POLITICAS DE INFRAESTRUCTURA FÍSICA Y TECNOLÓGICAS

DEFINICIÓN GENERAL

El Sistema de Gestión de Calidad de la Institución Universitaria ITSA, define a la Gestión Administrativa y la Gestión de TSI como procesos de apoyo que tienen como objetivo, apoyar la gestión misional de la institución, a través de la asignación de recursos humanos, físicos, tecnológicos y financieros adecuados para la prestación del servicio educativo.

En cumplimiento de la Misión y Política de Calidad, la Institución Universitaria ITSA, se apoya en los procesos de Infraestructura Física y Tecnológica, a través del cual se determina, proporciona y mantiene una infraestructura adecuada para garantizar las condiciones apropiadas para la realización de las actividades académicas y administrativas.

OBJETIVO

Establecer un marco de actuación para determinar, proporcionar y mantener la infraestructura adecuada de la Institución Universitaria ITSA, a través de los procesos de infraestructura física y tecnológica.

ALCANCE

Estas políticas son aplicables a todo el personal administrativo y docentes de la Institución Universitaria ITSA. Contempla la gestión de la infraestructura física y tecnológica.

RESPONSABLES

Rectoría, Vicerrectoría Administrativa y financiera, Responsable de Planta Física y Responsable de Tecnología y Sistemas de Información.

CUMPLIMIENTO

Las políticas de Infraestructura Física y Tecnológica son de obligatorio cumplimiento para todos los colaboradores, así mismo para consultores, contratistas y demás terceros que tengan una relación con la institución y acceso a las instalaciones.

POLITICA DE INFRAESTRUCTURA FISICA

En la Institución Universitaria ITSA, se conciben los recursos e infraestructura física de manera armónica en consonancia con el crecimiento de la población estudiantil, personal docente y administrativo, los adelantos tecnológicos, avances académicos con criterios de eficiencia y eficacia.

Estándares de Renovación y Actualización Física

- En el Plan Desarrollo de la institución, se definen los proyectos o programas de Recursos de Infraestructura Física, que harán parte del área estratégica.
- Los proyectos o programas de Recursos de Infraestructura Física, se ejecutan, a través del Plan de Acción Anual del Responsable de Planta Física, el cual tiene como objetivo, el seguimiento, control y evaluación al cumplimiento de las acciones resultantes de los proyectos o programas definidos en el Plan de Desarrollo.
- La estimación de los recursos necesarios para la ejecución de los proyectos o programas de infraestructura física, sustentados en el Plan de Desarrollo, se definirán en el Plan Financiero y se asignan conforme a los lineamientos definidos en la política para la asignación, ejecución y control de recursos presupuestales.
- Los proyectos o programas de Recursos de Infraestructura Física, estarán orientados al diseño, rediseño o renovación de espacios físicos modernos, funcionales, incluyentes, ambientalmente responsables, que promuevan la conservación y preservación del medio ambiente, y a la implementación de mecanismos de seguridad que contribuyan al desarrollo de las actividades académicas y administrativas de la Institución y al bienestar de la comunidad en general.
- Cuando sea necesario, el Consejo Directivo, decidirá de acuerdo a la disponibilidad presupuestal, el arrendamiento, la adquisición de terrenos, el desarrollo proyectos de construcción y la inversión en activos fijos.
- Se determinan las necesidades de infraestructura física, de acuerdo a la proyección de módulos del periodo académico siguiente, por lo cual, las necesidades de infraestructura variarán de acuerdo al crecimiento de la población estudiantil, crecimiento del personal y a las necesidades de los programas académicos.
- El Responsable de Planta Física, gestionara los requerimientos necesarios para la ejecución los proyectos de infraestructura física, como las actividades definidas en el programa de mantenimiento preventivo y correctivo, de acuerdo a lo definido en el Procedimiento de gestión del mantenimiento.

Estándares Generales

- La Institución propenderá porque en la infraestructura de la Institución se den las condiciones de aseo y seguridad apropiadas, se velará por el mantenimiento y adecuación de la planta física garantizando un ambiente propicio para el desarrollo de las actividades académicas y

administrativas y para ello se apoyará en el Programa de Mantenimiento Preventivo, en el Plan de Mantenimiento de Infraestructura y en el Plan de Limpieza.

