

**Universidad del Valle de Guatemala**  
**Dirección de Tecnología de Información y Comunicación**

# **Políticas de IT**



**Marzo 2010**

## **CONTENIDO**

INTRODUCCIÓN .....	3
POLÍTICAS INSTITUCIONALES .....	4
Proceso: USO DE LOS RECURSOS DE LA TECNOLOGÍA DE LA INFORMACIÓN INSTITUCIONAL .....	5
POLÍTICAS DE LA UNIVERSIDAD DEL VALLE DE GUATEMALA.....	6
POLÍTICAS Y NORMAS DE ADMINISTRACIÓN DE USUARIOS DE LA RED ADMINISTRATIVA – ACADÉMICA.....	7
POLÍTICAS DE SEGURIDAD INFORMÁTICA.....	13

## ***INTRODUCCIÓN***

Se vuelve imprescindible preservar características tales como la confidencialidad, integridad y disponibilidad de los datos que la Universidad tiene en custodia, y minimizar los riesgos asociados con el uso de tecnologías de la información y comunicaciones.

Para ello es necesario establecer una política de Uso de los recursos de la Tecnología de la Información de la Universidad del Valle de Guatemala, es por ello que en este documento se han recopilado las políticas y procedimientos relacionados.

Las políticas de la Universidad del Valle de Guatemala estarán regidas por las políticas Institucionales del Grupo Educativo del Valle, las cuales son de observancia general.

Seguido de ellas se encuentran las políticas propias de la Universidad del Valle de Guatemala las cuales son responsabilidad de la Dirección de Tecnologías de Información y Comunicación implantar las mismas y los procedimientos relacionados.

## ***POLÍTICAS INSTITUCIONALES***

	<b>Proceso: USO DE LOS RECURSOS DE LA TECNOLOGÍA DE LA INFORMACIÓN INSTITUCIONAL</b>
<b>Objetivo de la Política:</b>	Normar el acceso, la disponibilidad y la integridad de los sistemas de información electrónica.

- 1) La institución es dueña de las aplicaciones, los sistemas, el equipo de computación y las redes que componen su infraestructura técnica y de todos los datos que residen en ella; y es responsable de tomar las medidas necesarias para proteger la integridad, seguridad y la confidencialidad de sus sistemas, aplicaciones, datos y cuentas de usuarios.
  
- 2) Cada unidad de tecnología de información de las entidades es responsable de implantar las políticas y procedimientos necesarios para el cumplimiento de la política antes mencionada.
  
- 3) La institución cumple con toda la legislación aplicable a derechos de autor y propiedad intelectual de las aplicaciones de terceros utilizadas por las entidades.

# ***POLÍTICAS DE LA UNIVERSIDAD DEL VALLE DE GUATEMALA***

# **POLÍTICAS Y NORMAS DE ADMINISTRACIÓN DE USUARIOS DE LA RED ADMINISTRATIVA – ACADÉMICA**

## **1. Introducción**

El Departamento de Redes y Atención a Usuarios de la Dirección de Tecnologías de la Información y Comunicación de la Universidad del Valle de Guatemala, en su calidad de administrador y auditor de recursos los recursos informáticos de la institución, considera que al implementar tecnologías de redes de comunicación, tanto de área local (LAN) como de área amplia (WAN), los diversos servicios que sobre estas se puedan prestar (Internet, correo electrónico, redes de comunicaciones Microsoft, redes de comunicaciones Linux, etc.), y los diferentes medios por el cual se puede establecer la comunicación (localmente o remotamente, por medio de MODEM, etc.) se hace necesario que los investigadores, catedráticos y personal administrativo, estén enterados y conscientes de los compromisos, normas y reglamentos que ha adquirido y debe atender al registrarse como usuario de las redes y/o servicios.

