



**Políticas de uso de la Red Administrativa**

**en la**

**Universidad Adventista de las Antillas**

Esta política se ha establecido para proveer guías para el uso apropiado de las facilidades y sistemas de información de computadoras de la Universidad. Aunque esta política no cubre todos los aspectos acerca del uso de las computadoras, ofrece los principios básicos por los que se deben guiar los empleados y estudiantes de la Universidad y establece puntos específicos que sirven como referencia. Esta política será modificada a la medida en que nuevas interrogantes o situaciones surjan.

En apoyo a la misión de la Universidad para proveer asistencia en llevar a cabo el rol de la enseñanza e investigación rica en recursos que contribuyan a la innovación, cumplir con los objetivos administrativos y proveer un servicio al público de alta calidad, la Universidad provee, libre de costo, servicios de computadoras y recursos de información a todos los empleados, facultad, estudiantes registrados y visitantes autorizados.

Los sistemas de computadoras y redes son herramientas de trabajo que proveen acceso a información en y fuera del recinto, como también la habilidad de proveer comunicación con otros usuarios generalmente en todo el mundo. Este acceso es un privilegio y no un derecho y requiere que los usuarios actúen responsablemente.

A cada individuo autorizado se le proveerá una cuenta y una contraseña para poder tener acceso y hacer uso de los sistemas. Usted es responsable por todo el uso de computadora en su cuenta. Cuando se detecte alguna actividad ilegal, la Universidad responsabilizará a la persona que tiene asignada esa cuenta. Para protegerse, usted deberá prevenir el acceso no autorizado manteniendo su contraseña secreta y cambiándola periódicamente.

Individuos que, actuando en forma negligente y con intención, usen la cuenta de otro empleado para este tipo de acción o uso inapropiado, serán procesados bajo las reglas y reglamentos internos de la Universidad y todas las demás leyes y estatutos criminales estatales o federales que le apliquen, según sea el caso.

Aunque los sistemas operativos en la red que controla la Universidad están diseñados para restringir la habilidad de que personas no autorizadas puedan interferir con los privilegios de los usuarios, ningún sistema de computadoras que se comparte se encuentra a prueba de los esfuerzos de otros para destruirlo. Ninguno de los sistemas de computadoras, incluyendo los sistemas operativos de la Universidad podrán ser modificados sin la debida autorización del Director del Departamento de Servicios de Información y Tecnología (“ITS”). Hacer cualquier cambio o modificación al sistema operativo es fundamentalmente lo mismo que destruir las computadoras, sistemas y propiedad de la Universidad. Se prohíbe la conexión a la red administrativa de sistemas ajenos a la Universidad, incluyendo laptops, módems, “routers”, consolas de juego, puntos de acceso inalámbrico (“wireless AP”), “streaming box”, y obtener o bajar información de recursos no aprobados.

Está completamente prohibido el uso o la instalación de programas ajenos a los sistemas de computadoras de la Universidad, aún cuando se tenga licencia para ello. Cualquier programa o aplicación necesaria para llevar a cabo su ejecutoria eficientemente será provisto e instalado por personal autorizado de la UAA, con la aprobación y conocimiento del Director del Departamento de Servicios de Información y Tecnología (“ITS”).

Todo documento oficial deberá ser escrito o creado usando “Microsoft Office”, aplicación aprobada y de uso legal por la Universidad. La Universidad no promueve el uso de otras aplicaciones de oficina. Documentos existentes o creados usando otras aplicaciones deberán ser convertidos a un formato reconocido por “Microsoft Office” lo antes posible.

### **Reglas para el uso de los recursos de información:**

1. El uso de los sistemas o facilidades incluyendo las redes o acceso a los sistemas por personas ajenas al

recinto como por ejemplo, personas no empleadas o ex-empleadas está totalmente prohibido. Ninguna persona podrá autorizar a otra persona a hacer uso de los sistemas sin la previa autorización del supervisor inmediato y sin la autorización por escrito del Director del Departamento de Servicios de Información y Tecnología (“ITS”).

2. Obedezca todas las leyes, reglas, obligaciones y mensajes del Departamento de Servicios de Información y Tecnología (“ITS”) en la oficina, el salón de clases y laboratorios.
3. Los usuarios deberán respetar los derechos de otros usuarios, la integridad de los sistemas y los recursos físicos relacionados. No interfiera con los derechos de otros. Muchos miembros de la comunidad universitaria usan estos recursos y dependen de los mismos para poder llevar a cabo sus tareas y para almacenar información importante y confidencial, incluyendo programas de computadoras. Nunca obtenga acceso al sistema usando la contraseña de otra persona y no use cuentas que no han sido asignadas a usted. Está prohibido y ética-mente incorrecto, que individuos tengan acceso o intenten tener acceso o miren cualquier cuenta para la cual ellos no tienen autorización. Tal uso es prohibido y se considera robo de los recursos. Está también prohibido interrumpir intencionalmente, atrasar, poner en peligro o exponer el trabajo de otra persona u operaciones de la Universidad.
4. Mantenga su contraseña secreta y no la comparta con nadie. Cámbiela frecuentemente y si usted sospecha que alguien conoce su contraseña, cámbiela inmediatamente.
5. Nunca intente penetrar o modificar los sistemas de seguridad ni los sistemas operativos o conectar otra computadora a la red de la Universidad sin la debida autorización.
6. El comportamiento abusivo y/o “bullying” no esta permitido. No use la computadora para acosar, hostigar o molestar a otros; esto es muy importante en el uso de mensajes electrónicos, conferencias y boletíneros. El correo electrónico se deja regir por los mismos estándares que gobiernan cualquier otra forma de correo. No imprima o transmita mensajes obscenos, ofensivos, vulgares, abusivos o amenazantes. Material obsceno, derogatorio, o en contra de la filosofía de la Universidad, impreso o visible en el monitor de la computadora está prohibido.
7. Los usuarios deberán respetar las necesidades de los demás y los límites de los recursos de computadoras cuando usan los sistemas de información. Usted no es el único utilizando estos recursos. Use los recursos sabiamente y con prudencia, termine cuanto antes le sea posible para que otros puedan también hacer uso de ellos. Siempre salga de su cuenta: (a) cuando sale o va a estar fuera de la oficina por más de 30 minutos. Apague la computadora y monitor al final del día, o antes de salir del trabajo.
8. Si alguien le informa que lo que usted está haciendo está causando problemas al sistema, inmediatamente detenga lo que está haciendo y no repita tal acción.
9. No intente aumentar los derechos de usted ni los de otra persona, para sustituir otro usuario con el suyo o para obtener acceso no autorizado al sistema.
10. “Cracking” o “Hacking” se define como el acceso no autorizado o intentar el acceder un sistema o computadora o la base de datos sin autorización para hacerlo. Esta definición incluye los intentos no autorizados para violar las técnicas de seguridad establecidas para proteger los sistemas computarizados como también la experimentación no autorizada de los sistemas de equipos, programación y comunicaciones de los sistemas. Esta definición aplica aún cuando exista o no cualquier intento de obtener, alterar o destruir información en específico. Hacer o simplemente intentar el acto de “cracking” o “hacking” está totalmente prohibido y la persona responsable por dicho acto será

penalizada.

11. Las conexiones vía laptops, módems, “routers”, consolas de juego, puntos de acceso inalámbrico (“wireless ap”), “streaming box” y/o cualquier equipo que utilice la red de la UAA están prohibidas sin la debida autorización del Departamento de Servicios de Información y Tecnología (“ITS”). Estas conexiones pueden afectar los sistemas de la Universidad ya que no proveen la protección que se requiere o afecta el tráfico de información entre dispositivos.
12. La Universidad provee el servicio de Internet como una herramienta o recurso de apoyo para la educación e investigación consigo misma y con otras instituciones académicas para proveer acceso a recursos únicos y proveer la oportunidad de llevar a cabo trabajos colaborativos. La Universidad apoya este propósito, pero el uso de los recursos de Internet e Intranet para otros propósitos como juegos, “file sharing”, bajar o grabar películas o música está prohibido.
13. Obedezca y respete los derechos del autor protegidos por las leyes y use los recursos computarizados consistentemente con la misión de la Universidad. Gran parte del material o información que aparecen en el Internet es protegida aún cuando el autor no lo expresa. Los usuarios deberán asumir que el material está protegido y no copiarlo o diseminarlo sin autorización. La propiedad y el derecho a la privacidad pueden ser violados si se usan archivos o información que pertenecen a otros sin la debida autorización. Además de violar la ley, plagiarismo de material protegido por los derechos del autor es una violación del código de ética de la Universidad. Estos derechos también aplican a muchos de los programas para los que la Universidad tiene licencias con limitaciones específicas en el uso de los mismos.
14. No interfiera con la misión de la Universidad ni intente hacerle daño a la integridad del sistema computarizado.
15. La administración de la Universidad se reserva el derecho de acceder y examinar los archivos y las secciones actuales de uso de computadoras o de cualquier usuario para investigar violaciones o sospechas de violaciones de seguridad o de las políticas, interacciones que puedan contribuir al pobre funcionamiento u operaciones de las computadoras, o el no-funcionamiento de las mismas. Los usuarios no tendrán expectativas de privacidad con relación a sus archivos, base de datos o comunicaciones.

El personal administrativo del Departamento de Servicios de Información y Tecnología (“ITS”) tiene la responsabilidad de asegurarse de que la aplicación de estas regulaciones sea cumplida. Por lo tanto, ellos pueden referir casos a la administración de la UAA para que se contacte a las agencias pertinentes para la debida acción legal, dependiendo de las circunstancias y severidad de la situación.

Las consecuencias o penalidades que resulten por violaciones a estas regulaciones incluyen pero no se limitan, a:

- (a) **Advertencia:** Advertirle al usuario, con el entendimiento de que existen regulaciones y que cualquier recurrencia de ese tipo o patrón de comportamiento resultará en acción disciplinaria. Antes de tomar cualquier acción, se le brindará la oportunidad al usuario de proveer una respuesta o responder a las alegaciones.
- (b) **Pérdida de privilegios de uso:** Limitar o suspender los privilegios del usuario, incluyendo restricción de uso de los sistemas y facilidades por un período especificado. El Director del Departamento de Servicios de Información y Tecnología (“ITS”) puede suspender algunos o todos los privilegios de un usuario en caso de que exista la posibilidad de amenaza a la integridad de los recursos de información de

la Universidad con o sin notificación previa al usuario.

- (c) **Restitución de daños:** El usuario será responsable de pagar los daños de reparación del sistema y de cualquier material relacionado tales como: equipo, programas y facilidades.
- (d) **Despido, separación o expulsión de la Universidad:** Dependiendo de la severidad de la violación, si la persona es un empleado podrá ser inclusive despedido o separado de su relación de empleo con la Universidad.
- (e) **Referido a las autoridades pertinentes:** Cuando la conducta del empleado que usa los sistemas de información es tal que pudiera resultar en cometer un delito, la UAA en cumplimiento de su deber legal de así hacerlo, referirá el asunto para investigación por las autoridades pertinentes.

En caso de que necesite aclaraciones o tuviese preguntas en cuanto a esta política, es altamente recomendable que se comunique con el Director del Departamento de Servicios de Información y Tecnología (“ITS”) por correo electrónico [its@uaa.edu](mailto:its@uaa.edu) o teléfono 787-834-9595x2700.

La Universidad no se responsabilizará por pérdida de datos o la falla de cualquier instrumento de seguridad o privacidad o el mal funcionamiento de los mismos.

## **Apéndice I – Facilidades Tecnológicas**

### **Almacenamiento Disco privado (P:) y departamentales (X:)**

Cada usuario recibe acceso a un disco privado, que solo puede ser accedido a través de la red por el usuario. Una cuota máxima es impuesta para prevenir que el servidor se llene solo por algunos usuarios. Este disco se conoce como disco (P:).

En algunos Departamentos también existe un disco compartido, conocido como disco (X:) para almacenar documentos Institucionales que pueden ser accedidos por todo los usuarios de este departamento.

Recuerden que el Personal de ITS tiene privilegios administrativos para acceder a cualquier documento almacenado en estos discos. No almacene documentos personales, fotos o música, estos discos solo deben ser utilizados para almacenar documentos institucionales.

### **Mantenimiento de equipos**

Reparaciones - El mantenimiento de equipos tecnológicos es coordinado por el Departamento de Servicios de Información y Tecnología (“ITS”) en conjunto con suplidores externos.

Remoción de programas – La universidad se reserva el privilegio de remover sin previo aviso cualquier programa y/o material que se considere ilegal de cualquier equipo que acceda nuestra red de computadoras.

## **Apéndice II – Redes Sociales**

Uso de Redes Sociales en la UAA:

- Mantenga las cuentas personales y profesionales separadas.
- No añada estudiantes en su cuenta personal.
- No comparta información personal en su cuenta profesional.
- Si tiene acceso a redes sociales no debe hacer uso de cuentas personales en horas de oficina.

## **Apéndice III – Detalles ITS**

- Con la excepción de las computadoras portátiles, los equipos computadorizados no deben ser movidos o re-ubicados sin la debida autorización del Departamento de Servicios de Información y Tecnología (“ITS”).
- Sin excepción alguna los estudiantes no deben conectar equipos personales en la red administrativa de la UAA.
- Si usted accidentalmente daño, o encontró algún equipo defectuoso, favor de notificarlo al supervisor de laboratorio o área en la que se encuentra el equipo y este a su vez debe informarlo al Departamento de Servicios de Información y Tecnología (“ITS”).
- La UAA usa filtros de contenido en la red para asegurar, monitorear y limitar ciertas paginas por su seguridad y en apoyo a las creencias de la UAA. Sin embargo, si siente que equivocadamente alguna pagina a sido bloqueada por error debe notificarlo al Departamento de Servicios de Información y Tecnología (“ITS”).
- El sistema operativo oficial instalado en las computadoras institucionales sera (según lo permita la computadora) Windows 7 Pro en ingles para computadoras de Escritorio. Cualquier compatibilidad de otro sistema operativo, arquitectura o apoyo técnico de parte de ITS no sera garantizada.
- El “Web Browser” oficial en la UAA sera Internet Explorer.