MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DEL INSTITUTO TECNOLÓGICO DEL PUTUMAYO

Asesor SGC	Sebastián Muñoz Meléndez	Profesional apoyo SGC	**Firma**	
Vo. Bo. SGC	Ana Mirian Camacho	Profesional SGC	**Firma**	

ÍNDICE

INTRODUCCIÓN

Con la implementación del Manual de las Políticas de Seguridad y Privacidad de la Información, el INSTITUTO TECNOLOGICO DEL PUTUMAYO busca preservar sus activos de información (los servidores públicos, la información, los procesos, las tecnologías de información incluido el hardware y el software) y permitir un adecuado proceso de gestión de la información garantizando la integridad, confidencialidad y disponibilidad, así como también la continuidad de los servicios de la Institución.

Con el fortalecimiento en el procedimiento de la seguridad de la información la Institución busca establecer una cultura por parte de los servidores públicos, concientización y uso de buenas prácticas, permitiendo apoyar los procesos del Área TIC.

Además de convertirse en un compromiso por parte de la rectoría, vicerrectorías, personal administrativo y docentes acogiéndose a las Políticas emitidas en el presente manual, el Área TIC en coordinación con el área de comunicaciones se encargarán de realizar su difusión.

En el presente manual se abordarán los siguientes temas:

5.3 RESTRICCIONES.

5.4 EXCEPCIONES.

1. OBJETIVO

Establecer las políticas de seguridad de la información siguiendo todos los requisitos definidos por el SGSI y MSPI del gobierno digital, y promover la ejecución de seguridad y privacidad de la información en el Instituto Tecnológico del Putumayo.

2. ALCANCE

La política aplica para todo el Instituto Tecnológico del Putumayo enmarcada dentro de los lineamientos de Gobierno en Línea, a sus servidores públicos, contratistas, terceros, y proveedores dentro de sus áreas de responsabilidad.

3. JUSTIFICACIÓN

El Gobierno Nacional a través del Ministerio de las TIC, ha fomentado el uso de las Tecnologías de la información. Las políticas de seguridad reglamentan el comportamiento personal y profesional de los funcionarios y contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad. Y que la Institución cumpla con los requisitos legales a los cuales está obligada.

En la actualidad la Institución no cuenta con políticas de seguridad. Por lo que se requiere realizar y adoptar el presente manual para que el área de las TIC pueda realizar los ajustes y configuraciones necesarias, así como las capacitaciones a funcionarios, contratistas, estudiantes y terceros que visiten nuestras instalaciones o tengan acceso a nuestra información.

4. DEFINICIONES Y SIGLAS

4.1 DEFINCIONES

- **Activos (tecnológicos):** Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.
- **Antivirus:** un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.
- **Aplicaciones informáticas**: Es un software diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas.
- **Contraseña (clave):** Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.
- **Correo electrónico:** (También conocido como: e-mail, un término inglés derivado de electronic mail) es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación

electrónicos. Los mensajes de correo electrónico posibilitan el envío, además de texto, de cualquier tipo de documento digital (imágenes, videos, audios, etc.).

- **Copia de seguridad (backup):** Se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- **Cuenta de usuario**: Es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.
- **Datos:** Un dato es una representación simbólica (numérica, alfabéticos, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Dirección ip:** Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo (computadora, tableta, portátil, smartphone*)* que utilice el protocolo IP o *(Internet Protocol)*.
- **Estación de trabajo:** (En inglés *workstation)* es un computador de altas prestaciones destinado para trabajo técnico o científico, que facilita a los usuarios el acceso a los servidores y periféricos de la red.
- **Host (anfitrión):** Es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Comúnmente descrito como el lugar donde reside un sitio web. Un anfitrión de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de anfitrión (host name).
- **Intranet:** Red informática interna de una empresa u organismo, basada en los estándares de internet, en la que las computadoras están conectadas a uno o varios servidores web.
- **Licencia gpl:** General Public License (licencia pública general). Licencia creada por la free software foundation y orientada principalmente a los términos de distribución, modificación y uso de software libre.
- **Mensajería interna:** (También conocida en inglés como IM) es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados ya sea a una red como Internet, o datos móviles (3G, 4G, 4G, LTE, etc.) sin importar la distancia que exista entre los dos (o más) dispositivos conectados.
- **Política:** Proceso de tomar decisiones que se aplican a todos los miembros de un grupo
- **Portal web:** Un portal de internet (portal web en inglés) es un sitio web que ofrece al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a un mismo tema. Incluye: enlaces webs, buscadores, foros, documentos, aplicaciones, compra electrónica, etc.

