



UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

CONSEJO ADMINISTRATIVO

Políticas y Reglamentos para el Uso Aceptable de los Recursos de Redes de la Universidad Tecnológica de Panamá

Preámbulo / Introducción

La Tecnología tiene la capacidad para abrir las puertas a un vasto mundo de recursos de información, así como de personas, a cualquier estudiante o miembro de la comunidad universitaria con una conexión a Internet. Las oportunidades que tenemos con esta conectividad son casi ilimitadas, mas no así, los recursos computacionales y de conectividad disponibles. Este nuevo mundo virtual al que tenemos acceso requiere de políticas y reglamentos para asegurar un uso óptimo y correcto de los recursos.

El espíritu de este documento es establecer normas de convivencia y aprovechamiento de los recursos y servicios computacionales y de Internet en beneficio de nuestra comunidad universitaria. El desarrollo de políticas que sean bien entendidas, que circulen ampliamente y que sean efectivamente implementadas, conllevará a hacer de la Red Universitaria y el Internet un ambiente seguro y productivo para todos.

Se trata entonces de presentar lo que se conoce como **Políticas y Reglamentos para el Uso Aceptable** (en inglés AUP) para los recursos computacionales y de conectividad presentes en la red Universitaria. Estas políticas establecen entre otras cosas, el comportamiento esperado de los miembros de la comunidad universitaria hacia diferentes servicios de información (e-mail, www, videoconferencias, etc.) y las reglas en cuanto al uso adecuado de recursos físicos.

Estas políticas de uso son un reflejo directo de los códigos de conducta vigentes en la UTP y representan explícitamente la cultura de nuestra institución. Además, han sido elaboradas y revisadas por las autoridades competentes de la UTP, tomando en cuenta su viabilidad y aplicabilidad, basándose en la Ley, el Estatuto y Reglamentos de la Universidad.

Términos/Definiciones.

- **Red UTP:** Es el conjunto de recursos computacionales y de conectividad que permite la comunicación de datos e información a través de todo el Campus, Centros Regionales y Extensiones.

- **Servidor de Nombres de Dominio (Domain Name Server):** Es un servidor que mantiene una base de datos, desglosada por zonas, que contiene información acerca de las computadoras de la Red UTP e Internet.
- **Dirección Física (MAC Address):** Número que identifica la tarjeta de red.
- **Dirección IP:** Un número único que identifica una computadora en Internet. Por ejemplo 205.244.32.5
- **Estación segura:** Una computadora que cumpla con los requerimientos mínimos de seguridad de comunicación de datos estipulados por PANNet.
- **Nombre de Usuario (Username):** El nombre con que se identifica la cuenta de un usuario en un servidor.
- **Dirección de correo electrónico:** Es la dirección del buzón de correos. Consta del nombre de usuario, una @ y el nombre de dominio. En nuestro caso: **nombre.apellido@utp.ac.pa**
- **Cartas Cadena (Chain Letters):** Las cartas encadenadas son cualquier correo electrónico que solicita que el recipiente reproduzca y envíe la correspondencia a otros con el propósito de perpetuar la carta (o cadena). En ocasiones las cartas ofrecen promesas de ganancia personal, fortuna, o evitar el infortunio económico.
- **Correo basura (Spam Mail):** El correo basura corresponde a la utilización del servidor de correo electrónico con el propósito de propagar mensajes o propagandas a un amplio número de usuarios que posean cuentas en un servidor o Internet, en general.
- **Números de Identificación Personal (PIN):** Secuencia de números o caracteres que proveen acceso a un sistema determinado.

POLÍTICAS DE USO ACEPTABLE.

Disposiciones Generales

- 1.- La función de la Red de Convergencia de Voz, Datos y Video es "transportar" material que soporte la función académica e investigadora de la UTP. Este material incluye cualquier tipo de información, por ejemplo: el correo electrónico, la transferencia de archivos, la conexión a servidores internos y remotos, la navegación en la World Wide Web, el desarrollo y desempeño de aplicaciones sobre su infraestructura, y los que se designen como tales por parte de PANNet.
 - a. Dentro de este marco, la UTP permite el uso de la Red UTP a miembros de la comunidad universitaria ⁽¹⁾.
 - b. Adicionalmente, el acceso a Internet por los miembros de la comunidad universitaria es permitido para el propósito de actividades académicas y de investigación legítimas.

Nota:1.- La comunidad Universitaria es reconocida como todas las facultades, empleados, estudiantes y afiliados.

- 2.- El uso de la Red UTP por individuos u organizaciones que no sean parte del personal, estudiantes o afiliados legítimos ⁽²⁾, no está permitido.
- 3.- El objetivo primordial de estos servicios es brindar apoyo a las actividades académicas, investigativas, docentes y administrativas de los usuarios de la Red UTP. Basándose en el principio de acceso abierto y universal, la elegibilidad para el servicio al cual se le permitirá tal acceso, será determinada por las siguientes prioridades donde recursos insuficientes estén disponibles:
 - a. La prioridad más alta es para los miembros de la comunidad universitaria donde el acceso a la red es mandatorio por el requerimiento de un programa de investigación o programa de un curso o materia de la UTP.
 - b. En el próximo nivel, el acceso será garantizado donde sea demostrado, pero no mandatorio, el requerimiento de acceso a la red para algún programa de investigación o curso.
 - c. El nivel más bajo o no esencial de acceso será basado en el principio de acceso universal y en soporte del objetivo académico, aunque no sea directamente estipulado dentro de un curso o materia.
- 4.- El acceso a Internet en el campus, centros regionales y extensiones, debe hacerse desde una estación debidamente registrada y/o autorizada por PANNet. Dicho de otra forma, el computador debe estar registrado dentro de la base de datos de la UTP y estar localizado con una dirección IP legítima, la cual debe coincidir con la dirección física y/o Certificado Digital que le corresponde. De tener que realizar algún cambio por desperfectos técnicos de la tarjeta de red, el mismo debe ser notificado a PANNet.
 - a. La estación de trabajo debe soportar e implementar protección de clave de usuario y sistemas de seguridad de redes actualizados.
- 5.- Las reglas que gobiernan la libertad académica en la UTP aplicarán al uso de las redes de comunicación, donde el objetivo es la transmisión y persecución del conocimiento.
- 6.- Las políticas de uso aceptable de la red incluyen el uso de la red de comunicación para el propósito de soportar actividades administrativas asociadas con las actividades académicas y de investigación de la UTP, pero no excluyen la interacción social, hasta tanto no interfiera con los objetivos descritos en el artículo 1.
- 7.- El uso de la red de comunicaciones de la UTP para ganancias y actividades financieras no relacionadas con las actividades normales de la UTP es catalogado como una práctica inaceptable.
 - a. No será permitido bajo ninguna circunstancia, el vender o alquilar el espacio en disco disponible para WWW. De la misma forma, se considera inaceptable el vender o alquilar su cuenta de correo electrónico.
 - b. No es permitido utilizar la red y equipos computacionales para fines comerciales sin la expresa autorización escrita de la UTP.

Nota 2.- La definición de afiliado incluye organizaciones gubernamentales, semi-gubernamentales y no gubernamentales que se unan a la UTP en soporte de la empresa académica, de investigación y extensión. Los individuos que correspondan con este criterio deben ser considerados afiliados también.

- 8.- Todo usuario es responsable por el apropiado uso de los recursos que le ofrezca la red y se compromete a cumplir todas las disposiciones contenidas en este documento. Está taxativamente prohibido el uso y acceso de material de pornografía en todas sus formas, de tipo terrorista y cualquier otro material que esté o sea prohibido por la comunidad internacional.
- 9.- La instancia inmediata encargada de la vigilancia, supervisión y cumplimiento de este reglamento es PANNet.

De las cuentas, su uso y privacidad

- 10.- Las cuentas de todos los miembros de la comunidad universitaria, ya sean del servicio de correo electrónico o de ingreso a cualquier sistema de la UTP, son personales e intransferibles. La UTP no permite la transferencia de claves o Números de Identificación Personal (PIN) entre cualesquiera individuos. Tal acción es considerada inaceptable y será sujeta a acción disciplinaria.

Además:

- a. Las cuentas y todos los datos encontrados en la cuenta de un empleado de la UTP, serán removidos de todas las instalaciones de la UTP, al momento de la terminación de su contrato de empleo por cualquier razón que fuere.
- b. Las cuentas y todos los datos encontrados en la cuenta de un estudiante de la UTP, serán removidos al inicio del semestre siguiente definido en el calendario académico. Estudiantes dados de baja académica o que se han retirado por cuenta propia tendrán sus cuentas eliminadas al momento de la fecha efectiva de expulsión o retiro.
- c. Las cuentas y todos los datos encontrados en la cuenta de un estudiante de Post-Grado de la UTP, serán removidos al inicio del módulo siguiente, definido en su programa académico. Cuando se trate de la expulsión o retiro del estudiante, la cuenta será eliminada al momento de la fecha efectiva de expulsión o retiro.
- d. Las cuentas y todos los datos encontrados en la cuenta de un afiliado legítimo de la UTP, serán removidos al momento de la terminación de la afiliación formal.

La conservación, integridad y contenidos de la información dependen del usuario, quien es responsable de respaldar sus archivos.

- 11.- El uso del sistema de correo electrónico para la distribución de información no solicitada o propaganda no relacionada a las actividades normales y asuntos de la UTP, no está permitido (3).

Nota 3.- Esto incluye los correos cadenas (chain letters) y el correo basura (spam mail). Si usted considera que ha recibido tales mensajes, contacte a la Unidad de Redes y Comunicaciones de PANNet inmediatamente. Participar en una cadena de correos es una violación seria de las Políticas de Uso Aceptable.

- 12.- Las comunicaciones privadas a través de la Red UTP tendrán la misma protección que las comunicaciones privadas vía telefónica. La interceptación, lectura, copia o modificación de datos electrónicos privados (4) romperá este código de práctica y estará sujeto a procedimientos disciplinarios o legales. La UTP no garantizará esta privacidad como resultado de mantenimiento de rutina, falla técnica o actividad criminal. Además:
- a. A los miembros de la comunidad universitaria no le será permitido interceptar, leer (utilizando elementos tales como sniffers, SNMP, RMON, y otros), copiar, modificar o falsear datos electrónicos privados (ya sea en tránsito a través de la red o almacenados dentro de una computadora) sin el consentimiento escrito del propietario legítimo.
 - b. A los empleados de la UTP que posean password de root o supervisor no les será permitido interceptar, leer, copiar o modificar datos electrónicos (ya sea en tránsito a través de la red o almacenados dentro de una computadora).
 - c. Solamente el personal técnico de PANNet es el autorizado para monitorear el trasiego de datos en la red.
 - d. Cuando las autoridades de la UTP lo requieran, podrán acceder al correo electrónico, correo de voz y/o cuentas de computadoras sin el consentimiento del usuario, basados en situaciones que lo ameriten. Tales como:
 1. Cuando sea necesario cumplir con un proceso o requerimiento legal, o
 2. Cuando pueda contener información necesaria para la investigación de una sospecha de violación de la ley o norma, o de una seria sospecha de infracción a las políticas universitarias (por ejemplo: investigación de conductas inapropiadas, plagio o acoso), o
 3. Cuando sea necesario para mantener la integridad de los sistemas computacionales de la universidad, o
 4. Cuando pueda contener información necesaria para tratar una emergencia, o
 5. En el caso de personal directivo y funcionarios en general, cuando pueda contener información que sea necesaria para conducir los negocios ordinarios de la universidad.
 - e. De darse la situación prevista en el punto d, la universidad deberá notificar al usuario el acceso o apertura del contenido de su correo electrónico, correo de voz y/o cuentas de computadoras, tan pronto como sea posible por medio escrito; excepto cuando así sea determinado por requerimiento legal.
- 13.- Debido a que la UTP se esforzará en mantener la privacidad de las comunicaciones personales, ésta monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes. Además la UTP:
- a. Colectará estadísticas de utilización basado en las direcciones de redes, protocolo de red, y tipo de aplicación.
 - b. Progresivamente restringirá usuarios no esenciales (como se define en el artículo 3) cuando su utilización de la red resulte en la degradación del rendimiento. Tal restricción será notificada a los usuarios a través de medios apropiados.

Nota 4.- En este sentido, los datos electrónicos privados son definidos como toda la información que pueda ser almacenada dentro de un sistema de computador digital o transferida a través de un sistema de comunicación electrónico, y que exista en o esté siendo transferida desde o hacia el dominio registrado de un usuario que está protegido por un password para ese usuario.

- 14.- Las facilidades de la Red UTP no pueden ser usadas por cualquier individuo o grupos de personas para cualquier actividad de naturaleza ilegal o fraudulenta, incluyendo actividades ilegales como las definidas por las leyes locales, estatales e internacionales, así como la ley, el estatuto, reglamentos, políticas y regulaciones de la UTP.
- a. Cualquier actividad que se sospeche ilegal o fraudulenta debe ser inmediatamente reportada a la autoridad competente.
- 15.- A los usuarios que quebranten estas políticas y reglamentos de uso y acceso, les será eliminado el acceso a las redes de comunicación y computadoras de la UTP. Todos los otros estándares de conducta aplican al uso de la red y sus recursos. La violación de esta política de uso es considerada una violación de los reglamentos y estatutos de la UTP.
- a. En casos que involucren alegada actividad fraudulenta, la UTP puede, a discreción del Rector, suspender los privilegios de acceso en espera de los procedimientos legales.
- b. La ruptura de estas Políticas de Uso Aceptable y Acceso, que no involucren actividad fraudulenta o ilegal, serán referidas a un comité disciplinario, como lo indica el estatuto y los reglamentos de la UTP, relevante para su consideración.