- En el Programa de Mantenimiento Preventivo, se programarán las actividades para evitar daños, y garantizar el funcionamiento adecuado y permanente de la infraestructura de la institución, tales como:
    - Pintura
    - Mantenimiento a Aires Acondicionados
    - Mantenimiento de redes hidro Sanitarias
    - Mantenimiento de Rampas a Discapacitado
    - Jardinería
    - Mantenimiento de Silleterías
    - Impermeabilización Techos
    - Instalaciones eléctricas
    - Luminarias
    - Limpieza de tanques elevados
- En el Plan de Mantenimiento de Equipos e Infraestructura, se definen directrices que garantizan el buen funcionamiento de los equipos y la infraestructura para la prestación de los servicios en la institución, y así minimizar el riesgo originado por daños o deterioro de los equipos que brindan apoyo al proceso académico-administrativo.
- La Institución contará con un talento humano idóneo y competente, ya sea interno o externo, quien se encargará se ejecutar el Programa de Mantenimiento Preventivo y Correctivo.
- En el Plan de Limpieza, se establecen los lineamientos para el correcto desarrollo de las actividades de limpieza, con el fin de disponer de las condiciones óptimas para el efectivo desarrollo de los procesos académicos y administrativos en la institución.

POLITICA DE INFRAESTRUCTURA TECNOLOGICA

El Proceso de Tecnologías y Sistemas de Información, es considerado actualmente como un proceso de apoyo, dentro del macroproceso institucional, y el cual depende directamente de la Rectoría. Tiene como función principal el coordinar, gestionar, asesorar, evaluar y controlar las herramientas, infraestructura tecnológica y Sistemas de Información, para la automatización, el soporte y el desarrollo de los procesos académicos y administrativos de la Institución, el desarrollo de Ciencia y Tecnología, de acuerdo con las metas y objetivos institucionales.

Estándares de Renovación y Actualización Tecnológica

- En el Plan Desarrollo de la institución, se definen los proyectos o programas de Recursos de Infraestructura Tecnológica, que harán parte del área estratégica “Gestión Administrativa y Financiera”.
- La Vicerrectoría Administrativa asigna los recursos financieros de acuerdo a los lineamientos del Gestor del gasto (Rector) los cuales son ejecutados por el proceso de Tecnología y Sistemas de la información que son los encargados de la compra administración y mantenimiento de dichos recursos.
- Los proyectos o programas de Recursos de Infraestructura Tecnológica, se ejecutan, a través del Plan de Acción Anual del Responsable del proceso de Tecnologías y sistemas de la información y/o proyectos del Plan estratégico de TI - PETI, el cual tiene como objetivo el seguimiento, control y evaluación al cumplimiento de las acciones resultantes de los proyectos o programas definidos en el Plan de Desarrollo.
- Los proyectos o programas de Recursos de Infraestructura Tecnológica, están orientados a la renovación y actualización de la infraestructura de hardware que soporta los servicios institucionales, al Mejoramiento de la conectividad de internet en las sedes de la institución; a la ampliación de cobertura del servicio de conectividad inalámbrica (wifi), según necesidades académicas; y a la implementación de un sistema de gestión de la seguridad de la información basados en el estándar de seguridad de la información ISO 27001.
- Se determinan las necesidades de infraestructura tecnológica, de acuerdo a la proyección de cursos del periodo académico siguiente, por lo cual, las necesidades de infraestructura variarán de acuerdo al crecimiento de la población estudiantil, crecimiento del personal y a las necesidades de los programas académicos.

Política de Derecho de Autor

Es política de la Institución Universitaria ITSA el fomentar el uso legal de software y por tanto se prohíbe el uso y la duplicación de cualquier programa de computadora que no posea una licencia legítima, siguiendo las normas legales de derecho de autor sobre software.

Política de control de software y datos

No se permite a ningún funcionario, docente o estudiante realizar copias no autorizadas de información y/o programas originales pertenecientes a la institución; el uso de software no licenciado por ITSA en equipos de propiedad de la Institución debe estar autorizado previamente; el acceso a la información y/o datos de los sistemas de misión crítica se hará mediante el uso de perfiles de usuarios con responsabilidades y controles de acuerdo al cargo. Los datos y/o información generada por los aplicativos o programas adquiridos por ITSA deben ser utilizados sólo para fines institucionales. Toda la información registrados en equipos de propiedad y/o a cargo de ITSA, se consideran propiedad de la Institución, por lo que es responsabilidad de la persona a cargo cumplir la normatividad y leyes pertinentes.