Principalmente un portal en internet está dirigido a resolver necesidades de información específica de un tema en particular.

- **Privacidad de la información:** Es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.
- **Protocolo:** Es un sistema de reglas que permiten que dos o más Instituciones de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos
- **Puerto:** En informática, un puerto es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos. La interfaz puede ser de tipo física (hardware) o puede ser a nivel lógico o de software, en cuyo caso se usa frecuentemente el término puerto lógico.
- **Redes de comunicaciones:** Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos. Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc.).
- **Red local:** Es una red de área local (Local Area Network, LAN) los equipos informáticos están conectados a poca distancia.
- **Red wifi:** Wifi es una tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos, como computadoras, tablets, smartphones o celulares, etc, mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información.
- **Seguridad de la información**: Consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.
- **Servidores:** Es un ordenador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada: desde archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc
- **Spam:** Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales muy molestos para el usuario.

- **Virus:** Son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador.

4.2 SIGLAS

- **ITP:** Instituto Tecnológico del Putumayo
- **MSPI:** Modelo de seguridad y privacidad digital
- **TIC:** Tecnología de información y Comunicación
- **SGSI:** Sistema de gestión de la seguridad de la información

5. DOCUMENTOS DE REFERENCIA

- **Ley 527 del 18 de agosto de 1999**. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 del 14 de julio del 2000**. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- **Ley estatutaria 1266 del 31 de diciembre del 2008**. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018** "Por el cual se establecen los lineamientos generales de las políticas de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único reglamentario del sector de tecnologías de la información y comunicaciones", en el artículo 2.2.9.1.1.3, incluye la seguridad de la información entre los principios de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1 se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales, y respecto de estos últimos indica que son los elementos fundamentales de seguridad de la información, Arquitectura, y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.
- **Resolución número 000512 del 14 de marzo del 2019**. Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios del ministerio/fondo de Tecnologías de la información y las comunicaciones y se definen lineamientos frente al uso y manejo de la información.

6. CONDICIONES GENERALES

1. El incumplimiento de las instrucciones establecidas en el manual de políticas de seguridad y privacidad de la información, serán reportadas a control interno disciplinario para que tome las medidas pertinentes.
2. El documento establece una guía procedimental, dichas políticas son desplegadas y soportadas por estándares de seguridad informática, mejores prácticas, procedimientos y guías basados en los lineamientos de las normas ISO 27001.

7. DESCRIPCIÓN DEL CONTENIDO

6.1 POLÍTICAS DE SEGURIDAD RELACIONADA AL PERSONAL

6.1.1 ORGANIZACIÓN INTERNA RELACIONADA CON LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Activos relacionados: Inventario de Activos.

El documento de la política de seguridad y privacidad de la información debe ser presentado por el Vicerrector Administrativo para su revisión y aprobación ante el con comité institucional de gestión y desempeño.

La política de seguridad y privacidad de la información debe ser revisada mínimo cada año, o antes si se identifica la necesidad.

El Rector y Vicerrectores apoyarán activamente el proceso y las actividades relacionadas con la seguridad y privacidad dentro de la Institución, mediante la asignación de responsabilidades y/o recursos necesarios para su implementación.

El Área TIC´s realizará seguimiento al uso de los recursos tecnológicos, así como las proyecciones de la infraestructura tecnológica requerida, que permitan asegurar el desempeño óptimo de los sistemas de información de la Institución.

6.1.2 SERVIDORES PÚBLICOS Y CAPACITACIONES

Activos relacionados: Talento Humano.

Como parte de las obligaciones y funciones del personal y usuarios de terceras partes deben firmar y cumplir los términos y condiciones de la política de seguridad y privacidad de la información.

Todo el personal de la Entidad recibirá inducción y reinducción en la política de seguridad y privacidad de la información, en los procedimientos de gestión documental y actualización en el uso de los· equipos y el software asociado.