## **2. Servicios**

La red lógica de la institución se divide en dos grupos:

- a. Red de área local Administrativa-Financiera:** Sobre la cual se operan los sistemas administrativos.
- b. Red de área local Académica-Investigativa:** Sobre la cual se opera todo lo que pueda dar apoyo a la actividad docente y/o investigativa.
- c. En cada una de las redes se prestan los siguientes servicios:**
  - i.** Autenticación de Usuarios
  - ii.** Configuración de horarios de trabajo
  - iii.** Antivirus (de correo electrónico y de estación de trabajo)
  - iv.** Correo electrónico
  - v.** Navegación en Internet (Versión I para el área administrativa y versiones I y II para el área académica)
  - vi.** Acceso a recursos compartido de red (Impresoras, servidores de almacenamiento, etc.)
  - vii.** Asistencia remota (PC-Anywhere) o personalizada

## **3. Solicitud de Acceso a la Red**

El personal administrativo, de investigación y docente que desee tener acceso a cualquiera de estas redes, deberá completar el formulario de **“Solicitud de Acceso a la Red”**. Es importante que todos los datos de dicho formulario sean proporcionados, escribiendo no aplica ò NA. Este formulario debe ser presentado a la Dirección de Departamento de Redes y Asistencia a Usuarios (J-208) o a la Dirección de Tecnologías de la Información y Comunicación (J-204) para que se le de trámite. A continuación se da una explicación detallada de dicho formulario y de las normativas que rigen su autorización.

- a. **En la sección 1 del formulario, “Datos generales del solicitante”**, se requieren los datos completos del solicitante. Todos los datos requeridos deben ser proporcionados, de lo contrario no se le dará trámite a la solicitud.
- b. **En la sección 2 del formulario, “Horario de Acceso a la Red”**, deberá indicar el horario en el cual solicita el acceso de acuerdo al horario real de trabajo del solicitante.
  - i. La solicitud puede ser modificada o no procesada por cualquiera de los siguientes motivos:
    - Que la solicitud no tenga las autorizaciones necesarias o que esté incompleta
    - Que el horario solicitado no concuerde con el tipo de contratación o actividad laboral del solicitante.
    - Que se solicite acceso local (en el campus) los días domingo.
    - Que el horario solicitado exceda las 10 horas diarias para una persona de tiempo completo y de 6 horas diarias para personal de medio tiempo.
    - Que el horario solicitado no corresponda al horario laboral de la institución.
  - ii. Respecto a la autorización de los horarios se debe considerar lo siguiente:
    - El horario que se autoriza tiene una vigencia máxima de un año.
    - Para modificar temporal o permanentemente el horario de acceso a la red, se deberá presentar a la dirección del Departamento de Redes y Asistencia a Usuarios, el formulario correspondiente para dicho trámite.
    - La solicitud de modificación temporal o permanente de horario de acceso a la red, deberá contar con toda la información solicitada y las autorizaciones respectivas, y podrá ser modificada o rechazada por los mismos motivos expuestos en el inciso anterior.
- c. **La sección 3 del formulario, “Acceso a Sistemas”**. Solo aplica para el área administrativa. En esta sección se especifica el nombre del módulo (Presupuesto, Contabilidad, Bancos, Asignación, Secretaría);



la entidad relacionada (UVG, CAG, ALTIPLANO, PROESUR) y el nivel de acceso que se solicita (consulta; grabar; grabar y modificar; grabar, modificar y borrar; Supervisor). En algunos casos, también se debe especificar el número de cuenta bancaria.

- d. **La sección 4 del formulario, “Acceso a Servicios”**. En esta sección se solicita el acceso a los servicios como Internet, correo electrónico y recursos compartidos de red. El acceso a los servicios puede ser modificado o no autorizada por los siguientes motivos:
  - i. Que no esté claramente justificada la solicitud.
  - ii. Que el perfil del puesto de trabajo sea considerado como de alta seguridad u operativo. Por ejemplo, los usuarios de los sistemas financieros o puestos administrativos o académicos en los que dichos servicios no corresponden a su normal desempeño de labores.
- e. **La sección 5 del formulario, “Autorizaciones”**. En esta sección el solicitante deberá escribir su nombre nuevamente y firmar dicha solicitud aceptando la responsabilidad que eso implica. El nombre y la firma del Director del Departamento en el cual pertenece el empleado es indispensable, al igual que el sello. No se tramitará ninguna solicitud que no cuente con la autorización respectiva.
- f. **La sección 6 del formulario, “Controles del Departamento de Informática”**. Esta sección está reservada para los controles del departamento. Se lleva el registro de la fecha de la recepción y autorización de la solicitud, así como de los técnicos que la operaron.

