mismos incurre en la falla de los sistemas.

Cada funcionario de la Institución posee un nombre de usuario y contraseña para acceder al dominio, dicha configuración se hará inicialmente desde el proceso de recursos tecnológicos, allí mismo se darán los privilegios según el usuario, acceso a las unidades de red, acceso a la información, etc.

De igual manera, las aplicaciones existentes en la entidad, son de acceso restringido, según el perfil de cada funcionario podrá acceder y tendrá privilegios. La administración y mantenimientos de estas aplicaciones se darán en cumplimiento al contrato de adquisición y uso de la misma.

Todos los equipos de la entidad se encuentran conectados a un servidor de dominio, lo que resguarda la información, la configuración y lo que permite programar tareas para todos los equipos de la red.

Uso de equipos personales para el desarrollo de las labores por parte de los contratistas está permitido en la institución y estos deben contar con un antivirus licenciado y con las herramientas necesarias para el desarrollo de sus labores. La entidad no instalara software que ha licenciado en equipos que no son de la entidad, al igual que no apoya el uso de software no licenciado.

Política 11: Mantenimiento de sistemas de información en la Institución

Su objetivo definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. Definir los métodos de protección de la información crítica o sensible.

El proceso de Recursos Tecnológicos o área de informática deberá proveer la administración de los sistemas operativos y brindar soporte a los usuarios de los computadores institucionales, con los objetivos de garantizar la continuidad del funcionamiento de las máquinas y del "software" al máximo rendimiento, y facilitar su utilización a todos los procesos de la entidad.

Esta labor se desarrolla en tareas como:

- ✓ Mantenimiento de los equipos, detección y resolución de averías de manera preventiva y correctiva de acuerdo con las solicitudes que haga el usuario (Soporte- SIFI) y al plan de mantenimiento preventivo de equipos de hardware y software, de ser un problema mayor se deberá dar aviso a la empresa que provee el servicio de soporte y mantenimiento.
- ✓ Preservación de la seguridad de los sistemas y de la privacidad de los datos de usuario, incluyendo copias de seguridad periódicas Back ups.
- ✓ Evaluación de necesidades de recursos (memoria, discos, unidad central) y provisión de los mismos en su caso.
- ✓ Instalación y actualización de utilidades de software.
- ✓ Atención a usuarios (consultas, preguntas frecuentes, información general, resolución de problemas, asesoramiento).

En general, el mantenimiento de los aplicativos presentes en la Institución viene inmerso en el contrato de la adquisición de estos, por lo cual el proceso de recursos tecnológicos tiene como tarea vigilar y supervisar el cumplimiento del objeto del contrato. Los equipos que están fuera de garantía deberán entrar en proceso de soporte por la entidad y deberán entrar en proceso de dado de baja después que cumplan su vida útil (obsolescencia tecnológica).