El funcionario, contratista o docente que haga uso, genere y/o almacene información pertinente a ITSA, o sus relacionados, en el desarrollo de sus actividades o funciones asignadas, debe salvaguardar de terceros los datos, y proteger de perdida los mismos. ITSA proveerá mecanismos de protección para minimizar los riesgos por intromisión o pérdida, mediante la implementación de control de accesos a la red interna y espacios para copias de datos por parte de los usuarios que tengan equipos institucionales asignados.

Los datos almacenados en aplicativos de misión crítica, tendrán mecanismos de respaldo para que, en caso de fallos, pueda reconstruirse la información con al menos con al menos 24 horas de antigüedad.

Política de adquisición y control de hardware

La Institución Universitaria ITSA renovara, en lo posible, su planta de equipos de cómputo cada cuatro años, teniendo en cuenta el presupuesto, la vida útil de los equipos y la antigüedad u obsolescencia de los mismos, haciendo uso de las modalidades de contratación o arriendo a su alcance.

Los cambios en los equipos de cómputo de ITSA deben ser autorizados por el Proceso de Tecnologías y Sistemas de Información, así como el mantenimiento correctivo o preventivo que implique apertura solo debe realizarse por o en presencia siempre de un funcionario del grupo. El cambio en la ubicación de equipos puede hacerse solo con aprobación previa y en cualquier caso se comunicará al responsable del inventario.

Política para la adquisición de software

Todo programa de computadora que se adquiera en la Institución debe venir acompañado con las correspondientes licencias de uso o en su defecto de la autorización escrita para ello, excepto aquellos catalogados como Free u Open Source.

a) El interventor de compra de software debe asegurarse que recibe las licencias de usuario

para cada programa y/o computadora (cantidad de licencias de uso, concurrente o no), además de revisar:

- Manual de usuario (en medio magnético o físico).
- Medio en el que viene el software, si es descarga desde Internet que se posea el usuario y contraseña para realizar la descarga.
- Certificado de autenticidad en los casos que lo exijan.

b) Toda adquisición de software se realizará a proveedores legítimos, esto es, que cuenten con la aprobación del fabricante para la venta del software que se desea adquirir. En cada proceso de compra de software o aplicativos se solicitará, como requisito, la presentación de un certificado donde conste dicha autorización.
c) En caso de compra de computadoras con software preinstalado, el interventor debe asegurarse que se incluyan los originales de la licencia y los demás requisitos mencionados anteriormente.
d) Cuando se adquieran licencias de actualización "upgrade", el solicitante de la compra debe asegurarse que la cantidad no sobrepase el número de licencias en "full versión".

Política para el uso de software

El usuario del software tiene la responsabilidad de cumplir con las condiciones de uso de la licencia correspondiente a cada programa adquirido. No se permite exceder el número de copias autorizadas ya sea mediante la instalación en disco duro o a través de la red.

El retiro definitivo de cualquier software debe ser aprobado por el Responsable del Proceso de Tecnologías y Sistemas de Información, quien evidenciara el proceso y junto con el almacenista y un testigo, mediante acta que certifique la disposición final.

Si el retiro de la licencia del software establece condiciones o procedimientos particulares estos han de seguirse. Para toda clase de software, debe garantizarse que no exista ninguna copia instalada en ningún equipo, esto último debe certificarse y anexarse a la documentación de evidencia.

Los medios magnéticos tales como CD, cintas, discos u otros que contengan información sensible para la Institución, deben limpiarse mediante la neutralización de su campo magnético o hacer inservibles mediante trituración, previo a su disposición final.

Política para retirar de su uso hardware

Todo proceso relativo al retiro o baja de hardware debe tener concepto técnico respectivo y registrarse contablemente, y ser autorizado por acto administrativo de baja de bienes del representante legal de la Institución. La documentación que evidencie el retiro o disposición final se almacenará en el archivo de la Institución. La disposición final de lo retirado es autorizada

por el representante legal.

Política de seguridad informática

Es deber de cada empleado, funcionario, contratista y estudiante de ITSA asegurarse que está cumpliendo con las normas de la Institución, así como las leyes que rigen el uso de software y manejo de información y/o datos.

Cada usuario es responsable del uso que se haga con las cuentas que le han sido asignadas en la Institución, así como de la seguridad de sus contraseñas y de salvaguardar sus archivos electrónicos.

El Proceso de Tecnologías y Sistemas de Información realizará revisiones periódicas o aleatorias en los equipos a cargo de la Institución, para determinar si el software instalado cuenta con licencia o permisos de uso respectivo.

El usuario será responsable por el software y hardware instalado y los datos e información registrados en los equipos que se le hayan asignado, los programas deben estar dentro de los autorizados por el Proceso de Tecnologías y Sistemas de Información. Solo las actualizaciones de sistemas operativos o aplicativos oficialmente instalados están permitidas desde los sitios autorizados por el proveedor del mismo y esto es un deber de cada usuario que tenga equipo asignado o a cargo. Cada usuario tiene la obligación de informar de forma inmediata sobre cualquier anomalía o sospecha de violación en el equipo que se le ha dado en custodia, pues es el responsable del manejo del mismo.

Se evitará el uso no autorizado de programas rastreadores o sniffers, o que intenten vulnerar el funcionamiento y/o configuración de la red y/o equipos de cómputo; está prohibido a los estudiantes hacer uso sin autorización de los programas así clasificados.

El acceso a las salas de equipos servidores será sólo para personal del Proceso de Tecnologías y Sistemas de Información, en caso de autorizar el ingreso de personal diferente, siempre estará presente un funcionario del área. El acceso a áreas donde funcionen equipos activos de comunicación o servidores diferentes de los de misión crítica, en lo posible seguirá esta política. En lo posible, todos los sistemas de misión crítica manejarán loggins de transacciones o accesos, los que deben contener la información de trazabilidad de actividades que puedan permitir revisión.

Políticas del directorio activo para el dominio itsa.edu. local

USUARIOS

Son usuarios del directorio activo todos los estudiantes, docentes, funcionarios, contratistas y personal de apoyo que hagan uso de los Sistemas de Información y/o equipos de cómputo de

la Institución Universitaria ITSA.

EQUIPOS

Constituyen todos los equipos de cómputo institucionales utilizados como herramienta de apoyo a las actividades académicas o administrativas de los usuarios.
Los equipos y usuarios se agruparán en unidades organizativas con el fin de mejorar la administración y la aplicación de las políticas de seguridad definidas. Esta organización es la siguiente:
Dominio: itsa.edu. local

- Equipos
  - Salas y Laboratorios o Administrativos
  - Servidores
- Usuarios
  - Estudiantes
  - Docente
  - Administrativos

POLÍTICAS DE GRUPO

Las políticas de grupo definidas para el dominio itsa.edu. local son las siguientes:

- Política de fondo de pantalla estudiantes. Esta política establece automáticamente el fondo de pantalla de los equipos a los que accedan los estudiantes.
- Política de fondo de pantalla administrativos. Al igual que la anterior, establece el fondo de pantalla a los equipos donde inicie sesión el personal administrativo o docente.
- Política de contraseñas. Establece reglas para la creación de contraseñas seguras. Aplica a todas las cuentas de usuario. Política de acceso a carpetas compartidas. Define los permisos que tendrán los usuarios para acceder a carpetas y archivos compartidos. Aplica para las cuentas del personal administrativo.
- Política de control de aplicaciones estudiantes. Impide la ejecución de programas y aplicaciones no autorizadas a las cuentas de estudiantes.
- Política de control de aplicaciones administrativos. Impide la ejecución de programas y aplicaciones no autorizadas a las cuentas del personal administrativo y docente.
- Política de acceso a impresoras. Esta política es aplicable a las cuentas del personal administrativo y establece cuáles impresoras puede utilizar.
- Política de registro de impresión. Registra la cantidad de hojas impresas por el funcionario o

docente.

- Política para configuración de actualizaciones automáticas. Define cómo y cuándo se actualizarán los equipos de manera automática. Aplica para todos los equipos institucionales.

RESPONSABILIDADES

Administrador del Dominio

El Proceso de Tecnología y Sistemas de Información será el responsable de la administración y el mantenimiento del servicio de directorio activo y tendrá las siguientes funciones:

- Realizar la creación, registro, eliminación, modificación y renovación de las cuentas de dominio.
- Cambiar las contraseñas por solicitud del usuario o jefe de la dependencia.
- Establecer y aplicar políticas que mejoren el uso de los recursos de la red y garanticen la privacidad de los datos de los usuarios.
- Actualizar los datos de las cuentas.
- Realizar actualizaciones, mantenimientos y monitoreo del sistema.
- Solicitar los datos necesarios para la creación de las cuentas de usuario (nombre de la persona, tipo de vinculación, dependencia al que pertenece, nombre del cargo, email, etc.).
- Las cuentas de usuario se crearán dentro de dos (2) días hábiles, una vez recibida la solicitud.
- Creación de carpetas compartidas cuando se requiera.
- Mantenimiento de los servidores del directorio activo
- Realizar copias de seguridad periódicas de los datos de usuarios.

Líderes de Proceso / Decanos

- Solicitar la creación de las cuentas de usuario para cada persona de su dependencia.
- Informar sobre los cambios, rotación o desvinculación de personal.

Usuarios

- Aceptar y cumplir con las políticas descritas.
- Las cuentas de usuario y contraseña son únicas e intransferibles y es responsabilidad del usuario su uso adecuado.

- Entregar la cuenta a su jefe inmediato en caso de traslado o retiro.
- Resguardar las contraseñas y realizar los cambios cuando se requiera.
- Evitar instalar software no autorizado en el equipo.
- Facilitar la información a su cargo cuando sea requerida por las autoridades competentes en caso de ser requerida.
- No acceder a información confidencial sin la autorización del jefe del proceso responsable.
- No utilizar la cuenta para fines diferentes a los del servicio.
- Realizar respaldo de la información y garantizar la disponibilidad de la misma.

SERVICIOS

Generalidades

- Toda cuenta de usuario estará asociada a un grupo en particular del dominio.
- Cada proceso tendrá una carpeta compartida de 5 GB de almacenamiento disponible para todos los miembros del proceso.
- Un usuario del directorio activo puede iniciar sesión en cualquier computador de la intranet para tener acceso a sus recursos compartidos.
- De acuerdo a los permisos asignados, es posible que ciertos usuarios sólo puedan consultar información, pero no modificarla ni borrarla.
- Las impresoras se instalarán de acuerdo a los requerimientos de cada usuario.
- Se llevará un registro de la cantidad de impresiones realizadas por cada usuario del directorio activo.

Cuentas

- Las cuentas de usuarios no tendrán restricción de horario para iniciar sesión en el dominio.
- Las cuentas de directorio activo para los estudiantes se crean al momento de legalizar la matrícula académica.
- Todo trabajador nuevo vinculado a la Institución, deberá ser notificado al Proceso de Tecnologías y Sistemas de Información, con el fin de realizar la respectiva creación de la cuenta de Directorio Activo.
- El personal retirado o trasladado hacia otras dependencias también debe ser notificado al Proceso de Tecnologías y Sistemas de Información para realizar los respectivos cambios o eliminación de cuentas, roles y permisos.

- El nombre de usuario de la cuenta de directorio activo coincide con el usuario de academusoft.
- En caso de olvido de contraseña, se debe solicitar una nueva contraseña el Proceso de Tecnologías y Sistemas de Información.
- El usuario puede cambiar su contraseña en cualquier momento.
- Las contraseñas para las cuentas del personal administrativo tienen una vigencia de 3 meses, luego se debe modificar.
- Al modificar la contraseña no será posible utilizar contraseñas usadas anteriormente.
- Las contraseñas deben tener una longitud mínima de 6 caracteres y contener caracteres alfanuméricos y caracteres especiales.

