CONSEJO ADMINISTRATIVO
RESOLUCIÓN No. 4 DE 2017

POR MEDIO DEL CUAL SE ESTALECEN LAS POLÍTICAS PARA EL USO DE LOS RECURSOS Y SERVICIOS INFORMÁTICOS

El Consejo Administrativo de la Universidad Tecnológica de Bolívar, en uso de las facultades que le confieren los Estatutos Generales, y,

CONSIDERANDO

Que es función del consejo Administrativo establecer las políticas de desarrollo administrativo, estructurar estrategias, y desarrollar acciones que busquen el cumplimiento de las políticas administrativas de la Universidad.

Que la Dirección de Tecnologías de Información y Comunicaciones de la Universidad Tecnológica de Bolívar, presentó la propuesta de las Políticas del Uso de los Recursos y Servicios Informáticos, con el objetivo de establecer los mecanismos adecuados para la utilización de los recursos computacionales e informáticos y comunicación de datos implementados al servicio de la Universidad. El cual deberá ser de obligatorio cumplimiento para toda la comunidad educativa.

Que en consecuencia de lo anterior, el Consejo Administrativo en sesión 23 de octubre de 2017, registrada en el acta de esta instancia No. 5 de 2017 aprobó las Políticas para el uso de los Recursos y Servicios Informáticos.

Por lo anterior,

RESUELVE

PRIMERO: Aprobar las Políticas para el uso de los Recursos y Servicios Informáticos de la Universidad Tecnológica de Bolívar.

SEGUNDO: El presente documento rige a partir de su aprobación el día 23 de octubre del 2017, registrada en el Acta de Consejo Administrativo No. 5 de 2017, y deroga las disposiciones que le sean contrarias.

Publíquese y cúmplase.

Dado en Cartagena de Indias, a los 23 días del mes de octubre de 2017.

Para constancia firman:

JAIME BERNAL VILLEGAS, MD. PhD.
Rector

IRINA GARCÍA CÁLIZ
Secretaria General

VICERRECTORÍA ADMINISTRATIVA

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

POLÍTICAS PARA EL USO DE LOS RECURSOS Y SERVICIOS INFORMÁTICOS

El presente documento contiene las políticas y normas que en forma general regulan la utilización que la comunidad institucional puede hacer de los recursos computacionales e informáticos y de los distintos servicios de información y comunicación de datos que operan en la Universidad Tecnológica de Bolívar.

Su observación y cumplimiento es estrictamente obligatoria para todos los usuarios, en concordancia con su perfil y privilegios de acceso que se definan en cada caso, sin perjuicio de los reglamentos y normas específicas que se definan para el uso de espacios o recursos particulares, todo ello enmarcado en los reglamentos institucionales o en la ley.

La información está organizada en secciones que facilitan la utilización del documento así:

Sección 1. Políticas y criterios generales para el uso de los recursos computacionales de la institución.

Sección 2. Políticas y criterios generales para el uso de la red de datos y los servicios de comunicaciones.

Sección 3. Políticas y criterios generales para regular el uso del correo electrónico institucional

Sección 4. Políticas y criterios generales para regular el uso de los centros digitales de impresión.

Sección 5. Política de respaldo de Información.

Sección 6. Política para Gestión de usuarios y accesos a los sistemas de información

Sección 7. Reglamento de uso de las Aulas de Informática

Este documento se revisa anualmente, y sus modificaciones son autorizadas oficialmente por el Consejo Administrativo de la institución.

1. POLÍTICAS Y CRITERIOS GENERALES PARA USO DE LOS RECURSOS COMPUTACIONALES DE LA INSTITUCIÓN.

1.1. OBJETIVO.

En esta sección se reúnen los criterios y políticas generales que se aplican en la Universidad Tecnológica de Bolívar para el uso de los distintos componentes de la plataforma computacional y de servicios de redes. Dichas políticas constituyen el marco de referencia para la toma de decisiones pertinentes a la adquisición, asignación uso y protección de dichos recursos.

1.2. DISPOSICIONES GENERALES

1.2.1 Para todos los efectos, los empleados que tengan personal a su cargo, son responsables de dar a conocer y garantizar el cumplimiento permanente de las políticas establecidas en este documento, al interior de su equipo de trabajo.

1.2.2 Las dependencias de La institución pueden agregar guías y/o procedimientos particulares complementarios a estos, siempre que no sean contrarios a las políticas institucionales aquí establecidas y previo acuerdo con la Dirección de Tecnologías de Información y Comunicaciones, de modo que se garantice su coherencia con las normas de seguridad de la información y los recursos institucionales.

1.2.3 Las políticas y reglas contenidas en este documento serán revisadas anualmente por la Dirección de Tecnologías de Información y Comunicaciones, quien presentará las eventuales propuestas de modificación al Consejo Administrativo para su aprobación.

1.2.4 Las políticas y Normas consignadas en este documento son de cumplimiento obligatorio para todos los usuarios de los servicios, conforme se establece más adelante en cada caso

1.3 POLÍTICAS GENERALES PARA EL USO DE SISTEMAS Y SERVICIOS INFORMÁTICOS

PERMISOS DE USO PARA EQUIPOS Y SERVICIOS

1.3.1 En todos los casos la utilización de los sistemas de información por parte de cualquier usuario estará limitada por los permisos y autorizaciones que la institución le haya asignado al usuario. En consecuencia, se considera un uso indebido el acceso o intento de acceso por parte de un usuario a un equipo o servicio para el que no tenga autorización expresa. Se incluyen en esta disposición los servidores, computadores personales (fijos y portátiles), cuentas de acceso (identificadores y contraseñas), archivos de datos, aplicaciones de software etc.

1.3.2 El uso de identificadores tales como códigos de usuario y claves de acceso se considera estrictamente personal. En consecuencias, Se considera uso indebido utilizar el identificador y/o la clave de otra persona, o suministrar los datos propios para que otra persona los utilice. Al recibir oficialmente los datos de acceso a un determinado sistema o recurso, el usuario asume la responsabilidad de su protección. Por tanto, compartir esa información de acceso a los sistemas o

recursos con otras personas está estrictamente prohibido y puede ser causal de suspensión o retiro de los servicios al usuario por parte de la Dirección de Tecnologías de Información, sin perjuicio de cualquier otro proceso disciplinario que eventualmente se abra en su contra por parte de las dependencias autorizadas para ello.

1.3.3 El uso de los computadores ubicados en aulas de informática, laboratorios o salas de lectura de la biblioteca, se regirá por los reglamentos particulares establecidos por los administradores de esos espacios.

1.3.4 El intento de acceso o el acceso no autorizado a segmentos restringidos de una red, sistemas de información, software de seguridad o una cuenta o espacio a nombre de otro usuario, se considera una violación de las normas de uso, independientemente de la fortaleza o debilidad que haya en la protección de tales sistemas. El hecho de que un usuario intente conectarse local o remotamente a cualquier recurso para el que no tiene autorización se considera una falta grave

PRIVACIDAD, DERECHOS DE AUTOR Y PROPIEDAD INTELECTUAL

1.3.5 Es obligación de todos los usuarios el cumplimiento de la legislación vigente acerca de la protección de la intimidad y la propiedad intelectual. Por consiguiente, ningún usuario tiene autorización para instalar productos de software en los computadores de propiedad o al servicio de la institución, ***salvo las excepciones consideradas en esta política*** y siempre y cuando se haga evidente la existencia de la respectiva licencia del software a ser instalado.

1.3.6 De igual manera, ningún usuario tiene permitido acceder a, o copiar el contenido de buzones de correo electrónicos, direcciones datos o aplicaciones de software, sin permiso expreso y evidente del propietario de los mismos y/o de la institución. La violación a esta disposición se considera falta grave.

1.3.7 Todos los productos de software que se instalen en los equipos de cómputo institucionales deberán estar respaldados con el respectivo documento o contrato de licencia que soporta tanto el uso del producto como la cantidad de instalaciones del mismo.

1.3.8 La Dirección de Tecnologías de Información tiene la responsabilidad de asegurar que la legalidad del licenciamiento de software se cumpla sin excepción en todos los equipos de cómputo de propiedad de la institución y para tal efecto deberá implementar las medidas y controles que sean necesarias, incluyendo:

a. Verificación general periódica semestral del inventario de software instalado en equipos institucionales.

b. Verificaciones esporádicas o particulares cuando se considere necesario sobre equipos específicos.

c. remoción de cualquier contenido digital (software, audio, imagen, video y similares) que no cuente con el respectivo soporte de uso y sea evidentemente requerido.

1.3.9 Anualmente La Dirección de Tecnologías de Información rendirá informe sobre el estado del licenciamiento general en los equipos de la institución, el cual servirá de

insumo para el informe de gestión en lo relacionado con el cumplimiento de lo dispuesto en la ley en materia de derechos de autor.

1.3.10 La duplicación de productos de software licenciados a nombre de la institución no está permitida, se considera uso indebido y constituye falta grave.

1.3.11 El software licenciado a nombre de la universidad, estará a disposición de todos los usuarios en función de sus necesidades, y podrá ser instalado en equipos de propiedad de la institución, siempre dentro de los términos y condiciones del contrato de licenciamiento respectivo.

1.3.12 No se instalará software licenciado a nombre de la institución en equipos de cómputo no institucionales ni de terceros, con excepción de aquellos productos cuyo contrato de licenciamiento lo permita explícitamente.

