POLÍTICA PARA USO DE TECNOLOGÍAS DE INFORMACIÓN

CÓDIGO: **PO-CGTI-207**

REVISIÓN: **09**

FECHA DE APROBACIÓN: **13 DE MARZO DE 2006**
FECHA DE REVISIÓN: **27 DE ABRIL DE 2017**

	NOMBRE	PUESTO	FIRMA
ELABORÓ	GUSTAVO ALONSO GUTIÉRREZ ZAPATA	COORDINACIÓN DE REDES Y COMUNICACIONES	
	JAVIER ALBERTO ORDAZ NÁJERA	JEFATURA DE FUNCIÓN DE OPERACIÓN DE LA REDUACJ	
	SERGIO EDUARDO SOTO GALINDO	JEFATURA DE FUNCIÓN DE ADMINISTRACIÓN DE LA REDUACJ	
	OSCAR GERMAN SOTO FLORES	JEFATURA DE FUNCIÓN DE ADMINISTRACIÓN DE SERVIDORES	
	LUIS ALBERTO GARDEA	COORDINACCIÓN DE OPERACIÓN Y SISTEMAS	
	MARTHA URBINA PRIETO	JEFATURA DE FUNCIÓN DE ADMINISTRACIÓN DEL SISTEMA TELEFÓNICO	
	JOSÉ MUCIO LEINER DURANTE	JEFATURA DE FUNCIÓN DE DIAGNOSTICOS DE TI	
	EDMUNDO GARCÍA SOTO	JEFATURA DE FUNCIÓN DE OPERACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO	
	SILVIA MAGALLANES VALLEJO	JEFATURA DE VIDEOCONFERENCIAS	
	CELINA RODRÍGUEZ MATAMOROS	COORDINACIÓN DE DESARROLLO DE SISTEMAS	
	FERNANDO ESTRADA SALDAÑA	COORDINACIÓN DE DESARROLLO DE TECNOLOGÍA EDUCATIVA	
	LAURA ESTHER STEVENS CARRERA	JEFATURA DE CENTRO DE ATENCIÓN Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN	
REVISÓ	PATRICIA MÉNDEZ LONA	COORDINACCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN	
	LILIANA VICTORIA RAMOS MARTÍNEZ	SUBDIRECCIÓN DE PLANEACIÓN DE LA MEJORA DE LA GESTIÓN	
APROBÓ	ÁNGEL FERNANDO GÓMEZ MARTÍNEZ	DIRECCIÓN GENERAL DE PLANEACIÓN Y DESARROLLO INSTITUCIONAL	

Contenido ***Pág.***

Anexos

1.0 PROPÓSITO

Establecer los lineamientos para el uso correcto del equipo de cómputo, y de los servicios de tecnología de información (Internet, Intranet, SIIv2, bases de datos, software y sistemas de soporte académico/administrativo) en la UACJ y sensibilizar al usuario para el mejor aprovechamiento de los recursos informáticos, tomando en cuenta como factor importante la seguridad de la información ya que el mal uso de éstos recursos expone a la Universidad a riesgos tales como ataques a sistemas de información, infraestructura de TI, sistemas de comunicaciones y/o robo de información.

2.0 ALCANCE

Esta política es aplicable a la Comunidad Universitaria, así como a contratistas, consultores y visitantes en la UACJ, en relación al uso y manejo del equipo, servicios de TI e infraestructura de cómputo y comunicaciones que utilizan los recursos informáticos de la UACJ.

3.0 DEFINICIONES

3.1 **Cifrado.** Es la condición de cierta información al aplicarse algún método criptográfico utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

3.2 **ConectaUACJ.** Plataforma institucional que proporciona servicios de colaboración, comunicación, almacenamiento y redes sociales.

3.3 **Correo electrónico.** Sistema de mensajería que permite la transmisión y envío de mensajes de texto o contenido multimedia embebido, a través de redes de datos.

3.4 **Direcciones IP.** Identificador numérico único que se le designa a algún elemento en una red en Internet.

3.5 **Equipo de cómputo**. Todo dispositivo electrónico con el cual se pueda acceder a los recursos informáticos.

3.6 **Extranet.** Sistemas de información y comunicaciones de la RedUACJ que se acceden desde una red externa a través de Internet utilizando una conexión de red privada virtual VPN.

3.7 **Información sensible**. Toda información que sea clasificada como confidencial en base a las políticas institucionales.

3.8 **Internet.** Red mundial de comunicaciones que interconecta redes académicas, corporativas y comerciales.