#### 4. Política de uso y responsabilidades

##### a. Principio General

Los servicios de acceso a la red Administrativa-Financiera y Académica-Investigativa de la Universidad del Valle de Guatemala, con acceso a Internet y correo electrónico en algunos casos, se proveen para apoyar la administración de la institución y facilitar la investigación y educación abierta entre universidades, centros académicos y/o instituciones de investigación e instrucción. El uso para otros propósitos no es aceptable.

##### b. Usos específicamente aceptados

- i. **Red Administrativa-Financiera:** Tareas y operaciones estrictamente relacionadas con los sistemas financieros (presupuestos, contabilidad, bancos, tesorería, activos fijos, cuanta corriente, caja, etc.), administrativos (compras, bodegas, RRHH, etc.) y académicos (inscripciones, asignación de estudiantes, etc.). El uso de correo electrónico o cualquier otra comunicación o actividad para dar soporte a la gestión de la administrativa o que represente beneficio para la institución.
- ii. **Red Académica-Investigativa:** Todo lo relacionado al ejercicio puro de la docencia así como la comunicación con estudiantes, investigadores y educadores nacionales o extranjeros en conexión con la investigación e instrucción, siempre que red utilizada por los usuarios extranjeros provea acceso recíproco a los investigadores y educadores guatemaltecos. La comunicación e intercambio para el desarrollo profesional, con el fin de mantenerse actualizado, o para debatir temas de alguna especialidad. El uso para sociedades de las diferentes disciplinas, asociaciones universitarias, consultorías gubernamentales, o actividades normales relacionadas con las propias del investigador o educador. El uso para la solicitud o administración de donaciones o contratos para la investigación o instrucción, pero no para otro tipo de recaudación de fondos o actividades de relaciones públicas. El uso de correo electrónico o cualquier otra comunicación u actividad para dar soporte directo a la investigación o educación. Anuncios de productos o servicios nuevos para el uso en investigación o educación, pero no para publicidad de tipo comercial alguno.

##### c. Usos inaceptables de la red Administrativa-Financiera y Académica-Investigativa

- i. El uso de cualquier servicio o recurso (Internet, correo electrónico, equipos, suministros) para actividades remuneradas, a menos que estén cubiertas por el Principio General o los rubros de la sección sobre usos aceptables.
- ii. El uso extenso sin justificación adecuada, privado o para negocios particulares.
- iii. Cualquier actividad que pueda amenazar a la seguridad informática de la institución (ver documento de Políticas y Normas de Seguridad Informática), comprometer el prestigio de la misma o dar mal uso a los recursos informáticos.

#### **d. Responsabilidades**

- i. **Departamento de Redes y Asistencia a Usuarios:** Es responsabilidad del departamento de Redes y Asistencia a Usuarios, administrar y velar por el funcionamiento óptimo de los sistemas y servicios informáticos que se prestan en la institución. Cumplir con todas las normas y procedimientos que se estipulan en el documento de Políticas y Normas de Seguridad Informática de la Institución, siendo responsable directo de todos los recursos compartidos de la red en el nivel físico (servidores, suites, etc.) y lógico (backup's de bases de datos, programas y código fuente de los sistemas y archivos de usuarios almacenados en los servidores centrales).
- ii. **Usuarios de la red Administrativa-Financiera y Académica-Investigativa:** Al firmar la solicitud de acceso a la red, el usuario se hace total y único responsable de su usuario de red. También se compromete a cumplir con todas las normas y procedimientos que se estipulan en el documento de Políticas y Normas de Seguridad Informática de la Institución, siendo responsable directo de todos los recursos informáticos asignados a él, tanto en el nivel físico (computadora, impresora, UPS, etc.) y lógico (programas instalados y back-up's de los archivos de información que se encuentran almacenados en el disco duro de su computadora)
- iii. **Directores de Departamentos y/o Recursos Humanos:** Es responsabilidad de cada Director o jefe de Departamento notificar a esta unidad cuando alguno de sus subordinados haya dejado de laborar para la institución; ya sea directamente o por medio de un formulario para tal efecto, el cual puede ser

solicitado en la Oficina de Recursos Humanos; esto es con el objetivo de dar de baja de los sistemas informáticos al usuario de dicho empleado.