De los equipos (Hardware)

- 16.- Es atribución exclusiva de PANNet mover, abrir, desconectar y/o modificar de cualquier modo, los equipos de cómputo utilizados como equipos de enlace, servidores de red o equipos de navegación que tenga a su disposición.
- 17.- El mal uso o el daño intencional a los recursos computacionales de la institución a cargo de cualquier miembro de la comunidad universitaria, se considerará una falta grave y dará motivo a las sanciones estipuladas en la Ley, el Estatuto y Reglamentos Universitarios existentes.
- 18.- PANNet reportará ante la Rectoría, a los usuarios que cometan daños intencionales a los sistemas de cómputo y servidores que compongan la infraestructura de la UTP.

Nota 5.- Las preguntas y comentarios sobre estas políticas pueden ser dirigidas a: utp@utp.ac.pa.

REGLAMENTO PARA LAS POLÍTICAS DE USO ACEPTABLE.

Introducción

La UTP provee computadoras, cuentas de computadoras y correo electrónico, sistemas de redes y telefonía a su personal docente, de investigación, y administrativo y a sus estudiantes para el propósito de desarrollar la misión académica de la UTP y conducir los negocios de la UTP. Cualquier uso personal, ya sea de carácter incidental y/u ocasional de tales sistemas, incluyendo el correo electrónico y correo de voz, es permisible, y las comunicaciones y archivos personales transmitidos sobre o almacenados en los sistemas de la UTP no serán tratados diferentemente de las comunicaciones de negocios, pudiendo esto no ser garantía de que tales comunicaciones personales permanecerán confidenciales o privadas.

• Correo electrónico

1. PANNet es la dirección responsable y encargada de administrar el correo central de la UTP (cuentas y servidores).
2. Las cuentas de correo asignadas a cada usuario deben ser utilizadas de forma primaria para el envío y recepción de documentación oficial de la Universidad Tecnológica de Panamá.
3. El envío y recibo de mensajes de correo electrónico está sujeto a que exista una relación previa con la persona que lo envía.
4. Las cuentas de propósitos o uso general están predispuestas al recibo de correo basura por la naturaleza de las mismas, por lo tanto, no son objeto de investigación.
5. Se prohíbe responder a correo no solicitado o de fuente desconocida, aún cuando exista un procedimiento para remover su dirección de la lista de correo.
6. Nunca se debe abrir archivos adjuntos de correo recibidos de un origen desconocido o que de alguna forma se tenga sospecha de ellos. Ni tampoco se deben abrir archivos ejecutables, archivos cuya extensión desconozca o cuyo propósito haya sido vinculado con publicaciones de correo electrónico con virus.
7. El anuncio o publicación de una dirección de correo electrónico supone el recibo de correo basura de cualquiera índole, por lo tanto no es objeto de investigación.
8. No tomar ninguna acción indicada en el mensaje de correo basura (por ejemplo, distribuir alertas de virus) sin contactar primero a PANNet.
9. Reportar todos los casos de mensajes de correos basuras, como ejemplo, distribución de material ilegal u ofensivo, ataques de negación de servicio, entre otros) a PANNet.
10. Al suscribirse a una lista de envíos de correo debe conocer a profundidad los términos y condiciones del uso de las direcciones de los subscriptores ya sea que estas estén o no sujetas a venta o contrato con otras partes.
11. Al suscribirse a una lista debe conocer la naturaleza y el volumen del correo recibido, esto incluye el tópico tratado y la frecuencia de envíos de la lista, además debe existir un procedimiento claramente establecido para removerse
12. Para crear una lista de distribución, la misma debe responder a un proyecto o comisión de trabajo y ser avalada por la autoridad máxima de la unidad académica, de investigación o administrativa a la cual pertenece el funcionario.
13. Se prohíbe suscribir a cualquier persona a una lista de correos sin su permiso.
14. El uso e implementación de foros es libre, sin embargo se restringe en ellos el uso de las direcciones electrónicas propias del foro.

15. Se prohíbe el envío de correo electrónico no solicitado en cualquiera de sus formas (incluyendo cartas cadenas).
16. El tamaño del archivo adjunto estará limitado a las disposiciones de PANNet, basados en el soporte tecnológico.
17. Solamente la Administración es la autorizada para enviar información de eventos y actividades propias de la Universidad Tecnológica de Panamá a través del procedimiento establecido
18. Se prohíbe ocultar la identidad del emisor o la falsificación de los encabezados de correo.
19. Se prohíbe configurar el campo *Reply-To* a alguna dirección ajena sin su consentimiento.
20. Se prohíbe realizar ataques de negación de servicio, por ejemplo enviar enormes cantidades de correos con el propósito de sobrecargar los recursos del destinatario.
21. Se prohíbe enviar correo con contenido ilegal, según lo definido en las políticas de la institución.

• **Navegación en el WWW y recursos de Internet.**

1. En sitios Web publicados por la Universidad no debe haber:
 - a. Contenido que sea ilegal, difamatorio, abusivo o de acoso a otros.
 - b. Contenido que infrinja los derechos de propiedad intelectual de terceros.
 - c. Software que distribuya spam, virus, o programas que causen daño a computadoras o redes.
2. En sitios Web publicados por la Universidad no se debe permitir:
 - a. Suplantar a otro; hacerse pasar por otra persona.
 - b. Conexiones de puerta trasera.
 - c. Utilizar en cualquier nombre de dominio una marca registrada perteneciente a otro individuo u organización.
3. No debe conectarse a un sitio Web donde el acceso está sujeto a una tarifa.
4. Si el Espacio Web genera tráfico anormalmente alto, PANNet investigará y donde cualquiera de estos términos sea trasgredido, tomará acciones apropiadas.
5. Descarga de archivos con derecho de autor (copyright).
 - a. La descarga de archivos con copyright es responsabilidad propia del usuario y la misma estará sujeta a sanciones dispuestas por la Ley y el Estatuto Universitario y las leyes nacionales que legislen al respecto.
6. Acceso a sitios pornográficos.
 - a. El acceso a sitios pornográficos no está permitido, y el usuario de la red que se le compruebe el acceso intencional y descarga de material de este tipo será sancionado de acuerdo a la Ley, Estatutos y Reglamento Universitario.

• **Instalación de servidores DHCP, NAT, Proxies, Firewalls, IDS, y otros.**

1. El uso de DHCP se permitirá en condiciones que amerite PANNet y el mismo debe seguir las condiciones y acciones que PANNet estime pertinentes. PANNet deberá tener acceso al DHCP en todo momento.
2. PANNet es el único autorizado para instalar un sistema IDS. Si hay una unidad que solicite instalar y administrar un IDS, PANNet podrá hacerlo siempre y cuando la Unidad solicitante permita el libre acceso por parte de PANNet en el momento que así se requiera. PANNet establecerá los IDS que podrán utilizarse y las configuraciones pertinentes.
3. El uso de proxies y firewalls perimetrales serán autorizados por PANNet.

• **Condiciones de uso para la Red Inalámbrica.**

1. Objetivo.

Las condiciones de uso presentadas en este documento definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de una red inalámbrica en la Universidad Tecnológica de Panamá. Todas las políticas y reglamentaciones de uso de la Red UTP aplican a la red inalámbrica.

2. Alcance.

Estas condiciones de uso abarcan a todos los dispositivos de comunicación inalámbrica (por ejemplo: computadores portátiles, PDA, etc.) con capacidad de transmitir mensajes de datos y que se encuentren conectados a la Red UTP.

3. Condiciones de uso.

a. Identificación.

- Para hacer uso de la red inalámbrica se debe ser miembro de la comunidad universitaria.
- Todos los usuarios de la red inalámbrica deben autenticarse para hacer uso del servicio. Para tales efectos, se debe hacer uso del sistema de autenticación vigente, establecido por PANNet.
- Se debe registrar en PANNet, la dirección física de todas las tarjetas inalámbricas que van a acceder la red inalámbrica.

b. Seguridad.

- Toda información transferida a través de este medio viaja de manera INSEGURA por tanto la UTP no se hace responsable de la información trasegada por este medio.
- PANNet determinará las medidas mínimas de seguridad para usar las redes inalámbricas. El estándar podría variar dependiendo de la tecnología disponible y del grado de riesgos y amenazas.

- No se debe realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal y no es permitido por la UTP.

c. Tecnología.

- La red inalámbrica de la Universidad Tecnológica de Panamá usa el estándar 802.11 (en cualquiera de sus denominaciones, de acuerdo al soporte tecnológico establecido por PANNet). Las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar.
- Solo será soportado el protocolo IP en la red inalámbrica.
- PANNet limitará los anchos de banda de cada conexión según sea necesario para asegurar la confiabilidad y desempeño de la Red UTP y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios.
- No se permite la operación ni instalación de “puntos de acceso” (access points) conectados a la red cableada de la UTP sin la debida autorización por parte de PANNet.
- No se permite configurar las tarjetas inalámbricas ni ningún otro dispositivo que funcionen como “puntos de acceso”.