3.9 **Intranet.** Sistemas de información y comunicaciones localizados dentro de la RedUACJ.

3.10 **Nombres de dominio.** Identificador alfanumérico que se le designa a algún elemento en una red en Internet.

3.11 **RedUACJ.** Sistema de dispositivos de comunicaciones y de cómputo interconectados entre sí, que proveen acceso a servicios informáticos internos y externos.

3.12 **Script.** Archivo de texto o programa que contiene una secuencia de instrucciones o comandos que son interpretados por algún sistema operativo en particular, o alguna aplicación, con el fin de automatizar una tarea cuando se ejecuta.

3.13 **Sistema de información.** Programa informático diseñado para el manejo de datos de acuerdo a un modelo de negocio.

3.14 **SIIv2.** Sistema Integral de Información versión 2. Se refiere al conjunto de programas informáticos desarrollados para automatizar los procesos operativos y el manejo de la información en la Universidad.

3.15 **SPAM.** Envío o recepción masiva de mensajes de correo no autorizado o no solicitado.

3.16 **Malware.** Programa informático que contiene código malicioso cuyo fin es causar algún daño en los sistemas de cómputo.

3.17 **VPN.** Acrónimo por sus siglas en inglés de Virtual Private Network (Red Privada Virtual), la cual se refiere a un sistema que permite establecer conexiones seguras a través de redes públicas para conectarse a una red privada.

4.0 POLÍTICA

4.1 Disposiciones Generales Aplicables a la Comunidad Universitaria

4.1.1 El personal administrativo y académico podrá hacer uso del Internet para aplicarlo como instrumento de trabajo; para acceder a información técnica, científica, artística, o cualquier otra relacionada con temas de interés para la Universidad, siempre y cuando dicho personal cuente con el perfil y la autorización del Director General o responsable de la dependencia correspondiente. Para los alumnos podrán hacer uso de Internet como instrumento de apoyo a sus actividades

académicas siempre y cuando cumplan con las disposiciones establecidas en esta política.

4.1.2 Los datos o información que los empleados generen usando como fuente los sistemas de información propiedad de la Universidad, pertenecen a la misma, y deberán alinearse a la normativa establecida a nivel federal, estatal, municipal e institucional.

4.1.3 Las direcciones de correo electrónico, nombres de dominio, direcciones IP inherentemente son bienes intangibles de la Universidad, por lo que cualquier transacción que se realice con los mismos será considerada como realizada en su representación, salvo se exprese lo contrario en dichas transacciones. No se deben utilizar dichos recursos para propósitos que puedan influir negativamente en la imagen de la Universidad.

4.1.4 Los usuarios de los sistemas de información deben acceder solamente a información relacionada con sus funciones. Para acceder a los sistemas de información deberá existir autorización del responsable de la información a través de una solicitud física o digital.

4.1.5 La Coordinación General de Tecnologías de Información es corresponsable de la confidencialidad con el encargado de la información y responsable de la integridad y disponibilidad en los sistemas administrados directamente por la CGTI. Referente a los sistemas de información hospedados dentro de la infraestructura de TI, la CGTI será responsable en lo establecido en los acuerdos de nivel de servicio.

4.1.6 Es responsabilidad exclusiva del usuario, la información contenida en cualquier dispositivo de almacenamiento que esté bajo su responsabilidad dentro de la UACJ. (disco duro, disco compacto, memoria usb, etc.).

4.1.7 Es responsabilidad exclusiva del usuario la realización de respaldos de la información y/o correo electrónico institucional contenido en cualquier dispositivo de almacenamiento que esté bajo su responsabilidad dentro de la UACJ.

4.1.8 Es responsabilidad exclusiva del usuario que los equipos de cómputo bajo su resguardo se encuentre en un ambiente físico seguro.

4.1.9 Cualquier información que los usuarios consideren sensible o vulnerable deberá solicitar apoyo técnico a través del Centro de Atención y Servicios de Tecnologías de Información (CAST) en la extensión 2278, para determinar si procede la solicitud en base a las políticas institucionales y proporcionar el apoyo de protección de la información.

4.1.10 Todos los empleados son responsables de ejercer el buen juicio en lo que respecta al uso del equipo para cuestiones personales. Cada Responsable de UR, es

responsable de crear sus propios criterios y/o guías para el uso personal del Internet siempre y cuando dichos criterios no se contrapongan a las políticas y/o reglamentos institucionales. En la ausencia de dichos criterios y/o políticas, los empleados deberán de acatar lo que establezca su Dirección General o Coordinación General correspondiente.

4.1.11 En caso que algún Docente o Administrativo requiera acceder a algún servicio o sistema de la Universidad que no sea público, pero que esté disponible en la RedUACJ, podrá acceder a dicho recurso a través del uso de una conexión VPN solicitando el servicio a la CGTI.

4.1.12 La CGTI no está obligada a la instalación y configuración de software, reparación o mantenimiento de equipo de cómputo que no sea propiedad de la Universidad.

4.1.13 La publicación de los mensajes que tengan que ver con las labores académicas-administrativas de la Universidad deberán utilizar los medios oficiales y alinearse a las políticas aplicables.

4.1.14 Las políticas y lineamientos definidos por otras instancias de la UACJ, para el uso de un servicio de TI en específico, no deberán contraponerse con lo establecido en esta política.

4.1.15 Es facultad exclusiva de la CGTI la gestión y administración del software institucional y no se responsabiliza del software adquirido o instalado por otra instancia

4.1.16 Una vez que la CGTI reciba la notificación oficial de baja de un empleado, la cuenta quedará inactiva inmediatamente. En cuanto a la información contenida en la cuenta estará disponible un mes posterior a la fecha de la notificación.

4.1.17 Exclusivamente los alumnos con estatus de inscrito tendrán derecho a los servicios de conectaUACJ.

4.1.18 Para los alumnos con estatus diferente a inscrito, la cuenta de acceso permanecerá activa para ingresar únicamente a los portales institucionales pertinentes.

4.2 Disposiciones Generales Aplicables a la Coordinación General de Tecnologías de Información

4.2.1 Con el propósito de reforzar la seguridad y dar mantenimiento a los servicios que corren en la RedUACJ, personal autorizado de la UACJ tiene la facultad de monitorear cualquier equipo de cómputo, sistemas y/o tráfico de datos en cualquier momento, pudiendo capturar evidencia que se considere necesaria para la resolución de algún incidente de seguridad y/o para evidenciar el uso del recurso. El

resultado de dicho monitoreo quedará alineada a las leyes gubernamentales vigentes aplicables.

4.2.2 La UACJ se reserva el derecho de auditar redes y/o sistemas en forma periódica para asegurar el cumplimiento de las presentes políticas.

4.2.3 Solamente personal autorizado y debidamente identificado por la Coordinación General de Tecnologías de Información, podrá dar mantenimiento preventivo y/o correctivo a los equipos de cómputo asignados al personal administrativo y docente. En equipo de cómputo académico (centros de cómputo y laboratorios) es responsabilidad de los institutos y divisiones multidisciplinarias asignar al personal autorizado para realizar los mantenimientos preventivos y/o correctivos. En caso de Biblioteca es responsabilidad de la Coordinación del Centro de Servicios Bibliotecarios.

4.2.4 Solamente el personal adscrito a la CGTI podrá realizar la apertura de equipos de cómputo que estén bajo su responsabilidad.

4.2.5 Solamente el personal adscrito a la Coordinación de Redes y Comunicaciones podrá instalar y reubicar equipo de comunicaciones y aparatos telefónicos propiedad de la UACJ.

4.2.6 Únicamente los servidores administrados por la CGTI que requieran acceso público, podrán ser accedidos desde el Internet. La Coordinación General de Tecnologías de Información se reserva el derecho a identificar servidores no autorizados y a desconectarlos de la red hasta que se justifique el acceso público.

4.2.7 La CGTI se reserva el derecho de controlar y restringir el contenido al que se accede a través de Internet o Internet 2 con el fin de optimizar el recurso de ancho de banda, así como bloquear contenido malicioso que pudiera llegar por redes externas.

4.2.8 Con el propósito de proporcionar servicio de soporte y/o mantenimiento al equipo de cómputo, personal de la CGTI podrá tomar control remoto del equipo en cuestión con previa autorización del usuario.

4.2.9 Personal de la CGTI deberá realizar mantenimientos preventivos requeridos en base a los procedimientos establecidos en el Sistema de Gestión de la Calidad, con el fin de maximizar la disponibilidad de la infraestructura.

4.2.10 La CGTI dará a conocer la presente política a través de los medios de difusión oficiales de la Universidad o cualquier otro medio efectivo que sirva para éste propósito.

4.3 Disposiciones en Materia de Seguridad y Propiedad de la Información Aplicables a la Comunidad Universitaria

4.3.1 La interface de usuario para acceder a información contenida en sistemas de información y comunicaciones debe tener a la vista una clasificación de confidencialidad, de acuerdo a lo estipulado en los criterios de confidencialidad de las políticas institucionales, en caso de existir. Ejemplos de información confidencial incluye pero no limita a: información privada, estrategias corporativas, datos de trabajos de investigación, especificaciones, lista de clientes, configuración de equipos de comunicaciones, servidores etc. Cada empleado debe tomar las medidas necesarias para prevenir acceso no autorizado a dicha información.

4.3.2 Las claves de acceso se deben mantener seguras y no se deberán compartir. Cada usuario autorizado a una cuenta y clave de acceso es responsable de la seguridad de las mismas.

4.3.3 Es responsabilidad del usuario cambiar periódicamente su clave de acceso, y podrán ser cambiadas a petición del usuario o a petición del administrador de servidores si se cree que la cuenta pudo haber sido comprometida.

4.3.4 Las claves de acceso de las cuentas para la administración de los sistemas se deberán cambiar cada semestre o si se cree que la cuenta pudo haber sido comprometida.

4.3.5 Es responsabilidad del usuario que las computadoras de escritorio, portátiles y estaciones de trabajo encendidas y que permanezcan inactivas deberán asegurarse a través de una clave de acceso para firmarse al sistema operativo o, una vez firmado, deberá contar con una clave de acceso en el salva-pantallas que se deberá activar cuando no esté en uso el equipo. Si es necesario, se deberá usar cifrado de la información contenida en el disco duro del equipo de cómputo.

4.3.6 Todos los equipos de cómputo de uso administrativo deberán de estar en el dominio UACJ.MX.

4.3.7 En caso de los equipos dentro del dominio UACJ tendrán que utilizar el antivirus institucional y cumplir con las políticas establecidas por el administrador del dominio.

4.3.8 Todos los medios utilizados por el usuario para conectarse a los sistemas de Internet, Intranet, Extranet y relacionados, incluidos pero no limitados a: equipo de cómputo, software, sistemas operativos, medios de almacenamiento y cuenta de correo electrónico proveído por la UACJ deben estar protegidos a través de un software de monitoreo antivirus con una base de datos de virus actualizada, a menos que haya una política de excepción aplicable.

4.3.9 Los usuarios que requieran confidencialidad de los datos que transmiten a través de su conexión de red, podrán solicitar una conexión segura a través del Centro de Atención y Servicios en Tecnologías de Información.

4.3.10 Es responsabilidad de la Subdirección de Recursos Humanos, notificar a la CGTI las bajas de personal con el fin de efectuar la gestión de las cuentas de usuarios en los sistemas de información y/o comunicaciones.

4.3.11 Es Responsabilidad del encargado de la U.R que solicito los derechos de acceso Administrador del Módulo del Sistema de Información notificar a la CGTI el cambio del empleado para poder mantener la integridad de la información.

4.3.12 Los usuarios de los recursos tecnológicos propiedad de la UACJ no deberán involucrarse bajo ninguna circunstancia en cualquier actividad ilegal definida por leyes locales, estatales, federales o internacionales.

4.4 Actividades de Uso Inaceptable del Equipo de Cómputo o Recursos Informáticos Propiedad de la UACJ.

4.4.1 **Actividades de Sistemas y de Red.** Las siguientes actividades están estrictamente prohibidas sin excepciones:

A) Ingresar de manera no autorizada a los sistemas de autenticación del usuario o la seguridad de cualquier equipo de cómputo, de comunicaciones o cuenta de acceso.

B) Violaciones a los derechos de autor, secretos de marca, patentes u otra propiedad intelectual, o regulaciones o leyes similares, incluidas pero no limitadas a; la instalación o distribución de productos o software "pirata" que no esta adecuadamente licenciado para su uso por la UACJ.

C) Copia sin autorización de material con derechos de autor, incluido pero no limitado a; digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos reservados, música con derechos registrados y la instalación de cualquier software con derechos reservados para el cual la UACJ o el usuario final no tenga una licencia válida.

D) La introducción de programas maliciosos en la red o servidores o en cualquier equipo de cómputo de la UACJ (por ejemplo virus, gusanos, troyanos, bombas de correo electrónico, etc).

E) Revelar sus claves de acceso a otros o permitir el uso a su(s) cuenta(s).

F) Usar recursos informáticos de la UACJ para transmitir material relacionado con el acoso sexual o amenazas físicas, verbales o de cualquier otro tipo.

G) Hacer ofertas ajenas a los intereses de la UACJ, fraudulentas o no, de productos, bienes o servicios.

H) Explotar o generar hoyos de seguridad, causar interrupciones, trastornos en las comunicaciones o sistemas de información de la RedUACJ. La explotación y/o generación de hoyos de seguridad en los sistemas de cómputo y/o sistemas de información incluyen, pero no se limitan a:

- ❖Acceder a información para la cual la persona no sea autorizada.
- ❖Acceder a sistemas de información o al sistema operativo de cualquier dispositivo de cómputo con una cuenta para la cual no tenga autorización el usuario, a menos que estas acciones constituyan parte de los deberes del usuario.
- ❖Sustraer componentes internos del equipo de cómputo.

I) Para propósitos de ésta sección, interrupciones o trastornos en las comunicaciones incluyen, pero no se limitan a:
- ❖Análisis no autorizado del tráfico de la red,
- ❖Inundación de paquetes de cualquier tipo, denegación de servicio, inclusión de paquetes falsos en la red (packet spoofing), inclusión de información de enrutamiento mal intencionada.

J) El escaneo de puertos o el escaneo de hoyos de seguridad está expresamente prohibido a menos que sea autorizado y realizado por la Coordinación General de Tecnologías de Información.

K) Ejecutar cualquier forma de monitoreo de la RedUACJ, incluyendo la intercepción de cualquier información que no sea dirigida a la computadora del usuario.

L) Provocar o participar en un ataque de denegación de servicio a cualquier equipo de cómputo, de comunicaciones o elemento informático.

M) Usar cualquier programa, script o comando, o transmitir mensajes de cualquier tipo, con el propósito de interferir o deshabilitar una sesión de acceso remoto, a través de cualquier medio, localmente o vía Internet/Intranet/Extranet.

N) Proveer información clasificada como confidencial de la UACJ a terceras personas que no tengan autorización para recibirla.

O) Conectar cualquier dispositivo activo a la RedUACJ con la finalidad de extender la cobertura de la red alámbrica y/o inalámbrica de voz y/o datos.

P) En el caso de laboratorios físicos o virtuales de prácticas para la docencia e investigación que puedan afectar la infraestructura y/o servicios de voz y datos de la RedUACJ que proporciona la CGTI, el encargado deberá coordinarse con la CGTI con el fin de acordar los términos de operación del equipo o sistema.

4.4.2 **Actividades de mensajería electrónica y comunicaciones**

A) Transmitir mensajes de correo electrónico basura o cualquier otro material de publicidad.

B) Cualquier forma de acoso vía correo electrónico, correo de voz, fax, teléfono, radiolocalizador, o mensajería instantánea por el tipo de lenguaje, frecuencia o tamaño de mensajes.

C) Uso no autorizado o alteración del encabezado de cualquier mensaje de correo electrónico.

D) Solicitar correo electrónico para cualquier otra dirección de correo que no sea de uso del solicitante, con la intención de acosar o colectar mensajes.

E) Crear o reenviar cadenas de correo o cualquier otro esquema piramidal de cualquier tipo.

F) La generación de correo electrónico originado dentro de la RedUACJ a nombre de cualquier otra organización o persona.

4.5 Excepciones aplicables a los empleados adscritos a la CGTI y que estén facultados por sus legítimas responsabilidades de trabajo

4.5.1 Actividades de Sistemas y de Red

A) Ingresar a los sistemas de autenticación del usuario o la seguridad de cualquier equipo de cómputo, de comunicaciones o cuenta de acceso, con la autorización del usuario o si existe algún evento que pueda comprometer la seguridad y/u operación que justifique ingresar sin su autorización.
B) La introducción de programa maliciosos en un ambiente controlado de laboratorio separado de la REDUACJ para fines de evaluación, investigación y aprendizaje.
C) Monitoreo y análisis del tráfico de la RedUACJ
D) Pruebas de estrés
E) El escaneo de puertos o el escaneo de hoyos de seguridad.
F) Conectar todo dispositivo a la RedUACJ con la finalidad de extender la cobertura de la red alámbrica y/o inalámbrica de voz y/o datos.

4.5.2 Actividades de mensajería electrónica y comunicaciones

Transmitir mensajes de correo electrónico de publicidad autorizada por las instancias correspondientes en la UACJ.

4.5.3 **Sanciones.** Aquel usuario que se encuentre violando cualquiera de las presentes políticas, puede ser sujeto a acciones disciplinarias que serán determinadas por la autoridad competente.