Equipos

- Los equipos institucionales que utilicen los servicios de red ofrecidos por ITSA deberán ser parte del directorio activo.
- Todo equipo que ingrese al dominio contará con antivirus, inicio de sesión, actualizaciones automáticas, Fondo de pantalla institucional y acceso a los recursos de red.
- Los equipos deberán ser utilizados únicamente para fines institucionales.
- Cada equipo institucional tendrá un nombre único dentro del directorio activo.
- Los nombres de los equipos de salas y laboratorios se conformarán por el prefijo de la sede donde se encuentra el equipo, la nomenclatura del espacio físico y finalmente el número del equipo. Por ejemplo: SOL-B4-6-25 (SOL es la abreviatura de Soledad, B4-6 corresponde al Bloque B, piso 4 Sala 6 y el 25 es corresponde al número del equipo dentro de la sala).
- Los nombres de los equipos del personal administrativo, docentes y contratistas contendrá el prefijo de la sede donde se encuentra el equipo, la abreviatura o nombre del proceso al cual está vinculado y por último un numero consecutivo de acuerdo a la cantidad de equipos asignados al proceso o dependencia. Por ejemplo: BAQ- PLANEACION-03 (Corresponde al equipo 3 de Planeación ubicado en la sede de Barranquilla).
- Los nombres de los servidores estarán constituidos por nombres de animales y conformarán la granja de Servidores. Por ejemplo: Ballena.

USO INADECUADO DE LAS CUENTAS DE DOMINIO

El incumplimiento de las políticas aquí descritas o el mal uso de las cuentas de usuarios conllevará a:

- Bloqueo de la cuenta temporal o definitiva.

- El equipo de Tecnologías y Sistemas de Información, puede restringir el acceso a los servicios permitidos si evidencia algún riesgo de seguridad en las actividades realizadas por el usuario.

Política de manejo de medios

GESTIÓN DE MEDIOS REMOVIBLES

- Los medios de almacenamiento removibles como cintas, discos duros removibles, y dispositivos USB, que contengan información institucional confidencial, deben ser controlados y físicamente protegidos por el Proceso de Tecnologías y Sistemas de Información.
- La información que es almacenada en medios removibles (discos duros), que debe estar disponible por largo tiempo y la información que es almacenada en medios removibles (cintas) y que debe estar disponible por corto tiempo, es protegida y controlada adecuadamente para evitar que ésta se vea afectada por el tiempo de vida útil del medio.
- La información crítica o sensible de la Institución que se encuentra almacenada en un medio removible cuya vida útil es menor al tiempo de retención de la información establecida por la Institución, deberá respaldarse en otro medio para evitar la pérdida de información.
- Es de exclusiva responsabilidad de cada funcionario o contratista tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio.

DISPOSICIÓN DE MEDIOS REMOVIBLES

- En los medios removibles que sean reutilizados por funcionarios o contratistas se deberá realizar un borrado seguro de la información encontrada en dicho medio, antes de realizarse alguna reasignación.
- Los medios removibles que han contenido información confidencial que ya no se utilizarán, y que se dispongan para eliminar, retirar o trasladar de las instalaciones de la Institución se les debe realizar un borrado con un procedimiento seguro y documentado de la información. Para el retiro de dichos medios se debe contar con la autorización y supervisión del Proceso de Tecnologías y Sistemas de Información.
- En caso de que un medio removible o la información contenida en el mismo sufra daño, se debe informar al Proceso de Tecnologías y Sistemas de Información para valorar si el elemento se debería destruir físicamente o enviarlo a reparación.

RESPONSABILIDADES

El Proceso de Tecnología y Sistemas de Información es la responsable del manejo de medios, con el fin de ejecutar a cabalidad la tarea de preservar la confidencialidad, integridad y

disponibilidad de la información.
Todos los funcionarios, contratistas o terceros que almacenen información confidencial de la Institución Universitaria ITSA, deberán conocer y cumplir con el uso de esta política, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado del manejo de medios.

Esta política es responsabilidad de ser aprobada por las directivas de la Institución Universitaria ITSA, con el fin de garantizar la continuidad del negocio en caso de que un evento afecte la operación normal de la misma.

APLICACIÓN DE LAS POLÍTICAS DE MANEJO DE MEDIOS

- Reprimenda formal.
- Reembolso por algún daño causado.
- Terminación del contrato de trabajo o relación laboral (Basados en las disposiciones emitidas por las leyes colombianas en materia laboral).
- Demanda civil o penal.