## **5. Amonestaciones**

Además de la ética con que esta red debe ser manejada, se considera que todo usuario (profesional, catedrático, estudiante o de cualquier índole) que no cumpla con las normas establecidas en este documento, será amonestado con una nota originada por la Rectoría. Si la falta lo amerita, serán aplicados los lineamientos que sean dados por el Consejo Directivo de la Universidad.

## **6. Consultas y mayor información**

Para mayor información, puede dirigirse a la Dirección del Departamento de Redes o Asistencia a Usuarios (J-208 Ext.: 552) o a la Dirección de Tecnologías de la Información y Comunicación (J-204 Ext.: 571). También puede comunicarse por correo electrónico a: [soporte@uvg.edu.gt](mailto:soporte@uvg.edu.gt)

# **POLÍTICAS DE SEGURIDAD INFORMÁTICA**

Aprobadas por el Consejo Directivo el 3 de diciembre de 2003 según Acta 30-200

## **1. Introducción**

Los sistemas computarizados de información y las redes de computadoras son una parte integral de las operaciones de la Universidad del Valle de Guatemala. La Universidad ha efectuado una inversión sustancial en recursos humanos y financieros para crear estos sistemas.

Estas políticas y directrices se han establecido para:

- Proteger esta inversión
- Salvaguardar la información contenida en estos sistemas
- Reducir los riesgos de operación, y legales
- Proteger el buen nombre de la Universidad

## **2. Violaciones**

Las violaciones de estas políticas pueden resultar en acciones disciplinarias de acuerdo con las políticas de la Universidad. El no observar estos lineamientos pueden resultar en acciones disciplinarias por parte de la Universidades dependiendo de: el tipo y la severidad de la violación, si causa responsabilidades o pérdidas para la Universidad, y/o la existencia de violaciones repetidas.

## **3. Administración**

La Dirección de Tecnologías de la Información y la Comunicación (DiTIC) es la unidad responsable de la administración de estas políticas.

### **Contenido**

Los temas tratados en este documento incluyen:

- Enunciado de Responsabilidad
- La InterNet y el Correo Electrónico
- Virus de Computadoras
- Códigos de Acceso y Contraseñas
- Seguridad Física
- Propiedad Intelectual y Acuerdos de Licenciamiento

### **Enunciado de Responsabilidad**

En esta sección se discuten responsabilidades generales pertinentes a estas políticas. Las secciones posteriores enumeran responsabilidades adicionales.

### **Responsabilidad de Administradores**

Los administradores y supervisores deben:

- Asegurar que todo el personal apropiado conozca y cumpla con estas políticas
- Crear estándares de rendimiento, prácticas de control, y procedimientos adecuados para proveer un aseguramiento razonable que todos los empleados observen estas políticas

### **Responsabilidad de la DiTIC**

La DiTIC debe:

1. Desarrollar y mantener estándares y procedimientos escritos para asegurar la implementación de, y el apego a, estas directrices de políticas
2. Ofrecer el soporte adecuado para asistir a los empleados para cumplir con sus responsabilidades bajo estas directrices

### **La InterNet y sus servicios**

La InterNet es una red muy grande, de acceso público, que tiene millones de usuarios y organizaciones conectados en todo el mundo. Algunos de sus servicios más populares son el correo electrónico y el chat.

### **Política**

El acceso a la InterNet se provee a los empleados para el beneficio de la Universidad del Valle de Guatemala. Los empleados pueden conectarse a una variedad de recursos de información por todo el mundo.

Conversamente, la InterNet también esta repleta de riesgos y material no apropiado. Para asegurar que todos los empleados sean usuarios responsables y productivos de la InterNet, y para proteger los intereses de la Universidad, se han establecido los siguientes lineamientos para el uso de la InterNet y sus servicios.