1.3.13 La instalación de productos de software en equipos institucionales es un proceso controlado a cargo de la Dirección de Tecnologías de Información sujeto a las siguientes condiciones generales:

a. Para efectos de control de acceso, sin excepción todos los equipos de cómputo de propiedad de la institución deberán estar registrados en el Dominio institucional.

b. En cada equipo de cómputo se instalarán únicamente los productos de software esenciales para el desempeño de las funciones del cargo al que sirve.

c. El servicio de instalación de productos de software será provisto por la Dirección de Tecnologías de Información a través del equipo de soporte técnico.

d. Los usuarios de carácter administrativo no tendrán privilegios de instalación de software en los equipos a su cargo.

e. En función de las necesidades específicas de las dependencias académicas se podrán otorgar privilegios para la instalación de productos de software en los equipos a su cargo a los siguientes usuarios:

   i. Personal a cargo de laboratorios y aulas de informática.
   ii. Docentes de tiempo completo, previa solicitud.
   iii. Otros usuarios previa autorización de la Vicerrectoría Administrativa.

f. No se instalarán productos de software licenciados por la institución en equipos de cómputo no institucionales, con excepción de aquellos cuyo contrato de licenciamiento lo permita de manera explícita.

g. En todos los casos, el usuario a cargo del equipo es el primer responsable del cumplimiento de la legalidad en el licenciamiento del software instalado en los equipos.

h. la Dirección de Tecnologías de Información deberá desinstalar cualquier producto de software instalado en equipos institucionales cuyo licenciamiento no sea legal. En todos los casos se informará al usuario a cargo y a la vicerrectoría administrativa.

1.3.14 La protección de la propiedad intelectual y derechos de autor se extiende a archivos físicos y digitales de imágenes, video, sonidos, y texto, los cuales no pueden ser utilizados ni incluidos en ningún soporte a nombre de la universidad, si no se cuenta con el permiso expreso del titular de los mismos, aun si dichos recursos estén disponibles en soporte digital o se puedan descargar de internet. En consecuencia, la distribución electrónica o física de cualquier tipo de material protegido, a través de los equipos y/o servicios que son propiedad de la institución se considera uso indebido de los recursos.

1.3.15 La responsabilidad de cualquier acción violatoria de la legislación vigente sobre comunicaciones, propiedad intelectual o derechos de autor, recaerá en el usuario o usuarios que la cometan, la faciliten o la encubran. Igualmente, en caso de producirse alguna sanción hacia la institución, la institución repetirá la acción sobre los responsables, incluyendo las medidas judiciales a que haya lugar según sea el caso. de igual manera, En todos los casos, el usuario que posea privilegios de administración de software es el primer responsable del cumplimiento de legalidad del software instalado en los equipos a su cargo.

1.3.16 La conexión de equipos de cómputo particulares dentro de la red de la institución podrá hacerse a través de las redes inalámbricas. la desconexión de equipos institucionales y/o el uso de puertos físicos de red ubicados en laboratorios o aulas de cómputo para conectar equipos no institucionales requiere autorización previa de la Dirección de Tecnologías de Información. Obviar esta autorización se considera uso indebido de la red y puede dar lugar a la suspensión de los servicios de red, o a procesos de orden disciplinario.

1.3.17 El uso de los equipos de cómputo ubicados en oficinas administrativas y/o de apoyo, por parte de particulares (estudiantes, visitantes u otros), no está permitido. Para ello se requiere autorización previa de la vicerrectoría Administrativa sin la cual se considera indebido y riesgoso y puede dar lugar a acciones de carácter disciplinario en contra del usuario responsable del equipo en cuestión.

SEGURIDAD DE LOS DATOS

1.3.12 La responsabilidad primaria por la protección de la información almacenada en un computador de uso personal, le corresponde al usuario a cargo del mismo quien tiene la obligación de efectuar copias periódicas de sus archivos de datos en medios de respaldo. Se considera que esta tarea debe ejecutarse con una frecuencia mínima mensual. Dependiendo de la sensibilidad o importancia de los datos, la frecuencia de las copias de seguridad podrá ser mayor. La Dirección de Tecnologías de Información y Comunicaciones debe prestar el apoyo necesario en cada caso.

1.3.13 Todo usuario es responsable por la seguridad física básica de los equipos y recursos a su cargo. Por consiguiente, es responsable por tomar todas las medidas conducentes a evitar el robo, daño o pérdida de equipos o partes de ellos. Esta responsabilidad se extiende al cuidado básico de la máquina y a la observación de buenas prácticas de seguridad y protección para prevenir y evitar accidentes con electricidad, líquidos, alimentos y bebidas, incendios etc. El usuario responderá

por cualquier deterioro o pérdida que se demuestre que es imputable a su descuido, su negligencia o su incumplimiento de lo especificado en estas políticas.

1.3.14 Los equipos y servicios computacionales están a disposición de la comunidad institucional para apoyar las labores y funciones de los usuarios. Por consiguiente, aun si están disponibles, ningún usuario tiene autorización para utilizar los recursos que son propiedad de la institución para fines diferentes a los estrictamente laborales, como el ocio, la recreación, o los asuntos puramente privados.

1.3.15 La institución cuenta con una infraestructura de seguridad y protección de los recursos, (directorio activo, antivirus institucional) los cuales deben mantenerse activos en todos los computadores. La desactivación de los recursos de protección de un computador o el reemplazo por productos de protección diferentes, requiere el aval de la Dirección de Tecnologías de Información y Comunicaciones. Por consiguiente, La introducción (activa o pasiva) de software perjudicial como los virus, "gusanos", "troyanos" o de cualquier otro tipo se considera una falta grave. En consecuencia, el usuario siempre debe acudir al servicio técnico antes de efectuar cualquier configuración de su equipo o instalar cualquier producto de software.

1.3.16 La Dirección de Tecnologías de Información y Comunicaciones tiene la responsabilidad de informar a la comunidad de usuarios acerca de la disponibilidad de nuevos productos, servicios, actualizaciones o requerimientos de seguridad y la forma de aplicarlos en cada equipo. Y es responsabilidad de cada usuario en particular aplicar dichas productos o actualizaciones una vez reciba la notificación, a menos que la misma se aplique automáticamente.

1.4 POLÍTICAS PARA ASIGNACIÓN DE EQUIPOS DE COMPUTO

1.4.1 La institución podrá asignar un computador fijo a los cargos (cuyas funciones impliquen o requieran proceso de datos, gestión de documentos, administración de comunicaciones a través de internet o acceso a los sistemas de información institucionales.

1.4.2 La asignación de equipos se revisará anualmente para contrastar las características del equipo con las necesidades funcionales del cargo y las necesidades institucionales. Como resultado, la asignación puede modificarse si se considera necesario para atender las prioridades institucionales.

1.4.3 La asignación de computadores portátiles se hará para aquellos cargos que por la naturaleza de sus funciones requieran una alta movilidad.

1.4.4 En todos los casos la asignación de computadores requiere autorización de la Vicerrectoría administrativa. Esto es independiente del origen de los recursos con que se haga la adquisición.

1.5 POLÍTICAS PARA MOVIMIENTO Y TRASLADO DE EQUIPOS

1.5.1 Los equipos de cómputo se asignan a los cargos, no a las personas. Por consiguiente, en el traslado de un empleado a otro cargo en ningún caso implica el traslado de computadores, los cuales deben permanecer disponibles en el cargo al que han sido

asignados. El empleado trasladado asumirá la dotación de tecnología asignada a su nuevo cargo.

1.5.2 El traslado de una dependencia a una nueva localización implica el traslado de TODOS los equipos de cómputo a cargo del personal que labora en ella, excepto cuando la dirección de la universidad haya autorizado la asignación de equipos nuevos.

1.5.3 Todo movimiento o reasignación de equipos de cómputo y redes requiere el aval previo de la Dirección de Servicios Administrativos y de la oficina de Activos Fijos, para garantizar el adecuado control del inventario.

1.5.4 Salvo las actividades de venta de servicios, debidamente tramitadas conforme a los procedimientos administrativos, no se prestarán equipos de cómputo para su uso fuera de la institución ni para actividades ajenas a las institucionales.

1.5.5 El traslado de equipos entre sedes, debe efectuarse únicamente por parte de personal administrativo, respetando a los procedimientos establecidos por la Vicerrectoría Administrativa

1.5.6 El movimiento de equipos de una localización a otra o entre sedes requiere autorización de la oficina de Activos Fijos. Incumplir esta disposición se considera una falta.

1.6 POLÍTICAS GENERALES PARA LA ADQUISICIÓN DE EQUIPOS DE CÓMPUTO Y SOFTWARE.

1.6.1 Toda adquisición o reemplazo de equipos de cómputo o servicios de tecnología computacional o de redes debe contar con el concepto técnico previo o el acompañamiento del Coordinador de Hardware y Software de la Dirección de Tecnologías de Información y Comunicaciones, independientemente del origen de los recursos presupuestales.

1.6.2 Las adquisiciones de equipos deben planificarse considerando las siguientes variables como mínimo:

- Cantidad de usuarios
- Obsolescencia de los equipos actuales.
- Disponibilidad de recursos

1.6.3 La proyección de adquisiciones debe estar orientada a alcanzar gradualmente una disponibilidad de un computador por cada 5 estudiantes (meta) y debe actualizarse anualmente en función de las proyecciones de crecimiento.

1.6.4 Como política general las inversiones se deben planificar privilegiando la adquisición de lotes de equipos con especificaciones estándar por nivel de cargo, sobre la adquisición de equipos individuales.

1.6.5 Como política general, no se adquirirán equipos genéricos tipo CLON.

1.6.6 Las especificaciones de todo equipo a adquirir deben ser establecidas considerando el uso previsible del equipo, y la vida útil esperada del mismo.

1.6.7 Como política general se considera que la vida útil de un computador personal, de escritorio o portátil es de tres (3) años.

1.6.8 Toda adquisición de equipos de cómputo debe incluir garantía extendida a 3 años.

1.6.9 Al terminar la vida útil de un equipo, la Dirección de Tecnologías de Información y Comunicaciones decidirá si se reemplaza, o se repotencia, según el estado, nivel de uso y disponibilidad de recursos.

1.6.10 No se adquirirán equipos re potenciados.

1.6.11 Toda adquisición de software para uso de una dependencia en particular, deberá contar con la apropiación presupuestal respectiva proveniente de la dependencia interesada. No obstante, las adquisiciones de software para uso institucional general y todas las renovaciones de licencias de software se cubrirán con el presupuesto institucional de licenciamiento a cargo de la Dirección de Tecnologías de Información y Comunicaciones. Son excepciones el software que se requiere para el desarrollo de un programa de posgrados y proyectos.

1.6.12 Las renovaciones de contratos de licenciamiento de software se harán previa evaluación del uso por parte de la Dirección de Tecnologías de Información y la dependencia usuaria.

1.6.13 Las requisiciones de software ya sea para renovación o compra por primera vez a cargo de las diferentes dependencias o programas deben llegar al departamento de compra con el visto bueno del Coordinador de Hardware y Software. donde se debe informar si el software se necesita para un periodo específico o si lo usaran de aquí en adelante para poder incluirlo en el presupuesto del año entrante.

1.6.14 El departamento de compras enviara al Coordinador de Hardware y Software las cotizaciones recibidas para su revisión, el Coordinador de Hardware y Software verificara que se encuentre en ellas lo solicitado y enviara al usuario la cotización para la elaboración de la SDP.

1.6.15 El correo de contacto que debe quedar registrado en la compra es softwareutb@unitecnologica.edu.co donde deben llegar las licencias y toda la información necesaria para la activación del software en mención

2. POLÍTICAS Y CRITERIOS GENERALES PARA LA UTILIZACIÓN DE LA RED Y LOS SERVICIOS DE COMUNICACIONES

Objetivo:

Esta sección consigna la definición explícita de las políticas y criterios que rigen la prestación, utilización control y seguridad de todos los servicios de información y de comunicaciones de datos que la Dirección de Tecnologías de Información y Comunicaciones presta a la comunidad institucional de la Universidad Tecnológica de Bolívar través de la plataforma computacional y de redes.

El propósito de esta sección es el de establecer las medidas de naturaleza técnica y administrativa que se requieren para garantizar la seguridad de la plataforma computacional institucional (equipos, servicios e información), y de las personas (usuarios) que se sirven en cualquier forma de los elementos y servicios que se ofrecen a través de ella.

2.1 INFRAESTRUCTURA DE LA RED INSTITUCIONAL DE DATOS.

La infraestructura de la red institucional de datos se entiende integrada por los siguientes elementos:

a. Cableado de datos
b. Equipos comunicaciones de naturaleza activa y pasiva, incluyendo enrutadores, concentradores, equipos de conmutación (*switches*), centros de cableado y demás equipos que intervengan en el proceso de comunicación de datos.
c. Computadores servidores
d. Computadores de los usuarios.
e. Equipo periférico.

El uso de esta infraestructura se orientará por los siguientes criterios:

2.1.1 **Servicios**. Se define como ***servicio*** toda función propia de la plataforma hardware y/o software, que satisface necesidades específicas de comunicación o procesamiento de información, tanto a nivel individual como colectivo. Todos los servicios ofrecidos a través de dicha plataforma son propiedad de La Tecnológica y pueden ser asignados o suspendidos discrecionalmente por la Institución. En todos los casos, los servicios se entienden como herramientas de trabajo, su disponibilidad tiene el carácter de institucional, no personal, y por consiguiente la Tecnológica se reserva el derecho de su administración y control en la forma que considere conveniente.

2.1.2 **Recursos de la Red.** La red institucional de datos está conformada por los siguientes recursos:

a. Recursos de Hardware:
    1. Equipos de comunicaciones y centros de cableado

2. Computadores de utilización individual, los cuales pueden ser:
    - Asignados a usuarios específicos
    - Disponibles para uso general por parte de estudiantes y profesores
3. Computadores que operan como Servidores.

b. Recursos de Software
1. Sistemas Operativos
2. Herramientas de software de propósito específico

2.1.3 **Conexión y desconexión de equipos a la red.** La conexión a la red, de cualquier equipo no perteneciente a la institución requiere autorización de la Dirección de Tecnologías de Información y Comunicaciones. Esta autorización se entiende expresa, cuando la conexión del equipo la realice un empleado de esa dependencia.

Se exceptúan las conexiones a los segmentos de red inalámbrica abiertos que están a disposición del público.

2.1.4 **Responsabilidad sobre los equipos de red.** Los equipos electrónicos que forman parte de la infraestructura de la red y que estén o sean instalados en las dependencias de la institución se entienden a cargo de la Dirección de Tecnologías de Información y Comunicaciones, En todos los casos la dependencia (el usuario) se hará responsable por el buen uso y conservación de los mismos y de avisar a la Dirección de Tecnologías de Información, en caso de fallas o descomposturas, pero no está autorizada a manipularlos física ni lógicamente.

2.1.5 **Prohibición de instalación de equipos de red particulares.** Con el fin de garantizar la seguridad y la estabilidad de la red No se permitirá la instalación en la red de datos de equipos de red de propiedad particular de los usuarios tales como concentradores (*hubs*), *routers* o *access points* inalámbricos.

2.1.6 **Continuidad de los servicios.** Los equipos de comunicaciones y servidores que formen parte de la Red Universitaria de Cómputo e Internet deberán permanecer encendidos y operando las 24 horas del día y sólo deben ser manipulados y/o apagados en los casos de mantenimiento o reemplazo, siempre por parte del personal autorizado por la Dirección de Tecnologías de Información y Comunicaciones.

2.1.7 **Manipulación de los equipos de red.** Salvo el caso de emergencias, situaciones fortuitas muy especiales o de fuerza mayor, toda intervención a la infraestructura de red, incluyendo conexión y desconexión física de los equipos, debe hacerse únicamente por parte del personal de la Dirección de Tecnologías de Información y Comunicaciones y se efectuará previa información a los usuarios afectados, de manera que se minimice el impacto de toda suspensión eventual de servicios.

2.1.8 **Adquisición de equipos de comunicaciones.** La adquisición de nuevos equipos de cómputo y comunicaciones, se hará siempre tomando en cuenta como mínimo, factores de calidad, compatibilidad, desarrollo tecnológico, funcionalidad y especificaciones del equipo, garantía, soporte técnico y precio. Preferiblemente se debe contar con un mínimo de dos ofertas de proveedores diferentes, las cuales deben ser calificadas conforme a un sistema de puntuación previamente definido, que permita recomendar la mejor oferta.

2.2 USUARIOS.

2.2.1 Son usuarios de los servicios de información y comunicaciones las siguientes personas:

2.2.1.1 Usuarios académicos. Son los siguientes:
1. Estudiantes. De pregrado, posgrado y educación permanente.
2. Docentes. De tiempo completo y de cátedra, y profesores visitantes.

2.2.1.2 Usuarios administrativos. Son los siguientes:
1. Los empleados.
2. El revisor fiscal.

2.2.1.3 Usuarios especiales. Son los siguientes:
1. Los Egresados.
2. Los miembros del Consejo Superior.
3. Toda persona externa a la institución, a quien la Dirección General le asigne la calidad de tal.

2.2.2 **Privilegios de Usuarios.** La Dirección de Tecnologías de Información y Comunicaciones podrá asignar a cada usuario o grupo de usuarios un conjunto de privilegios de acceso y utilización de recursos que serán iguales para todos los usuarios adscritos a un perfil determinado. Toda modificación de privilegios de usuario requerirá la autorización del directivo a cargo de la dependencia a la que está adscrito el solicitante y será atendida en tanto no comprometa las políticas de seguridad y control.

2.2.3 **Derechos de los usuarios.** Son derechos de los usuarios de la red, los siguientes:

a) Todo usuario tiene derecho a que se le asigne acceso a los servicios de red, en función de sus necesidades laborales. La asignación o restricción de cualquier servicio se hará previa autorización del superior inmediato.

b) Todo usuario tiene derecho a recibir el soporte técnico necesario para corregir los problemas que se presenten como consecuencia de malfuncionamiento de la red, o de los equipos.

c) Todo usuario tiene derecho a solicitar que se le cancele o modifique la configuración de alguno de los servicios de red que tenga asignados. La modificación de servicios dependerá de la viabilidad técnica y de que se cuente con las autorizaciones respectivas.

d) Todo usuario que no cuente con los recursos necesarios para ello, tiene derecho a recibir apoyo de la Dirección de Tecnologías de Información y Comunicaciones

para la creación de copias de seguridad de su información. No obstante, es responsabilidad del usuario solicitar el servicio con la frecuencia necesaria.

e) El acceso a la red institucional desde localizaciones externas se considera un servicio, no un derecho. La asignación de este servicio dependerá de las políticas que al respecto establezca la Dirección General.

2.2.4 **Deberes y obligaciones de los usuarios.** Todos los usuarios de la red, tienen los siguientes deberes y obligaciones:

a) Mantener copias de seguridad de sus datos, para prevenir pérdidas de información por falla en los equipos a su cargo. Las copias de seguridad de las bases de datos institucionales son responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones y se ejecutan conforme al procedimiento establecido.

b) Mantener la privacidad de sus datos de acceso a los servicios tales como las claves de acceso, las cuales se entienden como de uso privado. Así mismo, debe seguir las recomendaciones que en este mismo documento se establecen para el manejo de sus claves de acceso.

c) Hacer una utilización razonable de los servicios, dentro de los límites establecidos por los reglamentos y los procedimientos.

d) Administrar eficientemente el espacio de almacenamiento de información asignado a su nombre. Esta obligación incluye la prohibición de almacenar cualquier clase de información o material pirata, ilegal o protegido por derechos de autor o propiedad intelectual sin el permiso expreso del autor o sin la debida licencia de utilización.

e) Cerrar la sesión en que encuentra trabajando, al terminar de trabajar, ya sea de correo o cualquier aplicación interna, como medida de prevención para evitar que usuarios inescrupulosos utilicen su identificación.

f) Informar a la Dirección de Tecnologías de Información y Comunicaciones, cuando por alguna razón, encuentre una sesión de otro usuario abierta, en cualquier equipo y el mismo esté desatendido. Adicionalmente, el usuario debe cerrarla y no hacer uso de ella

g) Solicitar, en caso de pérdida u olvido de su clave de acceso, la cancelación de la misma y la expedición de una nueva por parte de la Dirección de Tecnologías de Información y Comunicaciones.

h) Abstenerse de utilizar equipos y servicios para visita de sitios pornográficos o que trafican con material ilegal, y en general de sitios que no estén relacionados con las labores desempeñadas por el usuario. Igualmente, abstenerse de enviar a través de los servicios institucionales materiales que puedan ser considerados obscenos u ofensivos

i) Abstenerse de utilizar los servicios y recursos para el desarrollo de actividades no relacionadas con sus funciones, o para tareas ajenas a la institución.

j) Abstenerse de intentar violar o entrar a otras redes sin autorización.

k) Abstenerse de la publicación, envío, o distribución o difundir cualquier información incorrecta, difamatoria, infractora, obscena, ilegal o indecente, o para enviar archivos que contengan virus, caballos de Troya, bombas de tiempo, gusanos, *cancelbots*, archivos corruptos, o cualquier otro software de carácter malicioso o dañino, y/o programas similares que puedan dañar el funcionamiento del computador, de la red o de cualquier recurso computacional o informático.

l) Eliminar de su equipo todo contenido susceptible de ser catalogado como sospechoso.

m) Abstenerse de manipular la configuración de direcciones, nombres de equipos y/o de dominios, DNS y demás parámetros de red, sin la debida autorización de la Dirección de Tecnologías de Información y Comunicaciones.

n) Abstenerse de copiar y/o distribuir software cuya licencia lo prohíba.

2.2.5 **Sanciones.** El incumplimiento de cualquiera de los deberes y obligaciones por parte del usuario puede dar lugar a la restricción o cancelación de los servicios en forma temporal o permanente, dependiendo de la gravedad de la contravención, y puede ser causal de un proceso disciplinario en contra del responsable.

2.3 CLAVES DE ACCESO

2.3.1 **Identificación de los usuarios.** En todos los casos en que sea necesaria la identificación del usuario para acceder a un servicio, esta identificación deberá estar compuesta por un nombre de usuario (*user id*) y una palabra clave de acceso (*password*). Tanto el nombre de usuario y la palabra clave son datos de carácter privado del usuario, y su manejo confidencial es su responsabilidad exclusiva.

2.3.2 **Tipos de Claves.** Dependiendo del tipo de recurso o servicio que protegen se definen dos tipos de clave: Claves de usuario y Claves de súper usuario. Las claves de usuario restringen el acceso a un servicio o recurso por parte del usuario propietario del mismo, mientras que las Claves de súper usuario son de uso privativo del administrador de un servicio o recurso.

2.3.3 **Definición y uso de las Claves de súper usuario.** Las claves de súper usuario se asignan para proteger el acceso a servidores, y se manejarán conforme al siguiente procedimiento y recomendaciones:

- Para los servidores institucionales las claves de súper usuario serán definidas por el Jefe de Hardware y Tecnología.
- Para los servidores ubicados en dependencias específicas, la clave de súper usuario será definida por el jefe de la dependencia.
- La asignación de claves debe hacerse de acuerdo con los siguientes criterios:
  - Toda clave de súper usuario debe ser cambiadas con una frecuencia mensual.
  - Toda clave de súper usuario debe ser conocida únicamente por el administrador del equipo y el Director de Servicios Informáticos.

- Se debe mantener una copia de todas las claves de súper usuario en la caja fuerte institucional, en sobre sellado cuyo manejo es responsabilidad exclusiva del Director de Servicios Informáticos.

2.3.4 **Definición y uso de claves para usuarios no administradores.** En términos generales, el uso y administración de las claves de usuarios no administradores es potestativo de cada usuario, sujeto a las siguientes consideraciones:

1. Toda clave deberá tener una longitud mínima de 8 caracteres, combinando letras y dígitos y al menos un carácter en mayúsculas. Además, deben tenerse en cuenta las siguientes recomendaciones al definir la clave:
   a. No utilizar el nombre de usuario (*user-id*) con el que se identifica el buzón.
   b. No utilizar datos de naturaleza familiar como el nombre o apellido de su cónyuge o de sus hijos, ni una combinación de sus iniciales, ni una rotación o transposición de sus caracteres.
   c. No utilizar datos que sean fácilmente asociables con el usuario, tales como números de teléfono, de cédula, dirección de residencia, fechas de cumpleaños o aniversarios, identificación del vehículo o similares.
   d. No utilizar una palabra compuesta por repeticiones de un solo dígito o letras. Por ejemplo: "aaaaaa"
   e. No utilizar una palabra que resulte de cualquier rotación o transposición de los caracteres del *user-id* y/o de la clave anterior.
2. La clave inicial será generada automáticamente en el momento de definir la identificación del usuario, por parte de la Dirección de Tecnologías de Información y Comunicaciones.
3. Los usuarios tienen la obligación de cambiar periódicamente su clave, para garantizar la privacidad de su información. Esta actividad preferiblemente debe efectuarse con una frecuencia mensual. Todos los sistemas de información exigirán el reemplazo de la clave al vencer el término máximo establecido en ellos. Si se vence el término máximo, el acceso del usuario se bloqueará automáticamente
4. Obligatoriamente el usuario debe cambiar su clave de acceso inicial en la primera vez que ingrese al servicio o sistema en cuestión.
5. Cuando se detecten 3 intentos de acceso con una clave errada, el sistema debe bloquear el acceso del usuario.

2.4 SERVICIOS DE LA RED

2.4.1 **Definición**. Se define como Servicio de Red toda actividad de comunicación o intercambio de datos, oficialmente autorizada por la institución, sujeta a un formato específico y normalizada con un protocolo de comunicaciones estandarizado, susceptible de ser utilizado sobre la red de datos institucional, como son el correo electrónico, la navegación a través de páginas web, los servicios de mensajería de texto, voz e imagen, conferencias entre usuarios la transferencia electrónica de

archivos (FTP) y que están a disposición de los usuarios como herramientas de trabajo.

2.4.2 **Usos del servicio.** Los servicios de red disponibles en la institución se entienden como un recurso de naturaleza institucional y por consiguiente están a disposición de los usuarios para mejorar las condiciones de desempeño laboral y académico de los usuarios. Su propósito es el de facilitar las siguientes actividades de los usuarios:

a) Intercambio de información con terceros.
b) Actividades de capacitación, investigación o proyección social
c) Intercambio de información con toda la comunidad académica interna y externa.
d) Búsqueda de información en Internet.

2.4.3 **Controles a la información.** En términos Generales la Dirección de Tecnologías de Información y Comunicaciones no ejercerá controles especiales a la información que fluye por la red, con excepción de aquellos orientados a mantener la seguridad de la red. Por consiguiente, dicha información será responsabilidad del usuario que la genere. Con el fin de garantizar la seguridad de la información, la Dirección de Tecnologías de Información y Comunicaciones podrá controlar los siguientes parámetros de utilización:

a) Registro de todos los accesos que los usuarios realicen a los servicios y equipos de la red.
b) Registro de los sitios visitados por los usuarios en Internet.
c) Registro de la utilización de recursos especiales como centros de impresión y servidores de archivos.
d) Cifrado de información en tránsito.

2.4.4 **Disponibilidad de los servicios.** Todo servicio de red debe estar disponible las 24 horas al día, todos los días de la semana, salvo en los casos de mantenimiento que se avisarán con una anticipación mínima de dos (2) días, o de situaciones de fuerza mayor o caso fortuito.

3. POLÍTICAS Y CRITERIOS GENERALES PARA REGULAR EL USO DEL CORREO ELECTRÓNICO INSTITUCIONAL.

En esta sección se describen las políticas y criterios generales que regulan la prestación y el uso del servicio de correo electrónico institucional para los usuarios de la Universidad Tecnológica de Bolívar.

3.1 Definición.

3.1.1 Se entiende por **cuenta de correo electrónico** la asignación por parte de la Universidad de:

a. una dirección electrónica con la forma nombre@unitecnologica.edu.co

b. Un buzón (espacio en disco) para almacenar los mensajes, el cual tendrá una capacidad máxima.

c. Una palabra clave o *password* inicial, para acceder de manera privada a la cuenta.

d. La posibilidad de enviar y recibir mensajes dentro de la Universidad y hacia Internet utilizando la dirección electrónica asignada.

No forman parte de la cuenta de correo electrónico el equipo de cómputo para consultarla, ni el software cliente de correo electrónico que utilice el usuario.

3.1.2 Toda persona vinculada a la institución como docente o como empleado, puede solicitar una cuenta de correo electrónico en el servidor institucional. La institución se reserva el derecho de asignar la cuenta solicitada, previa evaluación de la necesidad expresada por el solicitante y la disponibilidad de recursos existente. En caso de que se le autorice, dicha cuenta será mantenida mientras dure la vinculación del solicitante con la institución, excepto en casos de fuerza mayor o mala utilización que eventualmente puedan causar la suspensión o cancelación de la misma. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor.

3.1.3 Los usuarios estudiantes, al matricularse adquieren el derecho a un buzón de correo electrónico en la plataforma utbvirtual.edu.co cuyas características funcionales son determinadas por el acuerdo de utilización proporcionado por gmail.com. Tendrán acceso a este servicio todos los estudiantes matriculados regularmente.

3.1.4 El correo electrónico se define como un servicio de naturaleza institucional propiedad de la Universidad. En consecuencia, ella podrá implementar medidas de control y monitoreo al uso de este servicio, para asegurar su estabilidad y su seguridad. La Dirección de Tecnologías de Información y Comunicaciones es la dependencia encargada de la administración de este servicio y tendrá la potestad para monitorear y controlar el tráfico de mensajes con el fin de evitar riesgos para los usuarios y para la institución.

3.2 Identificación

3.2.1 Con el fin de garantizar que la identificación del usuario en la dirección de correo electrónico sea única, los nombres de las cuentas de correo electrónico se construirán de acuerdo a la siguiente regla:

- Para Empleados y docentes: Se tomará la inicial del primer nombre seguida de las letras del primer apellido. En caso de que un nuevo nombre coincida con el de un usuario ya existente, se acordará un nombre distinto al nuevo usuario. De igual manera, en casos en que la construcción resulte incómoda, compleja, o difícil de recordar, la Dirección de Tecnologías de Información y Comunicaciones acordará un nuevo nombre con el interesado.
- Para estudiantes: Se constituirá un identificador de ocho caracteres conformado por la letra "T" seguida de los siete dígitos del código estudiantil. El nombre de dominio para estas cuentas es @utbvirtual.edu.co

3.3. Criterios de utilización y usos aceptables

3.3.1 Se asignará solamente una cuenta por cada usuario. Las cuentas para proyectos especiales o grupos, se asignarán previo acuerdo entre la Dirección de Tecnologías de Información y Comunicaciones y la dependencia solicitante. Toda solicitud de apertura de cuentas de correo electrónico debe hacerse por escrito.

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

3.3.3 Los usuarios del servicio de correo de la Universidad podrán recibir y enviar mensajes desde programas (clientes) de correo que utilicen los protocolos SMTP, POP e IMAP ó a través del *webmail* institucional. El servicio SMTP no se permite cuando se solicita desde localizaciones externas a la red, por razones de seguridad, para evitar que el servidor sea utilizado para el envío de correo no deseado por parte de terceros.

3.3.4 Todas las cuentas pertenecientes a estudiantes, grupos de estudiantes, grupos informales, proyectos especiales u otros similares tendrán una vigencia en el tiempo. Una vez vencida esta vigencia, el interesado deberá renovar su solicitud ante la Dirección de Tecnologías de Información y Comunicaciones para evitar la cancelación de la cuenta.

3.3.5 El usuario es el único responsable por el **buen uso** de su cuenta de correo electrónico. En consecuencia, al aceptar el buzón otorgado por la universidad, el usuario se compromete a:

- No enviar, contestar o redirigir mensajes de correo que constituyan cadenas o campañas de naturaleza política, religiosa, comercial o de cualquier otra índole que sea ajena a los propósitos estrictamente institucionales.
- No utilizar la cuenta para el envío o reenvío de mensajes SPAM o HOAX, o con contenido que pueda resultar ofensivo o dañino para otros usuarios (virus, pornografía), o que sea contrario a las políticas y normas institucionales.
- Evitar el envío de mensajes masivos sucesivos o repetitivos, a grupos grandes de direcciones los cuales pueden ser catalogados como SPAM (correo no deseado), causando la denegación del servicio por otras redes.
- Evitar el envío desde su buzón de materiales (textos, software, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En

especial debe evitar la distribución de software que requiera licencia, claves ilegales de software, programas para romper licencias (crackers), y en general cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario responsable, sin perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.

- Utilizar su cuenta únicamente para fines académicos y/o de investigación, o para los estrictamente relacionados con las actividades propias de su trabajo.
- No utilizar el buzón o el servicio de correo electrónico institucional para fines comerciales diferentes a los que sean relativos al interés institucional.
- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red institucional.
- Permitir la inspección de su buzón de correo en los casos en que, por necesidad o riesgo tecnológico, la Dirección de Tecnologías de Información y Comunicaciones lo considere indispensable, para lo cual esta dependencia previamente informará al usuario de la situación.
- No utilizar el servicio de correo para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.
- No Utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.
- Utilizar siempre un lenguaje apropiado en sus comunicaciones.
- Mantener copias de respaldo de sus archivos y de sus carpetas de mensajes de correo en su computador personal. En consecuencia, se entenderá, que el contenido del buzón de correo está integrado únicamente por archivos "en tránsito" y no almacenados permanentemente allí.
- Mantener activo y permanentemente actualizado en su computador personal el software de protección contra virus que revise el contenido de los mensajes entrantes y salientes. La actualización del software antivirus debe hacerse como mínimo semanalmente y es una responsabilidad de cada usuario.
- Evitar el envío de respuestas con copia A TODOS los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios salvo cuando se trate de una respuesta que por su naturaleza y/o contenido, necesariamente requiera ser conocida por todos ellos.

3.3.6 Los mensajes enviados hacia listas de correo o grupos de discusión, por los miembros de la comunidad universitaria y que utilicen las direcciones de correo de la Universidad deben contener un párrafo que exprese que "las opiniones expresadas en este mensaje son estrictamente personales y no necesariamente corresponden a la posición oficial de la Universidad Tecnológica de Bolívar".

3.3.7 La Institución se reserva el derecho de enviar al usuario toda información que considere necesaria o pertinente para garantizar un adecuado flujo de información interna, dado que el buzón se considera un medio de comunicación institucional. En ningún caso la información oficial que la institución entregue a sus usuarios a través del correo electrónico puede catalogarse como Correo No deseado.

3.3.8 La Dirección de Tecnologías de Información y Comunicaciones revisará los archivos anexos los a mensajes de correo electrónico, para verificar la ausencia de virus y/o de SPAM. La entrega de todo mensaje a su destinatario final estará sujeta a que esta comprobación sea exitosa. Por su parte el usuario deberá mantener activo y actualizado un software antivirus en su computador, como complemento.

3.3.9 La Dirección de Tecnologías de Información y Comunicaciones informática se reserva el derecho de dar de baja las cuentas que no tengan ninguna actividad por un período continuo de 30 días calendario. En estos casos, el nombre de la cuenta quedará reservado para el mismo usuario como mínimo durante el tiempo restante hasta la finalización del período académico.

3.3.10 Por intermedio de La Dirección de Tecnologías de Información y Comunicaciones la Institución se reserva derecho de monitorear y establecer controles adicionales a las cuentas que presenten un comportamiento sospechoso o que en forma comprobada que pongan en riesgo la seguridad de la red institucional.

3.3.11 El incumplimiento por parte del usuario de una o más de las obligaciones arriba descritas, puede ocasionar la suspensión y posterior baja del sistema de su cuenta de correo electrónico. Esta medida puede tomarse incluso con carácter preventivo y sin aviso previo, en los casos en que se detecte alguna actividad ilegal o de peligro inminente, originada en el buzón del usuario.

3.4. Correos en períodos de vacaciones

3.3.12 El departamento de recursos humanos solicitará a la dirección de TICs la inactivación temporal de los correos electrónicos de los empleados que disfrutaren sus vacaciones. La inactivación del correo electrónico se hace al inicio del período y se reactivará solamente cuando finalice su período de receso.

3.3.13 El empleado puede especificar el listado de las personas a las cuales quiere redireccionar los correos electrónicos que recibiere su cuenta durante el período vacacional. Durante este período, su buzón está inactivo, sigue recibiendo correos electrónicos y las personas que especificó en el redireccionamiento van a recibir copias de los mismos.

3.3.14 El empleado puede especificar el mensaje de contestación automática que se genera durante el período vacacional, y que podría contener indicaciones de a quién acudir durante su ausencia.

4. POLÍTICAS Y CRITERIOS GENERALES PARA REGULAR EL USO DE LOS CENTROS DIGITALES DE IMPRESIÓN.

Esta sección consigna las políticas y criterios generales para el uso de los centros digitales de impresión y fotocopiado de propiedad de la institución.

4.1 Usuarios y cupos

4.1.1 Todos los usuarios administrativos y docentes pueden solicitar la asignación de una cuenta de impresión y fotocopiado. La asignación de dicha cuenta deberá estar respaldada por la respectiva asignación presupuestal.

4.1.2 A cada usuario se le asignará una identificación y una clave de acceso en un equipo específico de impresión, conforme a distribución que organizará la Vicerrectoría Administrativa. Todos los usuarios deberán respetar esa asignación.

4.1.3 A cada usuario registrado en los equipos, se le asignará un cupo máximo mensual de impresiones y copias. Agotado ese cupo, el interesado deberá gestionar la ampliación del mismo ante la Dirección de Servicios Administrativos, a través del directivo que está a cargo de su dependencia. La ampliación del cupo no es automática ni obligatoria y estará sujeta a las políticas de restricción de gasto.

4.2 Criterios de Uso

4.2.1 Todos los trabajos institucionales de impresión y copiado **deben ser dirigidos por defecto** hacia estos equipos. El uso de servicios externos solo se autorizará en caso de emergencia o cuando se trate de trabajos especializados no realizables en los equipos institucionales o por razones de costo en función del volumen de documentos a imprimir.

4.2.2 El uso de impresoras locales de escritorio está definido solamente como medida de contingencia y solo para algunas dependencias autorizadas por la Vicerrectoría Administrativa en función de la conveniencia institucional. A estas dependencias, se les limitará el suministro de elementos consumibles para estas impresoras locales conforme a las políticas de restricción de gasto mensual.

4.2.3 En todos los casos el usuario deberá utilizar la modalidad de impresión protegida, toda vez que es su responsabilidad la de preservar la privacidad del contenido de sus trabajos de impresión.

4.2.4 Los equipos de impresión y fotocopiado son para uso exclusivo de la institución. Por consiguiente, no está autorizada la impresión o el copiado de materiales privados de los empleados.

4.2.5 Siempre que la naturaleza del trabajo lo permita, es obligación del empleado utilizar la modalidad de **impresión o fotocopiado a doble cara,** con el fin de ahorrar papel.

4.2.6 Al terminar un trabajo de impresión o copiado, Todo usuario tiene la obligación de verificar que la sesión de trabajo con la máquina quede cerrada.

4.2.7 La utilización indebida del servicio de impresión puede dar lugar al retiro del servicio al usuario por parte de la Dirección de Tecnologías de Información y comunicaciones

4.3 Administración y control

4.3.1 **Cada centro de impresión está asignado a un empleado que lo administra, y se encarga de supervisar su funcionamiento en general y de alimentar las bandejas con los distintos tipos de papel que la máquina maneja. Ninguna otra persona está autorizada** a manipular las bandejas de alimentación de la impresora ni el reemplazo de partes de la misma. En caso de que se requiera alguna acción especial de mantenimiento, se debe llamar al servicio de Soporte que ofrece la Dirección de Tecnologías de Información y Comunicaciones.

4.3.2 Ninguna persona diferente a los miembros del equipo de soporte a usuarios, está autorizada para mover, abrir, conectar, desconectar o manipular los equipos de impresión o sus componentes.

5. POLÍTICAS DE RESPALDO DE INFORMACIÓN

Objetivo: Con la finalidad de garantizar la operatividad ininterrumpida de los distintos sistemas de información que ofrece la institución es necesario fijar una política de respaldo de la Información que haga posible la recuperación rápida y completa del mayor volumen de información, en caso de contingencia.

5.1. Niveles de importancia de la información.

Se definen los siguientes niveles de importancia de la información:

- Nivel Crítico:
  - información institucional almacenada en las bases de datos asociadas a los sistemas de información institucionales.
- Nivel Alto:
  - Documentos de naturaleza estratégica
  - Documentos de naturaleza confidencial
  - Información almacenada en buzones de correos
  - Respaldos de sitios web.
  - información almacenada en los equipos personales de empleados del nivel directivo.
- Nivel Bajo: Archivos de trabajo de los usuarios que no clasifiquen en las dos categorías anteriores

5.2. Periodicidad y almacenamiento.

Nivel Crítico:

- Responsable: Jefe de Análisis y Diseño o quien el delegue.
- Frecuencia: Este respaldo debe ser realizado semanalmente y deberá incluir todas las bases de datos operativas de la institución. En épocas de alta transaccionalidad como en los períodos de matrícula, deberá efectuarse diariamente.
- Almacenamiento: Se almacenará la información en Cintas Magnéticas que se distribuyen por triplicado así: ejemplar 1: Caja Fuerte ejemplar 2: Secretaria General ejemplar 3: Dirección de Tecnologías de Información.

Nivel Alto:

- Responsable:
  - Información almacenada en servidores: Jefe de Hardware y Tecnología o quien el delegue
  - Información de usuarios de nivel directivo: Coordinador de Soporte a usuarios.
- Frecuencia: Se ejecutarán las copias de respaldo conforme al calendario que garantice una frecuencia mínima de respaldo mensual o cada vez que el usuario lo solicite.
- Almacenamiento: La información recopilada de cada usuario se almacenará en medios ópticos (CD / DVD) en un ejemplar cuya custodia estará bajo la responsabilidad del usuario

Nivel Bajo:

- Responsable: Coordinador de Soporte a usuarios.

- Frecuencia: mensual
- Almacenamiento: La información recopilada de cada usuario se almacenará en medios ópticos (CD / DVD) en un ejemplar cuya custodia estará bajo la responsabilidad del usuario.

6. POLÍTICA PARA LA GESTIÓN DE USUARIOS Y ACCESOS A LOS SISTEMAS DE INFORMACIÓN INSTITUCIONALES

6.1. OBJETIVO

Establecer las responsabilidades y los procedimientos aplicables para las acciones de creación, modificación, inhabilitación y/o eliminación de las cuentas de usuario para los sistemas de información institucionales, con el fin de minimizar los riesgos de pérdida de información.

6.2. ALCANCE

La presente política aplica para todas las cuentas de usuario de todos los sistemas de información de propiedad de la institución.

6.3. ELEMENTOS DE LA POLÍTICA DE GESTIÓN DE USUARIOS

6.3.1. Criterios generales

- La Institución podrá entregar cuentas de acceso a los sistemas de información, a aquellas personas que posean vinculación laboral con la institución, administrativa o docente, en concordancia con las funciones establecidas para cada el cargo que ocupan en el manual de funciones y a los usuarios que posean la calidad de estudiante, de conformidad con lo establecido en los reglamentos vigentes.

- La Institución propenderá porque la cantidad de cuentas de acceso a disposición de los usuarios existentes sea la mínima necesaria.

- Toda persona que requiera para el correcto desempeño de sus funciones acceder a un sistema de información institucional deberá poseer una cuenta de usuario, la cual se considera personal, intransferible y de uso exclusivo. El titular de la misma debe hacerse responsable por su uso adecuado y está obligado a tomar las medidas de seguridad necesarias para mantener la confidencialidad de sus credenciales de acceso. De Igual manera, en todos los casos el usuario titular de una cuenta de acceso es el responsable de las transacciones que se ejecuten con su cuenta durante el período de vigencia de la misma.

- Por Cada sistema de información habrá un usuario propietario, que se encarga de supervisar y autorizar todas las novedades que sucedan sobre las cuentas y perfiles de usuario del respectivo sistema de información-.

6.3.2. Apertura y asignación de cuentas de usuario

La apertura y asignación de una cuenta de usuario para acceso a los sistemas de información institucionales requiere los siguientes pasos:

6.3.2.1. Para empleados y docentes de la institución:

- En el momento de la vinculación del usuario con la Universidad, la Dirección de Gestión Humana comunicará la misma a la Dirección de Tecnologías de información, indicando los siguientes datos como mínimo:
  - Documento de Identidad del Usuario
  - Nombre completo del usuario
  - Cargo Asignado al usuario
  - Fecha inicial de la vinculación
  - Fecha de terminación

- La Dirección de Tecnologías de Información creará el respectivo usuario en el directorio activo y le asignará la cuenta de correo electrónico institucional. Igualmente informará las credenciales de acceso a la Dirección de Gestión Humana para que las entregue al usuario dentro del proceso de inducción respectivo.

- Si adicionalmente, para el cumplimiento de sus funciones el usuario requiere que se le asigne una cuenta para acceso a sistemas de información, se requerirá una solicitud formal de parte de la Unidad Administrativa o Académica a la que se encuentra adscrito el empleado, y la aprobación del usuario propietario del sistema de información

- La autorización para la creación de cuentas para acceso a los sistemas de información deberá incluir como mínimo los siguientes datos:

  - Nombre del usuario para quien se solicita asignar la cuenta
  - Perfil de usuario que se le debe aplicar. Debe corresponder a uno de los perfiles de usuario existentes.

- Las personas encargadas de autorizar y crear cuentas de acceso a los sistemas de información serán las siguientes:
  - Para cuentas de usuario en el sistema de información BANNER:
    Autoriza: Jefe de Admisiones y Registro Académico.
    Crea la cuenta: Jefe de Admisiones y Registro

  - Para cuentas de usuario en el sistema de información ICEBERG:
    Autoriza: Jefe de Contabilidad
    Crea la cuenta: Dirección de Tecnologías de Información.

  - Para cuentas de usuario en el sistema de información DOCUWARE:
    Autoriza: Director de Bibliotecas
    Crea la cuenta: Ing. Administrador del Sistema Docuware

  - Para cuentas de usuario en los sistemas de Información SIGIES, CALIDAD ON LINE
    Autoriza: Director de Planeación y Calidad
    Crea la cuenta: ing. Administrador de SIGIES

6.3.2.2. Para estudiantes:

- La creación de la cuenta de usuario mediante la cual el estudiante tiene acceso al sistema Banner, hace parte del proceso de Admisión, a cargo de la oficina e Admisiones y Registro Académico. A cada persona admitida como estudiante se le crea una cuenta única a partir de su admisión, con el rol de estudiante. Esta cuenta permanecerá vigente a partir de ese momento durante todo el tiempo de vinculación dela persona como estudiante.

- Una vez creada la cuenta del estudiante, la oficina de Admisiones y Registro comunicará formalmente las credenciales de acceso al interesado, como parte del mismo proceso de Admisión.

6.3.3. Restricciones aplicables a cuentas de usuarios

- Toda solicitud de asignación de cuentas de acceso a los sistemas de información institucionales debe cumplir las siguientes condiciones:

    - Una misma persona solo debe tener UNA cuenta de usuario para acceso a cada sistema de información al que tenga acceso autorizado, excepto en los siguientes casos:
        - funcionarios responsables de la administración técnica, soporte y desarrollo, que requieran más de un acceso, debidamente justificados.

        - Empleados que tengan simultáneamente el rol de estudiantes, en cuyos casos se les podrá asignar adicionalmente una cuenta de acceso al autoservicio de estudiantes del sistema académico.

        - Docentes que tengan encargo administrativo, a quienes se les asignará una cuenta de acceso al sistema de información, consistente con sus funciones, durante la vigencia de su encargo, adicional a la cuenta de acceso al autoservicio de docentes.

    - Cuando por razones de la operación se haga necesario asignar cuenta de usuario a un contratista, dicha cuenta necesariamente deberá estar asociada al vínculo contractual que relaciona al contratista con la institución.

    - En cualquier otro caso la asignación de una cuenta de acceso a los sistemas de información requerirá que la persona tenga un vínculo vigente con la universidad, debidamente registrado en el sistema de información de Gestión Humana, con la siguiente excepción:

      Excepción: Las cuentas de usuario para acceso a los sistemas de información institucionales, que se requieran por parte de entes de control del estado, revisoría fiscal, o empresas de auditoría debidamente autorizadas por la institución, podrán ser autorizadas por parte el propietario del respectivo Sistema de información, quien deberá indicar en la solicitud los siguientes datos:
        - Identificación de la persona responsable de la cuenta

- Nombre completo de la persona responsable de la cuenta
- Entidad a la que pertenece
- Finalidad de la asignación de la cuenta
- Período de vigencia de la cuenta

El reporte oportuno de las novedades relativas a cuentas asignadas por esta excepción es responsabilidad del propietario del respectivo sistema de información.

- Toda persona a quien se le asigne una cuenta de usuario para acceso a un sistema de información, deberá aceptar los términos y condiciones de uso de dicho sistema, las demás políticas institucionales relativas al uso de la tecnología y en especial la política de tratamiento y protección de datos vigente.

6.3.4. Modificación de cuentas de usuario.

- Toda cuenta de usuario permanecerá vigente únicamente durante el tiempo en que permanezca vigente el vínculo que las originó. La vigencia se determinará únicamente con base en la información suministrada por la Dirección de Gestión Humana.

- Toda cuenta de usuario deberá ser deshabilitada en los eventos o novedades que impliquen la ausencia del cargo por parte del titular de la misma, incluyendo: Licencias, Incapacidades, Comisiones, Suspensiones, vacaciones. La cuenta será rehabilitada al finalizar la novedad.

- Cuando una cuenta sea deshabilitada temporalmente por ausencia de su titular y se requiera encargar de sus funciones a otra persona, al usuario reemplazante se le deshabilitará el perfil de permisos que tiene habitualmente y se le asignará temporalmente el que corresponde al usuario a quien está reemplazando, durante el tiempo que dure la novedad. Finalizada ésta, se habilitará de nuevo la cuenta deshabilitada y al reemplazante se le restituirá su perfil habitual.

- Cuando una persona cambie de cargo dentro de la organización, se le retirará el perfil de usuario que tenía asignado, reemplazándolo por el perfil correspondiente al cargo que recibe. Esta modificación por parte de la Dirección de Tecnologías de Información, únicamente a partir del momento en que se reciba la respectiva comunicación del cambio de cargo por parte de la Dirección de Gestión Humana. Al aplicar la modificación la Dirección de Tecnologías de Información comunicará del hecho al usuario, a su jefe de área y al usuario propietario del respectivo sistema de información.

- La aplicación de excepciones a las políticas de modificación de cuentas requerirá autorización expresa de la Rectoría.

6.3.5. Eliminación de cuentas de usuario para acceso a los sistemas de Información

- En el evento de la desvinculación de un usuario, la Dirección de Tecnologías de Información bloqueará de manera preventiva todos sus accesos al recibir la notificación de parte de la

Dirección de Gestión Humana. La reactivación total o parcial requerirá igualmente la autorización de la Dirección de Gestión Humana.

6.3.6. Registro de eventos.

- La Dirección de Tecnologías de Información deberá llevar registro de los eventos que afecten las cuentas de usuario con los correspondientes soportes y autorizaciones.

6.3.7. Perfiles de usuario

- Cada cuenta de usuario tendrá asociado un perfil definido por un conjunto de permisos de acceso a los recursos del sistema en cuestión, los cuales pueden ser de solo lectura, o modificación de datos, y sobre objetos o secciones especificas en concordancia con las funciones que el usuario deba atender frente al receptivo sistema de información.

- Los Empleados que atienden el mismo cargo, con idénticas funciones deberán tener perfiles de usuario iguales para acceso a los sistemas de información.

- En caso necesario, cada jefe de dependencia podrá solicitar la modificación de los perfiles de usuario en su área, la cual requerirá aprobación del propietario del sistema de información. Las modificaciones afectarán a todas las cuentas que tengan asociado el mismo perfil.

- Los perfiles de usuario serán revisados de oficio anualmente por las dependencias, bajo la coordinación de la Dirección de Tecnologías de información.

6.3.8. Revisión periódica de accesos y Perfiles de usuario

- Anualmente se efectuará una revisión de los perfiles de usuario de los sistemas de información, cuyo objetivo es el de verificar su correcta estructura y ajuste a los procedimientos operativos de las distintas dependencias. Esta revisión se efectuará de la siguiente manera:

- La Dirección de Tecnologías coordinará una reunión con cada propietario de los sistemas de información, con presencia de los jefes de área, en la que se presentará la información de los perfiles de usuario existentes, y entregará la matriz de usuarios y perfiles existentes para su análisis.

- Cada jefe de área evaluará conjuntamente con el propietario del sistema de información la pertinencia y validez de los perfiles existentes.

- En caso de requerirse alguna modificación, el Propietario comunicará las modificaciones a la Dirección de Tecnologías de Información, utilizando la matriz de usuarios y Perfiles, así como la fecha en que dichas modificaciones deben entrar en vigencia.

- La Dirección de Tecnologías de Información aplicará las modificaciones autorizadas, e informará de ello tanto al usuario propietario como a la dependencia en cuestión.

- De las reuniones sostenidas para este proceso se levantarán actas, en las que constarán las modificaciones aplicadas con las respectivas justificaciones y autorizaciones.

7. REGLAMENTO DE USO DE LAS AULAS DE INFORMÁTICA

El presente documento contiene las políticas y normas generales que regulan la utilización de las aulas de informática de la institución por parte de la comunidad institucional en general. Su observación y cumplimiento es estrictamente obligatoria para todos los usuarios.

Capítulo I. Usuarios y Servicios

Artículo 1. Se consideran Aulas de Informática todas las aulas dotadas específicamente con recursos de hardware y software que la universidad posee como apoyo a las actividades docentes y de investigación tanto de pregrado como de postgrado, y que son de uso compartido por las diferentes dependencias y usuarios. Se excluyen de esta definición los laboratorios de propósito específico cuyo manejo y funcionamiento depende de las Direcciones de Programa.

Artículo 2. Son usuarios de las Aulas de Informática los siguientes:

- Estudiantes activos de los programas académicos de pregrado y postgrado que se encuentren debidamente matriculados, durante el tiempo de vigencia de su matrícula.
- Estudiantes de programas de educación permanente, durante el tiempo de duración del programa en que se encuentren matriculados.
- Profesores y empleados de la institución cuya vinculación con la universidad se encuentre vigente
- Personas externas y visitantes que sean previamente autorizadas por la Dirección de la Universidad.

Artículo 3. La universidad ofrecerá a los usuarios de las Aulas de Informática los recursos de hardware y software disponibles, para que sirvan como apoyo en sus actividades académicas tanto en pregrado como en postgrado.

Artículo 4. La administración de los recursos de las Aulas de Informática es responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones.

Artículo 5. las condiciones establecidas en el presente reglamento para la utilización de los recursos informáticos institucionales, son de obligatorio cumplimiento por parte de todos los usuarios.

Capítulo II. Normas básicas.

Artículo 6. Los usuarios pueden utilizar únicamente los servicios para los cuales hayan sido autorizados. No está permitida la libre instalación, copiado o modificación del software instalado en los equipos, sin la debida autorización del personal a cargo de las salas.

Artículo 7. Las prácticas individuales de estudiantes, deben quedar registradas en el sistema de reservas. El personal a cargo de las Aulas podrá exigir la identificación del estudiante como requisito para ingreso a las aulas. El documento de identidad válido para ingresar será el carné de estudiante vigente.

Artículo 8. Está prohibido para los usuarios el interferir con los procesos computacionales de la Universidad, mediante acciones deliberadas o accidentales que puedan afectar el desempeño y seguridad de los recursos informáticos o de la información institucional.

Artículo 9. Las clases que requieran el uso permanente de una sala durante un periodo lectivo, deberán ser solicitadas inscritas en el horario maestro del semestre por las dependencias académicas ante la oficina de Registro Académico. Una vez les sea asignada el aula, la asignación se respetará durante todo el período académico.

Artículo 10. Para aquellas clases en que ocasionalmente se requiera el uso de un aula de informática, el profesor encargado deberá reservar el horario deseado ante el Personal a cargo de las aulas, con una anticipación mínima de 3 días hábiles. En estos casos las solicitudes se atenderán en estricto orden de llegada.

Artículo 11. Al finalizar su clase, el profesor deberá asegurarse de entregar el aula al personal encargado, antes de retirarse. En consecuencia, se considera que la clase finaliza para los estudiantes en el momento en que el profesor abandona el aula. Solamente después de recibida el aula por parte del personal a cargo, se autorizará nuevamente el ingreso de estudiantes, el cual estará sujeto a la disponibilidad existente en ese momento.

Artículo 12. Las Aulas de Informática y los servicios que ellas ofrecen son para fines exclusivamente académicos. Por consiguiente, Está absolutamente prohibido usar los equipos de las salas y los servicios de red para jugar, enviar o recibir información pornográfica o de propósito comercial, así como para toda otra actividad de ocio en Internet.

Artículo 13. Los horarios de servicio serán establecidos y dados a conocer a todos los usuarios por la Dirección de Tecnologías de Información y Comunicaciones, y publicados en lugar visible. La utilización de los recursos de las Aulas de Informática en horarios diferentes debe estar debidamente autorizadas por el Director de Servicios Informáticos.

Artículo 14. En caso de pérdida, daño o deterioro de los equipos usados, el usuario debe reportar inmediatamente al personal encargado del aula para proceder a su reparación. Si se llegare a determinar que el daño fue causado por negligencia, mal manejo o maltrato del equipo, el usuario responsable deberá hacerse cargo del costo de la reparación o reemplazo del equipo si fuera el caso.

Capítulo III. Deberes y derechos de los usuarios

Artículo 15. Son deberes de los usuarios:

1. Hacer reserva de los equipos o de las salas con la debida anticipación, de conformidad con las políticas establecidas por la institución. En todos los casos el usuario debe someterse a la disponibilidad existente en el momento de su solicitud.
2. Cumplir con los horarios de servicio establecidos para trabajar en las Aulas de Informática.
3. Cumplir el turno solicitado en el sistema de reservas tanto para reservas individuales y de grupo, para lo cual se esperará hasta 15 minutos, pasados los cuales el usuario perderá el turno.
4. Cuidar y hacer buen uso de todos los recursos de hardware y software, así como los muebles y demás materiales que se encuentran disponibles para su uso en las Aulas de Informática.
5. Acatar las instrucciones y procedimientos especiales establecidos por la Dirección de Tecnologías de Información y Comunicaciones para hacer uso de los recursos de las Aulas de Informática

6. Abstenerse de FUMAR y consumir alimentos y/o bebidas al interior de las Aulas de Informática.
7. Abstenerse de consultar y/o descargar material pornográfico, ofensivo, perjudicial o contrario a los principios institucionales.
8. Abstenerse de instalar o modificar cualquier clase de software sin la debida autorización del personal a cargo de las Aulas. Durante las sesiones de clase, la autoridad para este efecto reposará en cabeza del profesor encargado.
9. Abstenerse de modificar la configuración de los equipos.
10. Abstenerse de conectar, desconectar, abrir o trasladar equipos. Estas labores son privativas del personal a cargo de las Aulas.
11. Mantener una correcta disciplina que no interfiera el trabajo de los demás usuarios de las Aulas de Informática.
12. Procurar el debido orden, limpieza y cuidado de los equipos al terminar la práctica ya sea individual o de grupo, esto incluye apagar los equipos adecuadamente y dejar el puesto de trabajo limpio y en orden.
13. Poseer copia de respaldo de toda su información privada. La Universidad no asume ninguna responsabilidad por pérdidas o modificaciones a la información que haya sido dejada por los usuarios en los computadores de las Aulas de Informática.

Artículo 16. Durante las sesiones de clase, la primera autoridad dentro del aula estará en cabeza del profesor a cargo, quien podrá apoyarse en el personal de auxiliares de informática si lo considera necesario. En todas las demás actividades la autoridad la ejercerá el Jefe de Servicios Informáticos para la Academia a través de respectivo Auxiliar de Informática a cargo del Aula.

Artículo 17. Son derechos de los usuarios:

1. Hacer uso de los equipos y servicios disponibles en las Aulas de informática en los turnos en que le corresponda de acuerdo con el horario de clases o en aquellos que haya reservado para prácticas libres.
2. Recibir tratamiento respetuoso por parte del personal administrativo de la universidad, profesores, compañeros de trabajo y demás usuarios de las Aulas.
3. Recibir asistencia técnica en cuanto a hardware y software se refiera, de acuerdo con las disposiciones que tenga definidos la Dirección de Tecnologías de Información y Comunicaciones

Capítulo IV. Préstamo de Equipos

Artículo 18. Los equipos de cómputo sólo se prestan temporalmente y para ser utilizados **dentro** de las instalaciones de la universidad, previa solicitud de la dependencia que lo requiera ante el Director de Servicios Informáticos, y con el lleno de los procedimientos administrativos vigentes. El préstamo de equipos se hará a solicitud de las dependencias de la institución. En ningún caso se prestan equipos a título personal.

Artículo 19. La dependencia que solicita un equipo en préstamo asume la responsabilidad por la conservación del mismo desde el momento en que lo recibe hasta el momento de su devolución.

Capítulo V. Causales de Sanción

Artículo 20. Son causa de sanción las siguientes acciones:

1. Utilizar los recursos de las Aulas de Informática para fines no académicos, no autorizados o que contrarios a los principios de la institución.
2. Suplantar en cualquier forma la identidad de otro usuario ante los funcionarios o ante los sistemas de información.
3. Violar o intentar violar los sistemas de seguridad de equipos locales o remotos, aún cuando no pertenezcan a la institución.
4. Perturbar el trabajo de otros usuarios con comportamientos que interfieran su trabajo.
5. No respetar los horarios de servicio de las aulas.
6. Faltarle al respeto a otra persona dentro de las aulas de Informática.
7. El desacato a las normas establecidas en el presente reglamento o a los procedimientos establecidos para los usuarios de las Aulas de Informática y en especial, la no observancia de los deberes del usuario prescritos en el artículo 15 de este reglamento.
8. Sustraer o cambiar equipos, partes o componentes de la dotación de hardware y software de las Aulas de Informática.
9. Instalar o desinstalar software en equipos y servidores de la institución sin la debida autorización.
10. Maltrato deliberado o negligente a los recursos de las Aulas de Informática o a las personas encargadas de su funcionamiento.

Capítulo VI. Sanciones

Artículo 21. sin perjuicio de la aplicación del régimen disciplinario previsto en el reglamento estudiantil. La Dirección de Tecnologías de Información y Comunicaciones suspenderá temporalmente el derecho de uso de las Aulas de Informática en los casos en que el usuario infrinja las disposiciones de este reglamento así:

a. A la primera infracción, se le cancelará el turno inmediatamente y se le suspenderá el servicio por el resto del día.
b. A la segunda infracción se le suspenderá el servicio por dos semanas y se reportará el caso a la respectiva dependencia académica o administrativa para el trámite disciplinario si hubiere lugar.
c. A la tercera infracción se le suspenderán los servicios de las Aulas de informática por el resto del semestre y se reportará a la respectiva dependencia académica o administrativa para el trámite disciplinario si hubiere lugar.

PARAGRAFO: En todos los casos la suspensión del servicio le impedirá al estudiante el ingreso a las Aulas para prácticas individuales o no dirigidas. Sin embargo, en todos los caos el alumno sancionado mantendrá su derecho para asistir a las sesiones de clase o de práctica

oficialmente programadas en los horarios de clases, en las que haya sido matriculado regularmente.

Artículo 22. El procedimiento para la aplicación de amonestaciones y/o sanciones a los estudiantes, será el previsto en el reglamento estudiantil.

Artículo 21. Cualquier situación no prevista en el presente reglamento, la resolverán los Vicerrectores de acuerdo con lo previsto en el reglamento estudiantil.