MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION PARA UNIVERSIDAD PEDAGOGICA Y TECNOLOGICA DE COLOMBIA

CONTENIDO

Este documento tiene como objeto dar a conocer las políticas Seguridad Informática que deben cumplir los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos de información de la Universidad Pedagógica y Tecnológica de Colombia.

De igual manera, establecen las reglas básicas con las cuales la UPTC debe manejar sus activos de información, a través de la implantación de normas y procedimientos de modo que aumente la protección de éstos recursos. Así mismo, identifican responsabilidades y establecen requerimientos mínimos para una protección apropiada y consistente de los activos de información de la Institución.

En este documento se entiende como usuarios a la Comunidad Universitaria (funcionarios públicos, funcionarios oficiales, docentes, aspirantes, estudiantes, egresados, contratistas internos y externos) en General, que hacen uso de servicios de tecnología de la información de la Institución.

1. POLITICA PARA EL MANEJO DE LA INFORMACION

Esta política tiene como finalidad establecer las directrices para proteger la información contra uso no autorizado, divulgación o publicación, modificación, daño o pérdida y establecer el cumplimiento de reglamentaciones y leyes aplicables a la Universidad Pedagógica y Tecnológica de Colombia.

- **Acuerdos de Confidencialidad**: Los funcionarios y contratistas de la Institución deben firmar acuerdos de confidencialidad al momento de realizar la legalización de sus respectivos contratos, en los cuales se comprometen a no divulgar, usar o explotar la información institucional a la cual tengan acceso.
- Los proveedores que requieran tener acceso a la información confidencial de la Institución, deben firmar un acuerdo de confidencialidad. En caso de que el proveedor no esté de acuerdo con la firma de éste, no podrá tener acceso a la información requerida.
- **Propietario de la Información**: La información institucional (artículos, revistas, contenidos de cursos, videos, fotos, información académica, entre otros) administrada, manejada o creada por los empleados de la Universidad independiente de su forma de vinculación es de la UPTC, al igual que los Sistemas de Información desarrollados por personal interno o externo. La Institución es propietaria de los derechos de esta información.
- **Derechos de Autor**: Está prohibido por las leyes de derechos de autor y por la UPTC hacer copias de la información institucional en cualquier formato, copias no autorizadas de software ya sea adquirido o desarrollado por la Universidad.
- La Universidad no realizará copias de seguridad de software que no le esté permitido.
- **Publicaciones de Seguridad de la Información**: Todos los usuarios de servicios de tecnologías de Información, deben aplicar las directrices dadas a través de publicaciones o comunicadas en capacitaciones o campañas Institucionales respecto a la Seguridad de la Información
- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la UPTC, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable y sin afectar la productividad.
- Los usuarios no deben propagar cadenas de mensajes de cualquier tipo y la comunicación de tipo comercial, político, religioso y en general cualquier contenido ofensivo para los funcionarios de la Universidad.

- Los funcionarios de la Universidad deben cumplir fidelidad como producto de las tareas que les fueron asignadas y guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la Institución de la cual tengan conocimiento en el ejercicio de sus funciones.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por UPTC y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Es deber de los funcionarios verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.
- **Equipos de procesamiento de datos tipo servidor**: Los administradores de servidores, bases de datos y demás roles que manejen información clasificada como semiprivada y privada, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción
- **Equipos de procesamiento de datos tipo servidor:** La administración de los equipos de procesamiento de datos tipo servidor que soportan servicios institucionales debe ser realizada por el Grupo Organización y Sistemas. Los servidores que no sean administrados por el Grupo Organización y Sistemas, el responsable del activo de información, debe presentar por escrito los motivos y justificación de esto a la Coordinación del Grupo Organización y Sistemas.

2. POLITICA DE USO DE RECURSOS TECNOLOGICOS

- **Instalación, Mantenimiento y Actualización de Hardware**: El personal adscrito al Grupo Organización y Sistemas es el único autorizado para instalar aplicaciones y realizar mantenimientos preventivos y correctivos en los equipos de cómputo de la Institución.
- **Uso de los Equipos de Cómputo**: Los equipos de cómputo (computadores, impresoras, portátiles, servidores, tablas y demás elementos similares) de la Institución serán utilizados únicamente por el personal autorizado para el desarrollo de las actividades asignadas.
- Todo funcionario, contratista y/o docente de la Institución es responsable del equipo que le sea asignado; el cual será incluido a su inventario personal, de acuerdo con el procedimiento Egreso de Bienes de Almacén A-AB-P05.
- Los dispositivos móviles (portátiles, tablets, celulares) propiedad de la Universidad, no deben ser desatendidos. El usuario deberá tomar las medidas de seguridad pertinentes que permitan garantizar la integridad y confidencialidad del activo de información.
- En caso de presentarse una falla o problema de hardware o software en una estación de trabajo o equipo portátil propiedad de la Universidad, el usuario responsable del mismo deberá informarlo al Grupo Organización y Sistemas a través de la mesa de ayuda, para una asistencia especializada y, por ningún motivo, deberá intentar resolver el problema.
- **Artículos de Decoración en Equipos de Cómputo**: Se debe mantener el equipo de cómputo libre de fotos, calcomanías y cualquier otro elemento que lo pueda deteriorar o comprometer su integridad.
- **Software en los Equipos de Cómputo**: Para todos los equipos de cómputo propiedad de la Institución, se instalará únicamente el software que cuente con licencia autorizada para uso en la Universidad. El software que no cumpla con estos lineamientos se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley antipiratería.
- **Software Antivirus**: Para todos los equipos de cómputo propiedad de la Institución, se instalará únicamente el software antivirus que el Grupo Organización y Sistemas establezca.
- Los usuarios que hacen uso de los servicios de Tecnología de Información y Comunicación, deben realizar tareas de escaneo de archivos y directorios, no deben cambiar o eliminar la configuración del software de antivirus en los equipos de cómputo propiedad de la Institución.

- Los usuarios no deben descargar archivos adjuntos que provengan de fuentes desconocidas, para evitar contaminación por virus informáticos y/o instalación de software malicioso en sus estaciones de trabajo o equipos portátiles.
- **Aplicaciones de Ofimática:** La suite de ofimática permitida por la Institución para equipos con sistema operativo Windows y Mac, son las versiones de Microsoft Office licenciadas por la Universidad. Se permite el uso de la versión libre de Open Office, en los equipos de cómputo propiedad de la Institución.
- **Sistemas Propietarios Desarrollados en la Institución.** La instalación de productos de software desarrollados por el Grupo Organización y Sistemas de la Universidad se realizará en los equipos de cómputo propiedad de la institución designados para tal fin.
- **Sistemas de información de entes de control:** El licenciamiento de los sistemas de información a través de los cuales se reporta información, es responsabilidad del ente de control respectivo.
- **Acceso a Código Fuente de Aplicaciones:** Está prohibido manipular el código fuente de una aplicación sin la autorización correspondiente del Grupo Organización y Sistemas, para generar cambios o mejoras a la misma. Si se requiere tener acceso al código fuente de una aplicación desarrollada en la institución, se debe solicitar permiso al GOS. Si se trata de una aplicación desarrolla por un proveedor externo, se deben revisar las condiciones del contrato.
- **Gestión de Cambios:** Se deben documentar todos los cambios que se realicen a los recursos tecnológicos de la Universidad de acuerdo con el procedimiento A-RI-P10 Procedimiento para la Gestión de Cambios y Entregas.
- **Documentación de Pruebas:** Se deben documentar todas las pruebas que se realicen a los recursos tecnológicos de la Institución. de acuerdo con el procedimiento A-RI-P10 Procedimiento para la Gestión de Cambios y Entregas.
- **Monitoreo de Equipos**: La Institución se reserva el derecho de monitorear los equipos de cómputo, conectados a la red de datos de la universidad, de los cuales se sospeche que están comprometiendo la confidencialidad, integridad y disponibilidad de la información.
- La universidad dispone de un Data Center, como lugar adecuado para el alojamiento de los equipos de procesamiento de datos tipo servidor.
- El Grupo Organización y Sistemas gestiona el mantenimiento periódico para el Data Center junto con los elementos que lo componen, para garantizar la integridad, disponibilidad y confidencialidad de los activos de información que se encuentran allí alojados.
- Los usuarios no pueden portar información de la Universidad clasificada como privada sin la previa autorización del propietario del activo de información independiente del medio que utilice.
- La instalación de un nuevo componente en la red de datos debe estar autorizada por la Coordinación del Grupo Organización y Sistemas.
- La adopción y uso de tecnologías de la información y la comunicación orientadas a la gestión de servicios institucionales, serán aprobados por el Grupo Organización y Sistemas.

3. POLITICA DE ACCESO REMOTO

La presente política contempla las comunicaciones electrónicas y conexiones remotas de usuarios autorizados para acceder a los servicios de la red de datos institucional.

- El Servicio de acceso remoto permite el acceso a la red de datos institucional a aquellos usuarios externos e internos expresamente autorizados por el Líder del Proceso de Gestión de Recursos Informáticos, para

que lo hagan desde redes externas o internas, el cual debe estar sujeto a autenticación con un nivel adecuado de protección.

- Solo Los equipos de procesamiento de datos tipo servidor y de comunicación tendrán habilitado el servicio de conexión de acceso remoto. Los clientes para acceder a estos recursos serán previamente identificados y autorizados.

4. POLITICA DE ESCRITORIO Y PANTALLA LIMPIOS

Esta política se aplica a la protección de cualquier tipo de información, cualquiera de sus formas y que pueden estar contenidas en escritorios, estaciones de trabajo, computadores portátiles, medios ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que se utiliza para apoyar la realización de las actividades laborales. El objetivo es reducir los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo.

- Todas las estaciones de trabajo deben usar el papel tapiz Institucional y contar con bloqueo de sesión automática después de 2 minutos de inactividad, el cual, debe mostrar la pantalla de inicio de sesión solicitando el ingreso del usuario y contraseña al ser reanudado.
- La información confidencial o sensible, cuando se imprime se debe retirar inmediatamente de las impresoras.
- Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo para proteger el acceso a las aplicaciones y servicios de la institución de personal no autorizado.
- Los datos sensibles almacenados en los equipos o sistemas de información, deberán encontrarse ubicados en rutas que no sean de fácil acceso.
- Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, así mismo debe cerrar la sesión o salir de todas las aplicaciones correctamente y dejar los equipos apagados (no sólo el monitor).

5. POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO

- Todas las personas que ingresen a la Universidad, deben hacer uso del Sistema de Control de Acceso.
- La Coordinación del Grupo Organización y Sistemas debe elaborar un listado del personal que por el rol de sus funciones está autorizado para ingresar al Data Center.
- Únicamente ingresará al Data Center el personal autorizado con los elementos necesarios para desarrollar sus labores.
- No se permiten las visitas al Data Center a no ser que sea para llevar a cabo labores de mantenimiento o auditorias.
- No se debe proveer información sobre la ubicación del Data Center o de los lugares críticos, como mecanismo de seguridad.
- Las puertas de acceso al Data Center, el área de Tecnología de Información y los Centros de Cableado deben permanecer siempre cerradas y aseguradas. De igual manera, todos los gabinetes y puertas de los equipos que se encuentran en estos lugares deben permanecer cerrados.
- Los funcionarios deben portar el carné que los identifica como empleados de la Universidad, mientras permanezcan dentro de las instalaciones de la Institución.

6. POLITICA DE INSTALACION DE CABLEADO

- **Instalación de Cableado Estructurado**: Planeación, diseño, construcción, instalación, administración y mantenimiento del cableado estructurado de telecomunicaciones de la Institución es responsabilidad del proceso Gestión de Recursos Informáticos, debe cumplir con las normas técnicas o estándares adoptados por el mismo, con el fin de garantizar la integridad, conservar la estética y la seguridad de las redes.

7. POLITICA DE COPIAS DE RESPALDO

- El Grupo Organización y Sistemas debe respaldar con copias de seguridad la información Institucional que sea de misión crítica, dichas copias deben ser tomadas y probadas de acuerdo al procedimiento A-RI-P03 Copias de Seguridad de la Información.
- El Grupo Organización y Sistemas debe garantizar copia de la información de configuración contenida en la plataforma tecnológica de la Institución como equipos tipo servidores, equipos activos de red y dispositivos de red inalámbricos, dichas copias deben ser tomadas y probadas de acuerdo al procedimiento A-RI-P03 Copias de Seguridad de la Información.
- El Grupo Organización y Sistemas debe garantizar copia de los productos de software que administra, dichas copias deben ser tomadas y probadas de acuerdo al procedimiento A-RI-P03 Copias de Seguridad de la Información.
- Los medios magnéticos que tienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra ubicada. El sitio externo donde se resguardan dichas copias, solo tendrá acceso el Grupo Organización y Sistemas.
- Es responsabilidad exclusiva de los usuarios, la creación de copias de seguridad de archivos usados, custodiados o producidos por estos. Para esto, deben tener en cuenta la Guía para Proteger Información en Equipos Computacionales A-RI-P03-G01.

8. POLITICA DE INTERCAMBIO DE INFORMACION

- El intercambio de información manual, solo debe utilizar los servicios de correos autorizados en la Universidad. De ser entregada por mano, debe ser entregada personalmente al destinatario y su entrega debe quedar registrada.
- Toda información enviada a través del correo Institucional, debe incluir en su pie de página, una advertencia en cuanto a su uso y autorizaciones al respecto, quedando bajo responsabilidad del receptor el cuidado y resguardo de la información.
- Todo intercambio de información a través de acceso remoto, debe cumplir con la Política de Acceso Remoto establecida por la Institución.
- El intercambio de información privada a o semiprivada por vía telefónica no está permitido.

9. POLITICA DE MANEJO DE INCIDENTES Y PETICIONES

- Todos los incidentes y peticiones solicitados por los usuarios de la Institución deben ser canalizados a través del sistema mesa de ayuda.
- Toda la información relativa a los incidentes reportados, debe ser manejada con total confidencialidad.
- El Grupo Organización y Sistemas reportará ante la autoridad competente los incidentes de seguridad que estén considerados como un delito informático.

10. POLITICA DE GESTION DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION

- El líder del SGSI informará el plan de continuidad de la seguridad de la información los procesos involucrados en el SGSI.
- La revisión del Plan de Continuidad de la seguridad de la información debe hacerse anualmente, dependiendo de los cambios y nuevos requerimientos en los procesos.
- El Data Center se debe proveer con unidades suplementarias de energía eléctrica (UPS) y se debe garantizar el óptimo funcionamiento de dichas unidades.
- Las copias de seguridad de los sistemas de computación que incluye sistema operativo, base de datos, aplicación, servicios, entre otros; deben ser almacenados en un lugar diferente de donde reside la información original, dentro de las instalaciones de la Universidad.
- Debe realizarse mantenimiento preventivo y periódico a los equipos servidores, de comunicaciones y demás equipos en los cuales haya configurados servicios, de tal forma que el riesgo a fallas físicas se mantenga en una probabilidad de ocurrencia baja.
- Debe realizarse mantenimiento preventivo a intervalos programados a equipos de cómputo de los usuarios finales, propiedad de la Institución, para reducir el riesgo de falla.
- Los planes de continuidad deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.
- La Institución gestiona y ejecuta los planes de capacitación para garantizar la formación y actualización de los funcionarios del Grupo Organización y Sistemas conforme a las necesidades de modernización tecnológica que se presenten y mantener la confidencialidad, disponibilidad e integridad de los diferentes activos de información de la institución, así como la continuidad en la prestación de servicios de Tecnología e Información.

11. POLITICA DE CUMPLIMIENTO

- El líder del proceso Gestión Normativa tiene la responsabilidad de identificar la legislación vigente que debe cumplir la Universidad en función de la protección de la información y divulgar estos requerimientos. Además, debe servir de apoyo en la interpretación, asistencia y manejo de dicha legislación.
- Todos los funcionarios de la Universidad deben cumplir con la Normatividad vigente adoptada por la Institución, leyes de derechos de autor, acuerdos de licenciamiento de software y acuerdos de confidencialidad.

12. POLITICA DE CONTROL DE ACCESO

- El control de acceso a todos los Sistemas de Información de la entidad y en general cualquier servicios de Tecnologías de Información, debe realizarse por medio de Credenciales de Acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.
- Para la asignación y/o eliminación de credenciales de acceso de usuarios institucionales administrativos, docentes y contratistas se hará de acuerdo al procedimiento de vinculación de servidores públicos A-GH-P03 y entrega de cargos A-GH-P05, y se tendrá en cuenta los lineamientos por el Grupo Organización y Sistemas en el procedimiento de Gestión de Identidad y Acceso A-RI-P20.

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de UPTC debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y de la Institución, que se definan por las diferentes dependencias de la Universidad, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.
- El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por el Grupo de Organización y Sistemas.
- La asignación de la contraseña para acceso a sistemas, se debe realizar de forma individual, por lo que el uso de contraseñas compartidas está prohibido. Al revelar o compartir la contraseña el usuario autorizado se expone a responsabilizarse de acciones que otras personas hagan con su contraseña.
- Los usuarios son responsables de todas las actividades llevadas a cabo con su identificación de usuario y contraseña.
- La contraseña inicialmente emitida por un administrador de sistema es válida solamente para la primera conexión del usuario, quien debe cambiarla antes de realizar cualquier actividad en el sistema.
- Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.
- Los usuarios deben tener en cuenta el siguiente lineamiento para la construcción de sus contraseñas:
  - ✓ Debe estar compuesta de al menos ocho (8) caracteres. Estos caracteres deben ser caracteres alfabéticos, numéricos y símbolos o caracteres especiales.
- La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.
- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente.
- La gestión de la contraseña asignada al usuario institucional, se realizará directamente por los usuarios a través del portal http://miclave.uptc.edu.co
- El Grupo Organización y Sistemas debe implementar en las bases de datos un límite de intentos consecutivos infructuosos para ingresar la contraseña, el cual, corresponde a cinco (5). Superado el tope se suspende el acceso del usuario hasta que el administrador de la base de datos active el usuario nuevamente.
- Cuando un usuario bloquee su cuenta debido a la superación del número máximo de intentos, debe reportarlo al Grupo Organización y sistemas, indicando a que sistema de información, para que se le active la cuenta y restaure su contraseña.
- La activación de la cuenta y obtención de acceso a la contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante el Grupo Organización y Sistemas como Usuario de la Universidad.
- Las contraseñas no se deben incorporar dentro de los productos de software, esto para garantizar que las contraseñas se puedan cambiar en el momento que sea necesario.
- Se debe hacer el cambio de las contraseñas proporcionadas por el fabricante (contraseñas por defecto) antes de poner en producción cualquier activo de información en la Institución.

13. POLITICA DE USO DE CONTROLES CRIPTOGRAFICOS

La Universidad establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso.

- Se utilizarán controles criptográficos en los siguientes casos:
  Para el resguardo de información, que sea clasificada como confidencial y la que surja de la evaluación de riesgos realizada por el propietario de la Información y el Comité de Seguridad de la Información.

  Para el almacenamiento de las contraseñas de los sistemas operativos, gestión de identidad y bases de datos.

- Se definirá el uso de un software para realizar la encripción de la información en los equipos de cómputo.

14. POLITICA DE GESTION DE LLAVES

- Las llaves criptográficas utilizadas para el cifrado de los datos deben estar clasificadas como Confidencial y ser protegidas contra divulgación, uso indebido o sustitución no autorizada restringiendo al mínimo el número de custodios necesarios y guardándola de forma segura en la menor cantidad de ubicaciones y formas posibles.
- Para reducir la probabilidad de compromiso, las llaves tendrán fechas de inicio y caducidad de vigencia.

15. POLITICA DE DISPOSITIVOS MOVILES

- Las características en las capacidades de los equipos serán definidos en función de la importancia de la información procesada o almacenada en cada tipo de usuario que utiliza un dispositivo móvil de la Institución.
- Todos los usuarios de dispositivos móviles que contengan información Confidencial o de Uso Interno deben usar la última o la más segura versión de los productos de software. Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.
- Los usuarios de dispositivos móviles deben mantener actualizado el software antivirus del dispositivo.

16. POLITICA DE GESTION DE MEDIOS REMOVIBLES

Esta política define las reglas para la protección de datos en diferentes medios de almacenamiento removible; considerando su administración, protección y traslado.

- Todos los medios removibles que contengan información sensible o confidencial serán almacenados en un ambiente seguro y vigilado según las especificaciones del fabricante y los niveles de clasificación de la información.
- Los medios removibles **NO** son alternativa de respaldo de información permanente, siendo responsabilidad de los usuarios mantener la información en los servidores, servicios en la nube o equipos destinados para ello.
- Los medios removibles deben ser escaneados cada vez que sea conectado a un equipo de la red de la Universidad, especialmente en lo concerniente a posible código malicioso.
- Debe formatearse el medio removible cuando la información pierda vigencia de acuerdo al Procedimiento A-RI-P23 Eliminación Segura de la Información.
- El funcionario debe dar buen uso a los medios removibles asignados, informando oportunamente cualquier deterioro.
- No se debe almacenar información confidencial en los teléfonos móviles.
- Una vez asignado el medio removible al usuario, es de su exclusiva responsabilidad tomar las medidas adecuadas para el almacenamiento y custodia necesarios de la información, para protegerla de accesos no autorizados, daño o pérdida.

17. POLITICA DE DESARROLLO SEGURO

- Para apoya los procesos operativos y estratégicos la Universidad debe hacer uso intensivo de las Tecnologías de la Información y las comunicaciones. Los productos de software pueden ser adquiridos a través de terceras partes o desarrollado por personal propio.
- El Grupo Organización y Sistemas debe elaborar, mantener y aplicar un procedimiento para la incorporación de sistemas de información, el cual debe incluir lineamientos, procesos, buenas prácticas, plantillas y guías que sirvan para regular los desarrollos de productos de software internos en un ambiente de aseguramiento de calidad.
- Los productos de software adquiridos a través de terceras partes deben cumplir con el procedimiento de incorporación de sistemas de información establecido por la Universidad.

18. PROHIBICIONES

- Queda prohibida la ejecución de cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada, así como evadir los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación servidor o cuenta de usuario, están restringidos.
- Está prohibido utilizar la infraestructura de tecnología de información y redes de la Universidad, para conseguir o transmitir material con ánimo de lucro.
- Está prohibida la utilización de la infraestructura de tecnología de información y redes de la Universidad para hacer algún tipo de acoso, difamación calumnia o cualquier forma de actividad hostil en contra de miembros de la comunidad universitaria y en general de cualquier persona o institución.
- Queda prohibida la instalación de puntos de acceso inalámbricos no autorizados en la Institución.
- La tecnología de información que provee la UPTC es para el desarrollo de los procesos institucionales exclusivamente. Por lo tanto, no está permitido el uso con fines personales de estos recursos.
- No se exime a los usuarios de la responsabilidad disciplinaria y legal correspondiente de toda aquella acción que no esté aquí documentada y pueda afectar la Seguridad de la Información de la Institución.