### **Uso aceptable**

Los empleados que utilizan la InterNet están representando a la Universidad. Los empleados son responsables de asegurar que la InterNet se utilice en una forma efectiva, ética y legal. Son ejemplos de uso aceptable, los siguientes:

- El uso de navegadores Web para obtener información pertinente a las operaciones de la Universidad
- Acceso a las bases de datos para obtener información necesitada
- Usar los servicios para contactos relacionados con las operaciones de la Universidad

### **Uso no aceptable**

Los empleados no deben utilizar a la InterNet para propósitos que son ilegales, no éticos, dañinos a la Universidad, o no productivos. Son ejemplos de usos no aceptables, los siguientes:

- Envío o re-transmisión de correos electrónicos de cadenas, pirámides, etc. Es decir mensajes que contengan instrucciones para re-enviar el mensaje a otros
- Envíos masivos de correo electrónico, es decir el envío del mismo mensaje a más de 10 beneficiarios o más de una lista de distribución
- Llevar a cabo negocios particulares utilizando recursos de la Universidad
- La transmisión de cualquier contenido que sea ofensivo, acosador, o fraudulento.

### **Descargas (Downloads)**

Las descargas de archivos, (bajar archivos) de la InterNet, no es permitido a menos que se cuente con permiso, por escrito, del Director de la DiTIC.

### **Responsabilidad de los empleados**

Un empleado que utilice la InterNet o sus servicios debe:

- Asegurar que todas las comunicaciones efectuadas sean por razones profesionales y que no interfieren con su productividad
- Ser responsable por el contenido de todo texto, audio o imágenes que coloque o envíe por la InterNet. Todas las comunicaciones deben contener el nombre del empleado
- Asegurarse de no transmitir información con derechos de propiedad intelectual sin el permiso correspondiente
- Conocer y seguir todas las políticas aplicables de la Universidad del Valle de Guatemala concernientes a la seguridad y confidencialidad de los registros de la Universidad
- Hacer una revisión de virus sobre cualquier archivo ejecutable, o que contenga macros, que se haya recibido por la InterNet

- Evitar la transmisión de información que no sea pública, sea de la Universidad o de sus miembros. Si es necesario transmitir este tipo de información, se requiere que los empleados tomen las medidas necesarias para asegurar que la información sea entregada a la persona adecuada que esté autorizada para recibir dicha información para un uso legítimo

## **Derechos de propiedad intelectual**

Los empleados que utilicen la InterNet no tienen permiso de copiar, transferir, renombrar, agregar, o borrar información o programas que pertenecen a otros, a menos que el dueño de los mismos le hayan conferido expresamente el permiso para hacerlo. La falta de observación de los acuerdos de derechos de propiedad intelectual o licencias pueden resultar en acciones disciplinarias por parte de la Universidad y/o acciones legales por parte del dueño de los derechos.

## **Monitoreo**

Todos los mensajes creados, enviados, o recibidos por medio de la InterNet son propiedad de la Universidad y *pueden ser considerados como información pública*. La Universidad del Valle de Guatemala se reserva el derecho de acceder el contenido de cualquier mensaje transmitido por medio de sus facilidades si esta cree, a su juicio, que tiene una necesidad operativa de hacerlo.

Todas las comunicaciones, incluyendo texto e imágenes, pueden ser entregadas a las autoridades legales o a grupos terceros sin el consentimiento previo de el remitente o el receptor. **Esto quiere decir que no debe colocar en sus mensajes cualquier cosa que no quiera ver en la página principal de un periódico o que deba explicar en una corte legal.**

## **Virus de computadoras**

Los virus de computadoras son programas diseñados para hacer cambios no autorizados a programas y datos. Por lo tanto, los virus pueden causar la destrucción de los recursos de la Universidad.

## **Generales**

Es importante saber que:

- Los virus de computadoras son mucho más fáciles de prevenir que curar
- Las defensas contra los virus de computadoras incluyen la protección contra el acceso no autorizado a los sistemas de computación, la utilización exclusiva de fuentes confiables de datos y programas, y la utilización de software especial anti-virus.