Todo· el personal de la Institución debe entregar a quien lo reemplace, al jefe inmediato o al supervisor del contrato los activos a su cargo (Equipos de cómputo, medios de almacenamiento, información, etc.) pertenecientes a la Institución, cuando ocurra alguna novedad del personal o al finalizar la contratación

6.1.3 INCIDENTES Y ATENCIÓN A USUARIOS

Activos relacionados: Talento Humano.

Todo incidente u ocurrencia que impacte sobre la seguridad o privacidad de la información en la Institución será reportada por los medios adoptados por la Institución al Área TIC´s.

Las solicitudes de atención realizadas por el personal de la Institución serán atendidas por el Área TIC

6.2 POLÍTICAS DE SEGURIDAD LÓGICA

Activos relacionados: Aplicaciones Informáticas, Servicios, Datos.

Las cuentas de usuario y contraseñas respectivas serán asignadas a todo el personal de la Institución por el área TIC.

Los usuarios deben ser incluidos en su grupo de trabajo correspondiente, dicho grupo debe tener sus debidas directivas de acuerdo con los permisos y accesos a los recursos de la red.

Se debe fortalecer una cultura de la aplicación de buenas prácticas y el uso adecuado de las cuentas de usuario, así como también concientizar al personal de la Institución sobre la importancia y las responsabilidades individuales que tienen con la información a su cargo. Por lo cual no es permitido que de un servidor público a otro se intercambien roles y/o cuentas de usuario para accesos a los diferentes sistemas de información.

En el caso de que se requieran cuentas públicas o compartidas, se deben proporcionar los mecanismos para su identificación.

La Unidad de Talento Humano notificará las novedades del personal de planta (retiro, ingreso, licencias, vacaciones, traslados, etc.) y del personal vinculado por prestación de servicios al Área TIC para los asuntos pertinentes (asignarle los permisos correspondientes, creación de usuario para la red e inactivación en caso de retiro. Inducción, etc.)

6.2.1 USO DE CONTRASEÑAS.

Activos relacionados: Aplicaciones Informáticas, Servicios, Datos.

Los diferentes sistemas de información que conforman la plataforma tecnológica del INSTITUTO TECNOLOGICO DEL PUTUMAYO incluyen características de restricción de contraseñas, que se aplican a la duración, la sintaxis y repetición. Se deben activar dichas restricciones y mantener una documentación de las características para las mismas.

Se debe concientizar y exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas. Entre las buenas prácticas que se recomiendan entre otras, tenemos:

- **Discreción**: Evitar los indicios como uso de mayúsculas, nombres de mascotas, familiares, fechas especiales.
- **Personal**: Las claves son de uso personal, son intransferibles. No comparta su clave, y si lo hace por necesidad de fuerza mayor, esta solicitud debe realizarla su superior en medio escrito. Cuando retome su usuario cambie de manera inmediata la clave.
- **Claves adecuadas**: En la actualidad el estándar de seguridad menciona que deben usarse claves con un tamaño mínimo de 8 caracteres, incluir mayúsculas, minúsculas, números y signos.

6.2.2 RESPONSABILIDADES DE LOS USUARIOS

Activos Relacionados: Aplicaciones Informáticas, Servicios, Datos.

Los equipos de cómputo de la Institución tienen configurado la opción de cierre de sesión después de un tiempo de inactividad, bloqueando la cuenta con contraseña al momento que requiera ausentarse.

Si un servidor público se ausenta de su puesto de trabajo, debe bloquear su equipo para que nadie haga uso de este sin su autorización, a excepción de que el jefe inmediato lo autorice.

Cada servidor público es responsable del contenido y uso del correo institucional.
Los servidores públicos implementarán buenas prácticas para el manejo de contraseñas, Los servidores públicos son responsables de proteger la información institucional con la infraestructura tecnológica proporcionada por la institución.

6.2.3 COPIAS DE SEGURIDAD

Activos relacionados: Datos

El Área TIC´S realizará y mantendrá copias de seguridad de la información institucional, que lo amerite de acuerdo con su clasificación y capacidad de la infraestructura tecnológica de la Institución. Dichas copias

cumplen con un estándar en cuanto a número, antigüedad, rotulación y lugar de almacenamiento, ya sea interno o externo de acuerdo con el procedimiento establecido.

6.2.4 RESTAURACIÓN DE LA INFORMACIÓN

Activos relacionados: Datos

Todos los sistemas de información que componen la plataforma de la Institución incluirán la documentación necesaria para garantizar la ejecución de tareas de recuperación de la información.

Cada procedimiento de restauración de información incluirá las funciones y responsabilidades del personal participante en la restauración de esta.

6.2.5 SOFTWARE DE LOS EQUIPOS DE CÓMPUTO

Activos relacionados: Aplicaciones Informáticas, Talento humano

Todos los computadores de la Institución estarán configurados y vinculados al dominio. Windows, Office y antivirus deberán estar respectivamente licenciados.

La información institucional se almacenará únicamente en la partición del disco duro o unidad lógica, destinada para tal fin.

No se permitirá el uso de dispositivos de almacenamiento USB, salvo en los casos que sea necesario.

El personal encargado del Área TIC realizará el seguimiento de los equipos de cómputo conectados a la red de la Institución.

El personal encargado del Área TIC programará y ejecutará mantenimiento preventivo al software de los equipos de cómputo conectados a la red de la Institución.

6.2.6 CAMBIOS AL SOFTWARE

Activos relacionados: Aplicaciones informáticas

Se documentarán todos los cambios o modificaciones al software.

Antes de cambiar sistemas operativos y/o aplicaciones para la Institución se realizarán las pruebas necesarias para garantizar su correcta operación.

6.2.7 SERVIDORES

Activos relacionados: Equipos informáticos.

- ✓ Los servidores que proporcionan los servicios a la Institución deberán:
- ✓ Funcionar todos los días (7 X 24) con el fin de garantizar la disponibilidad del servicio (A excepciones a las ventanas de mantenimiento programadas).
- ✓ Ser monitoreados por el personal asignado en el Área TIC.
- ✓ Recibir mantenimiento preventivo mínimo dos veces al año y recibir mantenimiento
- ✓ semestral de acuerdo con el plan de mantenimiento.
- ✓ Recibir mantenimiento anual que incluya la revisión de su configuración.
- ✓ Los Servidores de la Institución no deben ser empleados como estaciones de trabajo, ni tener instaladas aplicaciones de usuario final, tales como navegadores y clientes de correo electrónico, así como tampoco software de escritorio.
- ✓ Las excepciones a esta recomendación deben estar documentadas y aprobadas por el profesional del Área TIC en el caso de que algunos servidores requieran la instalación de software de usuario final para el funcionamiento de aplicaciones.
- ✓ Los usuarios con derechos de administrador deben tener dos cuentas distintas, una de uso administrativo y otra para tareas generales, se debe usar la cuenta con privilegios de administrador sólo cuando se tenga que realizar en los servidores, estaciones trabajo, infraestructura de la red cableada o inalámbrica, impresoras, etc, labores que requieran de estos privilegios.

6.2.8 CORREO ELECTRÓNICO

Activos relacionados: Servicios, Talento humano.

El Área TIC se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra y la información contenida en la mensajería electrónica debe tener la protección adecuada.

La gestión de contraseñas será suministrada por el servidor de dominio de la Institución de acuerdo con las directivas configuradas ya que cada cuenta se autenticará con el mismo usuario asignado a cada host.

Los mensajes enviados a través del sistema de correo electrónico de la Institución no podrán incluir contenidos ofensivos (lenguaje/imágenes vulgares, etc.).

Para la creación, modificación y desbloqueo de una cuenta de correo se debe dar cumplimiento al procedimiento correspondiente y dirigirse al funcionario líder del área correspondiente. Se deberá diligenciar el formato respectivo (medio físico o electrónico).

Los servidores públicos que usan el servicio de correo electrónico deben conocer la importancia del buen uso del mismo y concientizarse de los peligros a los que la Institución se expone por su mal uso como ataque de virus, spam, interceptación, descargar archivos adjuntos infectados, etc.

El servicio de correo electrónico, tanto interno como externo deberá ser usado única y exclusivamente para intercambio de información de interés institucional, quedando prohibido la suscripción a cualquier sitio web con el correo corporativo, a excepción de aquellos que sean estrictamente relacionados con la misión de la Institución

6.2.9 DE ACCESO A TERCEROS

Activos relacionados: Talento humano, Aplicaciones Informáticas, servicios.

Los usuarios considerados como terceros son los proveedores, personal externo o personal que tenga algún tipo de relación con la Institución.

Para garantizar el acceso al personal externo a los sistemas de la Institución se deben registrar en el Área TIC previa autorización del profesional responsable del proceso o área funcional.

La asignación de privilegios será limitada de acuerdo con tiempo y las actividades a realizarse.

Los usuarios terceros se acogerán a los acuerdos y políticas de seguridad contenidas en el presente manual y lineamientos generales de la Institución.

La red inalámbrica de acceso libre es un servicio que permite conectarse a internet a personal externo de la Institución (visitantes, proveedores) sin la necesidad de algún tipo de autenticación, esta red de invitados permitirá utilizar los servicios de Internet, en las zonas de cobertura del INSTITUTO TECNOLOGICO DEL PUTUMAYO, los usuarios invitados no tendrán acceso a la Red de la Institución ni a ningún recurso de uso privado.

6.3 POLITICAS DE REDES Y COMUNICACIONES

6.3.1 ACCESO A LA RED DE DATOS DE LA INSTITUCIÓN

Activos relacionados: Servicios, Aplicaciones informáticas

Todos los equipos que no hagan parte del inventario tecnológico del INSTITUTO TECNOLOGICO DEL PUTUMAYO deben tener instalado y actualizado un ANTIVIRUS para poder ser ingresados a la red de la Institución y de esta manera tener los servicios internos (Impresión, Mensajería interna, Internet, etc.).

No se permitirá el ingreso a la red de datos de equipos de cómputo que tengan el antivirus vencido, versión de prueba o gratuito.

Cada equipo que se requiera ingresar a la red de datos del INSTITUTO TECNOLOGICO DEL PUTUMAYO y obtener los servicios ya mencionados anteriormente debe ser revisado y registrado de acuerdo con el procedimiento vigente en el Formato de direcciones MAC por el personal encargado del Área TIC para determinar que estos no se encuentran infectados y disponen de ANTIVIRUS debidamente licenciado y actualizado.

Por ningún motivo los computadores de escritorio o portátiles, impresoras o cualquier otro dispositivo que requiera acceso a internet, se puede conectar a una red diferente de las autorizadas por el Área TIC.

6.3.2 EQUIPOS DE REDES Y CONFIGURACIÓN

Activos relacionados: Redes de comunicación, equipos informáticos.

Todos los puertos y protocolos de los dispositivos utilizados en la red, que no estén en uso serán bloqueados adecuadamente.

Al momento de diseñar, actualizar o realizar cambios en la red, se considerarán todas las medidas de seguridad y ventajas que los equipos de red estén en capacidad de proveer en lo posible utilizando equipos de alta tecnología con la asesoría del Área TIC.

Todos los dispositivos de red deberán estar correctamente salvaguardados, tomando en cuenta aspectos como ubicación, protección física y suministro eléctrico.

Se definirá un procedimiento de reemplazo de hardware y software, ya sea a través de acuerdos con proveedores (precios, tiempo de reposición, disponibilidad) o si es posible mantener respaldo en el Área de Recursos Físicos con la asesoría del Área TIC.

El Área TIC es la responsable de proporcionar el servicio de acceso remoto y las políticas de acceso y autenticación a los recursos informáticos disponibles en la Institución.

6.3.3 CONTROL DE CONTENIDOS Y USO DE INTERNET.

Todos los servidores públicos tendrán acceso a Internet para el cumplimiento de sus funciones y obligaciones.

Los servidores públicos de la Institución deben utilizar el servicio de internet de forma responsable y eficiente, este solo se debe limitar a las actividades relacionadas con las funciones del cargo.

Todos los sitios y descargas serán susceptibles de supervisión y/o bloqueo por parte del Área TIC si se consideran perjudiciales y/o improductivos para el INSTITUTO TECNOLOGICO DEL PUTUMAYO.

La infraestructura tecnológica, los equipos y los servicios utilizados para acceder a internet pertenecen al INSTITUTO TECNOLOGICO DEL PUTUMAYO y la Institución se reserva el derecho a supervisar el tráfico de internet, los sitios visitados y servicios utilizados.

Queda prohibida la instalación de aplicaciones de mensajería instantánea, sólo se permitirá los autorizados por la Institución.

Si un servidor público no está seguro de que un servicio o portal visitado constituye un uso aceptable de internet, deberá consultar con el personal del Área TIC y solicitar más información y asesoramiento al respecto

6.4 POLÍTICAS DE MANEJO DE HARDWARE Y SEGURIDAD FÍSICA

6.4.1 CONTROL DE ACCESO FÍSICO

Activos relacionados: Equipos informáticos, instalaciones, equipo auxiliar.

Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

Todos los servidores públicos portarán su carné para el ingreso a las instalaciones del INSTITUTO TECNOLOGICO DEL PUTUMAYO, así como también realizar su registro en la entrada en los medíos que disponga la Institución.

Únicamente el personal del Área TIC puede ingresar a los Centros de Datos, cuando un funcionario no autorizado o visitante requiera ingresar a los cuartos de los Centros de Datos, debe solicitar autorización mediante comunicación interna al Área TIC.

6.4.2 MANTENIMINETO Y SEGURIDAD FÍSICA

Activos relacionados: Equipos informáticos, instalaciones, redes de comunicación.

Se debe mantener actualizado el inventario de todos los equipos y dispositivos que formen parte de la infraestructura tecnológica de la Institución, debe incluir características como: fecha de adquisición, proveedor, modelo, responsable, garantía, y demás aspectos que la oficina responsable estime conveniente, además de contener la hoja de vida del estado actual del equipo y las

configuraciones o mantenimientos realizados. Es necesario que el Área de Recursos Físicos y Mantenimiento, reporte al Área TIC los nuevos ingresos de elementos de tecnología y comunicaciones para ser ingresados al sistema de seguimiento que se maneja en el área.

El Área TIC realizará el mantenimiento periódico preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física en informática, y su acondicionamiento específico, de acuerdo con el procedimiento establecido.

El Área TIC formulará y ejecutará el plan de mantenimiento preventivo de los equipos.

El cambio de lugar al interior del área de un equipo de cómputo se debe coordinar con el Área TIC y Recursos Físicos, los cuales dispondrán de las condiciones adecuadas para su traslado tales como: puntos de red, eléctrico y demás aspectos; así como también se debe actualizar en el inventario las razones de cambio y el nombre del nuevo responsable si lo hay.

Los equipos de cómputo, cables, UPS, planta eléctrica, aires acondicionados, dispositivos de almacenamiento y de comunicación inalámbrica, deben estar amparados en pólizas contra todo riesgo.

1

No está permitido el consumo de líquidos, alimentos, ni humo dentro de los centros de datos o lugares donde se encuentren los equipos de cómputo.

6.4.3 DOTACION Y PROTECCION DE LOS CENTROS DE DATOS

Activos relacionados: Equipamiento auxiliar, instalaciones.

Se deben implementar mecanismos de seguridad física como detectores de humo, medidores de temperatura, humedad, sensores de movimiento, aire acondicionado, cableado debidamente instalado, instalaciones eléctricas, sistemas de respaldo eléctricos, puertas seguras y demás elementos en las áreas donde se encuentran los equipos de comunicación y servidores propiedad de la Institución con el fin de protegerlos.

Las instalaciones de comunicaciones y eléctricas deben estar protegidas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

El Área TIC debe contar con un plano actualizado de las instalaciones de red de comunicaciones y eléctricas de la Institución.

6.4.4 CONTROL DE MEDIOS DE ALMACENAMIENTO.

Activos relacionados: Datos.

Los medios deben ser eliminados de manera segura y sin peligros (técnica, ambiental e industrialmente), usando procedimientos formales.

Los procedimientos para la manipulación y almacenamiento de información deben ser establecidos para proteger la información de la divulgación no autorizada, o un mal uso en coordinación del Área de Archivo.

Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer las copias de seguridad y el personal encargado de su protección.

6.5 POLITICAS DE SEGURIDAD LEGAL

6.5.1 LICENCIAMIENTODE SOFTWARE

Se prohíbe en el INSTITUTO TECNOLOGICO DEL PUTUMAYO software no autorizado y sin licenciamiento en los sistemas de la Institución.

El Área TIC del INSTITUTO TECNOLOGICO DEL PUTUMAYO es la única que autoriza la instalación de software en los equipos de la Institución, el cual debe contar con licencias de uso.

Se debe mantener el inventario de software (licencias) y actualizarlo cada vez que se instale nuevo software en los equipos de la Institución.

De igual forma, los terceros o contratistas que tengan equipos propios dentro de las instalaciones del INSTITUTO TECNOLOGICO DEL PUTUMAYO son los responsables por las licencias del software instalado en dichos equipos.

Se considera una falta grave que los usuarios, instalen o ejecuten cualquier tipo de programa en los equipos de la Institución conectados a la red de datos que no esté autorizado por el Área TIC.

El Área TIC establecerá un cronograma para realizar las revisiones periódicas que permita asegurar el cumplimiento de los requisitos legales y reglamentarios sobre la propiedad intelectual en la Institución.

6.5.2 GESTION DE LA CONTINUIDAD DEL NEGOCIO

El Área TIC con el apoyo de la alta dirección (Consejo Directivo, Rector y Vicerrectores) deben crear un plan de contingencias informáticas que contenga al menos los siguientes puntos:

Identificar los sucesos que pueden ocasionar interrupciones en los procesos de la Institución, así como también identificar los riesgos, y las consecuencias para la seguridad de la información

Contar con procedimientos informáticos alternos que permitan continuar con la operación de la Institución.

Tener los respaldos de información en un lugar seguro, fuera del perímetro físico donde se encuentran los equipos.

Tener el apoyo de medios magnéticos o en forma física (documentos), de los procesos necesarios para reconstruir los archivos dañados.

Se debe disponer de los planes necesarios para mantener o· recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempos requeridos, después de la interrupción o la falla de los procesos críticos para la Institución; para que toda acción correctiva se efectúe con la mínima degradación posible de los datos

Es importante tener un directorio actualizado del personal interno o externo de soporte, a los cuales se pueda llamar en el momento que se presente las fallas.

Ejecutar pruebas de la funcionalidad y revisiones periódicas del plan de acuerdo con la identificación de prioridades para asegurar su actualización y su eficacia.

6.5.3 RESTRICCIONES

Las políticas definidas anteriormente se establecen como un firme compromiso por parte de todos los servidores públicos del INSTITUTO TECNOLOGICO DEL PUTUMAYO y así mismo deben ser divulgadas a través de toda la organización siendo implementados de forma que genere confianza y garantice la funcionalidad de los sistemas de la Institución:

Se prohíbe intentar, evadir o violar la seguridad o autentificación de usuario de cualquier host, red o cuenta.

Se prohíbe a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios aún con la autorización expresa del usuario propietario de la misma.

Se prohíbe el almacenamiento, instalación, configuración o uso de software no licenciado o no autorizado o de datos no autorizados en los equipos informáticos del INSTITUTO TECNOLOGICO DEL PUTUMAYO.
Se prohíbe el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.

Se prohíbe el hurto, robo, sustracción o uso no autorizado de datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos del INSTITUTO TECNOLÓGICO DEL PUTUMAYO.

Se prohíbe el acceso, modificación o alteración no autorizada de componentes, datos o información de los activos informáticos del INSTITUTO TECNOLÓGICO DEL PUTUMAYO.
Se prohíbe el uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medíos digitales provenientes de fuentes no certificadas o de terceros, sin la previa revisión y autorización del Área TIC.

Se prohíbe el almacenamiento y reproducción de aplicaciones, programas o archivos de audio o video que no están relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.

El software y hardware, se debe verificar para asegurar que son compatibles con otros componentes del sistema.

Sé prohíbe la instalación en los equipos de la Institución de juegos y/o software diferente al instalado y autorizado por el profesional responsable del Área TIC del INSTITUTO TECNOLÓGICO DEL PUTUMAYO.

6.5.4 EXCEPCIONES

Cuando se realicen eventos, capacitaciones, talleres, conferencias o visitas de personal externo que requieran hacer uso de los servicios de la red de datos del INSTITUTO TECNOLÓGICO DEL PUTUMAYO, se podrán habilitar equipos de manera temporal por el tiempo necesario, previa solicitud del profesional del área interesada.

En el caso de ser necesario habilitar servicios restringidos (redes sociales, YouTube u otros portales), también se deberá realizar la solicitud justificada por parte del profesional de la unidad responsable del proceso. (Si aplica)

Entre las directivas de seguridad dispuestas por la Institución se encuentra configurado el firewall para restringir algunas categorías y sitios de Internet, por lo tanto, pueden existir portales que a pesar de ser inofensivos están restringidos su acceso, en este caso, los servidores públicos pueden notificar a el Área TIC para habilitarlos siempre y cuando cumplan con las políticas establecidas por la Institución.