## **Responsabilidad de la DiTIC**

La DiTIC:

- Instalará y mantendrá un software anti-virus adecuado en todas las computadoras
- Responderá a todos los ataques de virus, destruirá cualquier virus detectado, y documentará cada incidente

## **Responsabilidad de los empleados**

Estas directrices son aplicables a todos los empleados:

- Los empleados no introducirán, con conocimiento, un virus computacional en las máquinas de la Universidad
- Los empleados no utilizarán diskettes, cintas, cartuchos zip, u otros medios de almacenamiento, de origen desconocido
- Los medios de almacenamiento que ingresen a la Universidad deben ser revisados antes de leerlos
- Cualquier empleado que sospeche que su estación de trabajo ha sido infectada por un virus debe APAGAR INMEDIATAMENTE la estación y llamar a la DiTIC

## **Códigos de acceso y contraseñas (passwords)**

La confidencialidad y la integridad de los datos almacenados en los sistemas computacionales de la Universidad deben ser protegidos por controles de acceso para asegurar que solamente los empleados autorizados tengan acceso. Este acceso estará restringido a exclusivamente las capacidades que sean adecuadas para las funciones de trabajo de cada empleado.

## **Responsabilidad de la DiTIC**

La DiTIC será responsable de la administración de los controles de acceso a todas las computadoras de la Universidad. La DiTIC procesará la adiciones, eliminaciones y cambios cuando se reciba una solicitud, por escrito del supervisor del empleado.

Las eliminaciones podrán ser procesadas con una solicitud oral, previa a la solicitud por escrito. La DiTIC mantendrá una lista de los códigos de acceso y contraseñas administrativas y guardará esta lista en un lugar seguro.

## **Responsabilidad de los empleados**

Cada empleado:

- Será responsable de todas las transacciones que se efectúen con su ID de usuario (login) y contraseña
- Resguardará su contraseña y no la dará a otros. Las contraseñas deben cambiarse inmediatamente si se sospecha que puedan ser del conocimiento de otros. Las contraseñas no deben registrarse (guardarse) en lugares de donde fácilmente puedan ser obtenidas.
- Cambiará sus contraseñas, por lo menos, cada 30 días.
- Deberá utilizar contraseñas que no sean fácilmente adivinadas por otros,
- Debe cerrar sus sesión de trabajo cuando debe abandonar su estación de trabajo durante un período prolongado.

### **Responsabilidad de los supervisores**

Los administradores y supervisores deben notificar, de inmediato, a la DiTIC cada vez que un empleado se retire de la Universidad o es transferido a otro departamento para que su acceso sea revocado. La terminaciones involuntarias deben ser reportadas en el momento de la terminación.

### **Responsabilidad del Departamento de Recursos Humanos**

El Departamento de Recursos Humanos debe notificar mensualmente, a la DiTIC, sobre transferencias y retiros de los empleados. Las terminaciones involuntarias deben reportarse en el momento de la terminación.

### **Seguridad Física**

Es política de la Universidad proteger hardware de computación, software, datos, y documentación, del mal uso, robo, acceso no autorizado, y amenazas ambientales.

### **Responsabilidad de los empleados**

Las siguientes directrices son aplicables a todos los empleados:

- Los medios de almacenamiento: diskettes, cintas magnéticas, CD-ROM's, cartuchos ZIP, etc., deben ser almacenados fuera de vista cuando no estén en uso. Si contienen información altamente sensitiva o confidencial, deben ser guardados bajo llave.
- Los medios de almacenamiento deben ser resguardados de las amenazas ambientales como el calor, luz solar directa, y campos magnéticos.
- Los equipos críticos de computación, e.g., servidores de archivos, deben ser protegidos con una fuente ininterrumpible de energía (UPS). Otros equipos deben estar protegidos, al menos, con un supresor de transientes.
- Deben evitarse las amenazas ambientales al hardware como, comida, humo, líquidos, humedad alta o baja, y temperaturas extremas (calor o

- frío).
- Como la DiTIC es responsable de todas las instalaciones de equipo, desconexiones, modificaciones, y relocalizaciones, los empleados no deben efectuar estas operaciones. Esto no aplica a movimientos temporales de computadoras portátiles para las cuales se haya hecho una conexión inicial por la DiTIC.
  - Los empleados no retirarán equipo portátil, como "notebooks" y "laptops", del campus sin el consentimiento informado de su supervisor. El consentimiento informado significa que el supervisor sabe qué equipo se retira, qué datos hay en él, y para qué propósito será utilizado.
  - Los empleados deben ejercer cuidado para salvaguardar el equipo electrónico que se les ha asignado. Aquellos que sean negligentes en esta responsabilidad pueden ser responsabilizados por cualquier pérdida o daño que resulte.

### **Acuerdos de propiedad intelectual y licenciamientos**

Es la política de la Universidad del Valle de Guatemala, ajustarse a todas las leyes concernientes a la propiedad intelectual.

### **Referencia legal**

La Universidad del Valle de Guatemala y sus empleados están sujetos al cumplimiento de la Ley de Protección de Derechos de Autor y Derechos Conexos de la República de Guatemala (Decreto 33-98). El incumplimiento de la misma puede exponer a la Universidad del Valle de Guatemala y el(los) empleado(s) responsable(s) a penalizaciones civiles y/o criminales.

### **Alcance**

Esta directriz se aplica a todo el software que sea propiedad de la Universidad, licenciado a la Universidad, o desarrollado utilizando recursos de la Universidad por empleados y vendedores.

### **Responsabilidad de la DiTIC**

La DiTIC:

- Mantendrá registros del software propiedad de la Universidad
- Auditará, aleatoriamente, las computadoras de la Universidad para verificar que únicamente tengan instalado software autorizado.

### **Responsabilidad de los empleados**

Los empleados no:

- Instalarán software a menos que hayan sido autorizados por la DiTIC. En las computadoras de la Universidad se instalará, exclusivamente, software que es propiedad de, o haya sido licenciado a, la Universidad.
- Copiarán software a menos que tengan una autorización de la DiTIC
- Descargarán (bajarán) software a menos que tengan una autorización de la DiTIC.

### **Penalizaciones Civiles**

Las violaciones a las leyes de propiedad intelectual exponen a la Universidad y a el(los) empleado(s) responsable(s) a las siguientes penalizaciones:

- Responsabilidad por daños sufridos por el dueño de los derechos
- Ganancias atribuibles a las copias
- Multas de hasta US\$ 100,000 por cada copia ilegal

### **Penalizaciones criminales**

Las violaciones a las leyes de propiedad intelectual que son cometidas, con conocimiento, y para el propósito de ventaja comercial o ganancia financiera privada, exponen a la Universidad y el(los) empleado(s) responsable(s) a las siguientes penalizaciones criminales:

- Multas de hasta Q. 100,000 por cada título infringido
- Prisión de hasta 4 años

(Esta página esta intencionalmente en blanco)

**UNIVERSIDAD DEL VALLE DE GUATEMALA**  
**Dirección de Tecnologías de la Información y la Comunicación**

**Recepción de Políticas de Seguridad de la Información**

Este formulario se utiliza para dar acuse de recepción de, y confirmación de aceptación de los lineamientos plasmados en, las Políticas de Seguridad de la Información de la Universidad del Valle de Guatemala.

**Procedimiento**

Complete los siguientes pasos:

- Lea las Políticas de Seguridad de la Información
- Firme y ponga la fecha en los espacios provistos abajo
- Devuelva únicamente esta página a la DiTIC

**Firma**

Al firmar, acuerdo lo siguiente:

- i. He recibido y leído una copia de - Políticas de Seguridad de la Información- y las comprendo en su totalidad.
- ii. Cualquier equipo de cómputo, software y medios de almacenaje que me provea la Universidad contiene información propietaria y confidencial acerca de la Universidad del Valle de Guatemala, y sus miembros, y que esta es, y seguirá siendo, propiedad de la Universidad en todo momento;
- iii. No copiaré, duplicaré (exceptuando para propósitos de copias de respaldo de mi trabajo en la Universidad del Valle de Guatemala), diseminaré, o permitiré que alguien más copie o duplique cualquiera de esta información o software;
- iv. A mi retiro de la Universidad del Valle de Guatemala, por cualquier motivo, devolveré inmediatamente a la Universidad el original y copias de cualquier software, materiales de computación, o equipo de computación que pude haber recibido de la Universidad que esté, ya sea, en mi posesión o de otra forma directa o indirectamente bajo mi control.

Firma del empleado:

Nombre del empleado:

Fecha:

Departamento o Unidad: