



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

## RESOLUCIÓN No 125-CSUP-2019

### EL CONSEJO SUPERIOR UNIVERSITARIO POLITÉCNICO DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

#### CONSIDERANDO:

**Que**, el artículo 227 de la Constitución de la República del Ecuador establece: *“La Administración Pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, transparencia y evaluación”*.

**Que**, el artículo 233 de la Constitución de la República del Ecuador determina: *“Ninguna servidora, ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos”*.

**Que**, el numeral 1) del Art. 7 de la Ley Orgánica de la Contraloría General del Estado, publicado en el Registro Oficial Suplemento Nro. 595 del 12 de junio del 2002, señala: *“....., la Contraloría General del Estado, expedirá, aprobará y actualizará, normas de control interno que sirvan de marco básico para que las instituciones del Estado y sus servidores establezcan y pongan en funcionamiento su propio control interno”*.

**Que**, el numeral 410-04 de las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de recursos públicos, expedida mediante



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

Acuerdo de la Contraloría General del Estado Nro. 39, publicado en el Registro Oficial Suplemento No, 87 del 14 de diciembre del 2009, dispone:

*"..... la máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria y la Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de la información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran".*

**Que**, el Art. 1 del acuerdo ministerial No 166 de 19 de septiembre de 2013, publicado en el Segundo Suplemento del Registro Oficial No. 88 de 25 de septiembre de 2013 señala: *"Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información".*

**Que**, la información en la UPEC, es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes para los ejes transversales de la Institución, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad de sus funciones esenciales, la administración de riesgos y la consolidación de una cultura de seguridad.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Que**, el literal a) del Art. 16 del Estatuto vigente de la Universidad Politécnica Estatal del Carchi en lo relacionado a las funciones y atribuciones del Consejo Superior Universitario Politécnico, lo faculta para: *“a. Aprobar el Estatuto universitario y sus reformas, debiendo someterlas a trámite de aprobación final ante el Consejo de Educación Superior”*;

En uso de sus facultades constitucionales, legales y estatutarias resuelve expedir las:

## **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI**

### **CAPÍTULO I**

#### **DEL ÁMBITO, OBJETO Y DEFINICIÓN DE TÉRMINOS**

**Art. 1.- Ámbito.-** Esta norma establece las políticas de seguridad de la información de la Universidad Politécnica Estatal del Carchi-UPEC como un pilar fundamental para implantar sistemas y procedimientos alineados a la Gestión de la Seguridad de la Información.

**Art. 2.- Del Objeto.-** El objeto de las políticas de seguridad de la información es definir los lineamientos que regulen la protección de los sistemas de información a nivel estratégico y que garantizan la confidencialidad, integridad y disponibilidad de la información que se genera, utiliza, comparte y almacena en medios electrónicos para la prestación de los servicios institucionales de la UPEC.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 3.- Alcance.-** Las políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de la seguridad de la información entre la comunidad universitaria y proveedores de servicios informáticos de la UPEC.

La UPEC realizará el seguimiento de la implementación de las políticas para verificar su cumplimiento y el compromiso de los funcionarios de la Institución con la seguridad de la información.

**Art. 4.- Obligatoriedad y cumplimiento.-** Las políticas de seguridad de la información son de total obligatoriedad y cumplimiento para todos los miembros internos o externos de la Institución que requieran el uso de los servicios informáticos institucionales o el acceso autorizado a la información.

Los usuarios de los servicios quedan obligados a observar el Reglamento de Seguridad de la Información, cuya infracción dará lugar a la aplicación de sanciones de acuerdo con el ordenamiento jurídico vigente.

## CAPÍTULO II

### DISPOSICIONES GENERALES

**Art. 5.- Importancia.-** Las políticas de seguridad de la información buscan el establecimiento de la gestión de la seguridad de la información en la UPEC, especialmente para: la protección de activos, definición de objetivos de seguridad de la información; y, la definición de un marco normativo que determina la postura de los miembros de la comunidad universitaria respecto a la protección de sus activos tecnológicos.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 6.- Definición de términos.-** Para efectos de la aplicación de las políticas de seguridad de la información se entenderá por:

- a) **AMBIENTE DE PRODUCCIÓN.-** Es el entorno real donde trabajan los usuarios finales con los sistemas informáticos implementados en la Institución.
- b) **ACTIVOS DE INFORMACIÓN.-** Recursos de información necesarios para que la Institución funcione y consiga los objetivos que persigue la alta dirección.
- c) **ADMINISTRADOR.-** Técnico responsable por mantener y administrar un servicio tecnológico.
- d) **APLICACIONES DE SOFTWARE.-** Son los programas diseñados para o por los usuarios para facilitar la realización de tareas específicas en los equipos informáticos.
- e) **CONFIDENCIALIDAD.-** Propiedad de prevenir la revelación y divulgación intencionada o no intencionada de información a personas o sistemas no autorizados.
- f) **CONTROL DE CAMBIOS.-** Es el procedimiento que permite al administrador de sistemas informáticos implementar cambios o actualizaciones de los mismos en el ambiente de producción.
- g) **DISPONIBILIDAD.-** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella como usuarios autorizados, ya sean personas, procesos o aplicaciones.
- h) **GESTIÓN DE LA CONTINUIDAD.-** Proceso permanente de mejora que garantiza la continuidad de las operaciones que dependen de los servicios informáticos de la Institución.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- i) **INFORMACIÓN SENSIBLE.**- información personal y privada de una persona.
- j) **INTEGRIDAD.**- Propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- k) **PLAN DE CONTINUIDAD.**- Es un plan de acción que involucra medidas preventivas, detectivas y correctivas que permite a una organización garantizar la continuidad en sus servicios informáticos.
- l) **POLÍTICA.**- Principios generales que la Institución se compromete a cumplir, en base a reglas y directrices del comportamiento esperado por los funcionarios.
- m) **RECURSOS TECNOLÓGICOS.**- Medio tecnológico tangible o intangible empleado para cumplir un propósito.
- n) **SEGURIDAD DE LA INFORMACIÓN.**- Conjunto de medidas preventivas y correctivas que permiten custodiar y proteger la información de los sistemas tecnológicos bajo los principios fundamentales de integridad, confidencialidad y disponibilidad.
- o) **SERVICIO.**- Requerimientos de usuario para uso de recursos tecnológicos, equipos o sistemas informáticos.
- p) **SISTEMA DE INFORMACIÓN.**- Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información, según determinados procedimientos, tanto automatizados como manuales.
- q) **TECNOLOGÍA DE LA INFORMACIÓN.**- Conjunto de hardware y software operados por la Institución que procesan información.





# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- r) **USUARIO.-** Persona que utiliza los servicios y sistemas informáticos en la Institución.

## CAPÍTULO III

### RESPONSABLES DE LA SEGURIDAD DE LA INFORMACIÓN

**Art. 7.- De los responsables de la Seguridad de la Información.-** La organización de la seguridad de la información de la UPEC será compromiso de la máxima autoridad de la Institución, y que conjuntamente con el Oficial de Seguridad Informática y la Dirección de Tecnologías de la Información y Comunicación realizarán el seguimiento de la implementación de la presente política y del control.

**Art. 8.- De las funciones de la máxima autoridad de la Institución.** Será función de la máxima autoridad de la Institución con respecto a la seguridad de la información, la designación del Oficial de Seguridad Informática, quien no pertenecerá a la Dirección de Tecnologías de la Información y Comunicación de la Institución.

**Art. 9.- De las funciones del Oficial de Seguridad Informática.-** Son funciones del Oficial de Seguridad Informática las siguientes:

- a) Establecer los requisitos mínimos de seguridad para la adquisición, desarrollo o actualización de sistemas de información que no vulneren los principios de confidencialidad, integridad y disponibilidad de la información;



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- b)** Definir políticas, normativas y procedimientos para el adecuado tratamiento de incidentes que afecten la seguridad de la información;
- c)** Gestionar la aprobación de políticas y normativas institucionales relacionadas a la seguridad de la información;
- d)** Difundir la normativa y procedimientos en materia de seguridad de la información dentro de la institución;
- e)** Verificar el cumplimiento de las normas, procedimientos y controles de seguridad en relación a los sistemas informáticos institucionales;
- f)** Actualizar periódicamente las políticas de seguridad de la información con un plazo mínimo de una vez al año o cuando ocurrieran cambios significativos que pudieran comprometer su aplicabilidad y eficacia en la Institución;
- g)** Definir controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a las redes de la institución;
- h)** Coordinar el proceso de gestión de la continuidad de los servicios informáticos institucionales frente a incidentes inesperados que amenazan la seguridad de la información de la Universidad;
- i)** Solicitar recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información en base a planificación y gestión de la capacidad tecnológica; y,
- j)** Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas.





# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 10.- De las funciones del responsable de la Dirección de TIC.-**  
Son funciones del responsable de las Dirección de TIC con respecto a la seguridad de la información:

- a) Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas;
- b) Analizar continuamente la gestión de la capacidad de los sistemas y equipos informáticos en operación y proyectar las futuras demandas de capacidad para soportar los requerimientos de los usuarios frente a la disponibilidad de los servicios informáticos;
- c) Implementar los controles de seguridad definidos para evitar software malicioso, accesos no autorizados;
- d) Gestionar los incidentes de seguridad de la información de acuerdo a procedimientos establecidos;
- e) Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas.

## CAPÍTULO IV

### SEGURIDAD DE LOS ACTIVOS INFORMÁTICOS

**Art. 11.- De la seguridad de los activos informáticos.-** La seguridad de los activos informáticos tiene como finalidad realizar la constatación de existencia de inventarios y el buen uso de los activos tecnológicos de hardware y software de la UPEC para salvaguardar la información y garantizar su confidencialidad, integridad y disponibilidad.

En consecuencia, la Dirección de TIC deberá considerar lo siguiente:

- a) Verificar el inventario de los equipos informáticos de la UPEC.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- b) Verificar el etiquetado en los equipos informáticos en la institución.
- c) Administrar y custodiar los equipos activos (Switches, Firewall, WLC, Access Points) y pasivos de la red de datos (Racks, Patch Pannel, entre otros);
- d) Administrar el inventario de aplicaciones de software, sistemas operativos y utilitarios;

El usuario deberá considerar lo siguiente:

- a) Evitar retirar las etiquetas de los activos informáticos de la institución;
- b) Reportar cualquier incidente o fallo de los equipos de la red de la universidad a la Dirección de TIC;
- c) Evitar acceder y manipular los equipos de red; y,
- d) Informar a la Dirección de TIC sobre la adquisición, cambio o actualización de aplicaciones de software de carácter académico, administrativo o de cualquier otra índole que sean utilizadas dentro de las instalaciones de la Universidad.

## CAPÍTULO V

### SEGURIDAD DE LA INFORMACIÓN

**Art. 12.- De la seguridad de la información.-** La información debe ser clasificada bajo criterios de control de acceso para garantizar su confidencialidad e integridad. En consecuencia, el encargado de administrar la información que reposa en medios digitales deberá considerar lo siguiente:



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- a) Clasificar los activos de información en base a principios de seguridad: confidencialidad, integridad y disponibilidad.
- b) Definir niveles de clasificación de la información como: información secreta, información confidencial, información privada e información pública.

El usuario deberá considerar lo siguiente:

- a) Respetar los acuerdos de confidencialidad de la información de la universidad.

## CAPÍTULO VI

### SEGURIDAD EN LOS SERVICIOS DE INTERNET

#### Y CORREO ELECTRÓNICO

**Art. 13.- Del uso adecuado del correo electrónico institucional.-** El correo electrónico es una herramienta cuyo uso está autorizado para los usuarios en las actividades de información, control, supervisión y seguimiento de los procesos institucionales que efectúa la UPEC, así como su uso en labores administrativas, académicas y de docencia. En consecuencia, la Dirección de TIC deberá:

- a) Definir una estrategia para la gestión de cuentas de usuario de correo electrónico;
- b) Controlar el envío no autorizado de correos masivos; y,
- c) Proveer de una cuenta de correo electrónico para cada usuario y limitar su uso para el cumplimiento de las funciones institucionales para la que fue requerida.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

El usuario deberá considerar lo siguiente:

- a) Utilizar el correo electrónico exclusivamente para el cumplimiento de tareas académicas y administrativas propias de las funciones que realiza en la universidad.
- b) Destruir los mensajes con origen desconocido, y asume su responsabilidad por las consecuencias que pueda ocasionar la apertura y ejecución de los archivos adjuntos;
- c) Evitar enviar por este medio, información confidencial, privada, reservada o sujeta a sigilo, a menos que existan evidentes garantías y autorización para ello;
- d) Utilizar el correo electrónico institucional como medio de comunicación, por lo que es obligatorio para todos los usuarios revisar su cuenta de correo institucional para recibir disposiciones o pedidos que deba atender o responder;
- e) Mantener de manera confidencial las credenciales de acceso al correo electrónico;
- f) Evitar correos masivos, correo no deseado ("spam"), cadenas, realizar suscripciones en páginas web con contenido malicioso y cualquier otra acción que no esté relacionado con el normal ejercicio de sus funciones a las cuentas asignadas dentro o fuera de la Institución.

**Art. 14.- Del uso de Internet y sus aplicaciones.-** El servicio de internet y sus aplicaciones son herramientas autorizadas en las actividades de control y supervisión que efectúa la UPEC, así como en las labores administrativas, académicas y de docencia se debe garantizar su uso adecuado.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

En consecuencia, el administrador del servicio de internet deberá considerar lo siguiente:

- a) Determinar el tipo de contenido al que acceden los usuarios de la red de datos; y,
- b) Establecer las reglas de acceso y bloqueo de contenido inapropiado en los dispositivos de seguridad de red.

El usuario deberá considerar lo siguiente:

- a) Usar apropiadamente los servicios y aplicaciones que brinda la Internet, evitando el acceso a sitios restringidos dentro de la Institución;
- b) Solicitar el acceso a un sitio determinado o que se haya restringido a la Dirección de TIC; y,
- c) Evitar realizar instalaciones de equipos para acceso a Internet sin previa autorización de la Dirección de TIC.

## CAPÍTULO VII

### CONFIDENCIALIDAD DE LA INFORMACIÓN

#### PARA EL TALENTO HUMANO

**Art. 15.- De la confidencialidad de la información.-** La UPEC consciente de la importancia que tiene el talento humano para el cumplimiento de sus objetivos institucionales, realizará un proceso formal de selección, acorde con la legislación vigente y considerando aspectos relacionados a la seguridad y confidencialidad de la información.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 16.- Del acceso a los sistemas informáticos para nuevo personal.-** La Dirección de TIC otorgará el acceso a los sistemas informáticos al nuevo personal de la institución en base a las funciones asignadas y asegurará el retiro de cuentas de usuario al personal que termine su relación laboral, verificando que exista la devolución de activos tecnológicos de la UPEC.

## CAPÍTULO VIII

### DE LA SEGURIDAD EN LAS OPERACIONES

**Art. 17.- De la seguridad en las operaciones.-** La seguridad y continuidad de las operaciones realizadas en la UPEC y de los servicios informáticos se efectuarán mediante el monitoreo de servicios, gestión de la capacidad, protección contra código malicioso, respaldos de información y la seguridad de la documentación de sistemas.

**Art. 18.- Del monitoreo y revisión de servicios.-** Se llevará un control de los niveles de desempeño de los servicios contratados a terceros para verificar el cumplimiento de los acuerdos.

El administrador de los servicios contratados deberá considerar lo siguiente:

- a) Monitorear los niveles de desempeño de los servicios contratados a terceros; y,
- b) Presentar el informe con los niveles de desempeño de los servicios contratados a terceros.

**Art. 19.- De la gestión de la capacidad.-** Se debe asegurar el desempeño de los servicios y aplicaciones de software en la UPEC mediante la





# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

realización de proyecciones de los requerimientos futuros con la finalidad de brindar continuidad en las operaciones y servicios institucionales. En consecuencia, la Dirección de Tecnologías de TIC deberá considerar lo siguiente:

- a) Administrar y monitorear la capacidad de los recursos tecnológicos disponibles en la universidad;
- b) Generar un plan de capacidad tecnológica con proyecciones de requerimientos futuros.

**Art. 20.- De la protección contra código malicioso.-** Se realizarán controles contra código malicioso en los sistemas operativos con la finalidad de mantener su estado normal de funcionamiento frente a potenciales amenazas, resultado de vulnerabilidades imprevistas en la infraestructura tecnológica de la UPEC. En consecuencia, el administrador de los equipos informáticos y sistemas operativos deberá considerar lo siguiente:

- a) Prohibir la instalación y el uso de software que no disponga de licencia de uso autorizada;
- b) Mantener actualizado el software de antivirus en los equipos informáticos para evitar la propagación de virus y malware a través de dispositivos de almacenamiento y correo electrónico; y,
- c) Mantener los sistemas operativos actualizados con las últimas versiones de seguridad disponibles.

El usuario deberá considerar lo siguiente:

- a) Prescindir de instalar software no autorizado;
- b) Solicitar la autorización para la instalación de software específico;



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- c) Informar las alarmas por infecciones de virus que se presenten en los equipos informáticos;
- d) Revisar los medios de almacenamiento para descartar la presencia de virus o cualquier otro programa malicioso y evitar su difusión;
- e) Verificar regularmente que su computador disponga de software antivirus actualizado; y,
- f) Evitar abrir o reenviar mensajes de correo electrónico que no provengan de fuentes conocidas y confiables.

**Art. 21.- De los respaldos de Información.-** Se realizarán respaldos de información para salvaguardar la información generada en los sistemas informáticos de la UPEC de manera segura. En consecuencia, el responsable de realizar respaldos de información deberá:

- a) Establecer la prioridad de la información crítica a ser respaldada;
- b) Establecer los procedimientos de respaldos de información; y,
- c) Establecer procedimientos regulares de verificación y restauración de los medios de respaldo para garantizar su confiabilidad en caso de requerirlo.

El usuario deberá considerar lo siguiente:

- a) Mantener toda la información institucional ordenada en los equipos informáticos de los puestos de trabajo para ser almacenada en un servidor de archivos de la UPEC;
- b) Crear periódicamente respaldos de la información que utiliza para realizar sus funciones en el servidor de archivos de la UPEC; y,
- c) Evitar nombres demasiado largos a los archivos creados ya que esto ocasiona inconvenientes con las tareas de respaldo.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 22.- De la seguridad de la documentación de los sistemas.-** Se debe custodiar la documentación de los sistemas informáticos y aplicaciones de software con la finalidad de salvaguardar la información y evitar vulnerabilidades de seguridad.

## CAPÍTULO IX

### SEGURIDAD EN EL CONTROL DE ACCESO

#### A LOS SISTEMAS INFORMÁTICOS

**Art. 23.- De la seguridad en el control de acceso a sistemas informáticos.-** Se establecerán los procedimientos para el control de acceso a los equipos, redes y sistemas informáticos, seguridad en sesiones de usuario, seguridad en puestos de trabajo, registros de auditoría y la utilización de antivirus y firewall con la finalidad de evitar accesos no autorizados.

**Art. 24.- Del control de acceso a equipos y sistemas informáticos para los usuarios administradores.-** La Dirección de TIC designará a los responsables de los servicios informáticos de la UPEC, a quienes se asignarán cuentas para la administración de los sistemas y equipos informáticos, con la finalidad de salvaguardar la integridad y confidencialidad de la información.

La Dirección de TIC deberá considerar lo siguiente:

- a) Gestionar cuentas de usuario de administrador de acceso a los equipos y sistemas informáticos; y,



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- b) Definir una estrategia para la gestión de cuentas de usuario que permitan el acceso a los sistemas informáticos.

**Art. 25.- Del control de acceso a equipos y aplicaciones de software para los usuarios.-** El acceso a equipos y aplicaciones de software para los usuarios será autorizado para realizar tareas de carácter: administrativo, académico, investigativo o cualquier actividad que se relacionen con los objetivos y planes institucionales de la UPEC.

En consecuencia, la Dirección de TIC, deberán considerar lo siguiente:

- a) Prevenir accesos no autorizados por miembros internos y/o externos a la Institución; y,
- b) Asignar responsables de las diferentes unidades de la Dirección de TIC para la creación de cuentas de usuario de acceso a los sistemas.

**Art. 26.- De la autenticación de usuario en los sistemas informáticos.-** Se definirá el acceso a los sistemas informáticos mediante la autenticación, que será validada a través de un usuario y contraseña para cada usuario de la Institución.

**Art. 27.- Del uso de cuentas de usuario en los sistemas informáticos.-** Se establecerán procedimientos de identificación y autenticación de usuarios en las aplicaciones de software de la UPEC. En consecuencia, el administrador de los sistemas deberá considerar lo siguiente:

- a) Evitar realizar actividades regulares desde cuentas de usuario de administrador;
- b) Evitar el uso de usuarios genéricos; y,



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- c) Establecer el procedimiento de autenticación y bloqueo de cuentas cuando se generan accesos no autorizados.

El usuario deberá considerar lo siguiente:

- d) Utilizar las cuentas de usuario asignadas para realizar sus labores en la institución; y,
- e) Evitar la transferencia o compartición de cuentas de usuario personales.

## **Art. 28.- De la asignación, cambio y recuperación de contraseñas.-**

Se establecerá el procedimiento para la asignación, cambio y recuperación de la contraseña de los usuarios que tienen acceso a los sistemas informáticos de la UPEC para garantizar el acceso a los mismos.

En consecuencia, la Dirección de TIC deberá:

- a) Definir el tipo de usuario, permisos y nivel de acceso a los servicios informáticos;
- b) Establecer el formato y la longitud de caracteres para la contraseña;
- c) Limitar la cantidad de intentos permitidos de inicio de sesión; y,
- d) Definir un procedimiento para la recuperación de contraseña.

El usuario deberá considerar lo siguiente:

- a) No divulgar el usuario y contraseña asignada; y,
- b) Dar un buen uso al usuario y contraseña asignada.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 29.- Seguridad en las sesiones activas de usuario de equipos y sistemas informáticos.-** Las sesiones de usuarios activas en los equipos y sistemas informáticos deben cerrarse al abandonar el lugar de trabajo para evitar el acceso no autorizado, vulnerando el principio de confidencialidad.

En consecuencia, el administrador de los sistemas y equipos informáticos deberá:

- a) Definir el tiempo de inactividad de las sesiones en las aplicaciones de software;
- b) Establecer un mecanismo de cierre de sesión automática luego de cumplir el tiempo de inactividad de la sesión de usuario; y,
- c) Verificar la configuración del protector de pantalla de los equipos informáticos.

El usuario deberá considerar lo siguiente:

- a) Evitar dejar sesiones abiertas en las aplicaciones de software de la universidad y de los equipos informáticos cuando no se encuentren en el lugar de trabajo;
- b) Guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial;
- c) Archivar la información sensible que pueda encontrarse en impresoras, copiadoras o en el puesto de trabajo; y,
- d) Evitar colocar claves de acceso a los sistemas informáticos en espacios visibles para otros usuarios o terceros.





# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 30.- De la habilitación de puertos de red.-** La habilitación de los puertos de red de la Institución será administrada y controlada por la Dirección de TIC para la prestación de los servicios informáticos. En consecuencia. El administrador de red deberá:

- a) Habilitar exclusivamente los puertos de red autorizados; y,
- b) Llevar un registro de los puertos habilitados que utilizan los servicios informáticos.

**Art. 31.- De la segmentación de la red.-** Se realizará la distribución de la red institucional mediante la segmentación permitiendo una adecuada administración y control de la red de datos de la UPEC. En consecuencia, el administrador de red deberá:

- a) Identificar los segmentos de red de acuerdo a las necesidades de los usuarios;
- b) Establecer el segmento de red crítico donde se encuentren los equipos principales de la red de datos;
- c) Asignar las direcciones de red a cada uno de los segmentos;
- d) Documentar la información de los segmentos de red de datos; y,
- e) Informar el funcionamiento e incidentes en cualquiera de los segmentos de red establecidos.

**Art. 32.- Del enrutamiento de la red.-** Para garantizar la seguridad de la red se configurará las puertas de enlace para validar la conexión de los equipos informáticos de los usuarios a la red Institucional de la UPEC y se dividirá las redes en dominios lógicos de red, dominios de red interna, dominios de red externa e inalámbrica.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

En consecuencia, el administrador de red deberá:

- a) Determinar el enrutamiento que cada segmento de red requiere, de acuerdo a las necesidades de los usuarios;
- b) Configurar el enrutamiento necesario en los equipos de borde de la red; y,
- c) Registrar el enrutamiento para cada uno de los segmentos de red.

**Art. 33.- De la protección de antivirus y reglas del firewall.-** Para proteger los equipos y salvaguardar la información generada en los sistemas informáticos de la UPEC, se debe implementar el uso de firewall y antivirus como una barrera de seguridad frente a potenciales amenazas. En consecuencia, la Dirección de TIC deberá:

- a) Instalar antivirus en los equipos informáticos;
- b) Implementar Firewall como medida de protección en la red; y,
- c) Definir las reglas para la detección de intrusos en los equipos de seguridad de la red.

**Art. 34.- De los registros de auditorías al sistema integrado informático.-** Se establecerán registros de auditorías en el sistema integrado informático de la UPEC para llevar un control interno de las operaciones críticas que realizan los usuarios al acceder al sistema.

## CAPÍTULO X



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

## SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS INFORMÁTICOS

**Art. 35.- De la seguridad en la adquisición, desarrollo y mantenimiento de los sistemas informáticos.-** La seguridad en los sistemas informáticos adquiridos, desarrollados o en etapa de mantenimiento debe ser analizada con la finalidad de evitar fallos de seguridad y garantizar la continuidad de los servicios informáticos de la Institución. En consecuencia, La Dirección de TIC establecerá los lineamientos para garantizar la incorporación de medidas de seguridad en las aplicaciones de software desarrolladas o adquiridas de terceros.

**Art. 36.- Del análisis y especificaciones de los requerimientos de seguridad.-** Se establecerán los requisitos mínimos de seguridad de la información que deben cumplir las nuevas aplicaciones de software o las existentes y que sean sometidos a mejoras o cambios; dichos requisitos deben ser considerados en la fase de análisis del software y verificados en la fase de pruebas.

**Art. 37.- Del control de cambios en los sistemas informáticos.-** Se definirán procesos de control de cambios en la implementación de aplicaciones de software en ambiente de producción para evitar la presencia de errores y fallas de los sistemas informáticos de la UPEC. En consecuencia, la Dirección de TIC deberá:

- a) Crear diferentes ambientes de programación para el desarrollo de aplicaciones de software seguro;
- b) Asignar responsables para la implementación de cambios a las aplicaciones de software;



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

- c) Revisar el informe de paso a producción, el cual contendrá información de todos los cambios a realizar en las aplicaciones de software; y,
- d) Entregar acceso físico o lógico al ambiente de producción únicamente para propósitos de soporte, cuando sea autorizado a usuarios internos o externos en la Institución.

**Art. 38.- De los procedimientos para el control de cambios.-** Se establecerán los procedimientos para realizar el control de cambios de las aplicaciones de software de la UPEC. En consecuencia, el administrador del control de cambios deberá:

- a) Definir el proceso de paso a producción para las aplicaciones de software;
- b) Elaborar el informe de paso de pruebas a producción;
- c) Comunicar las ventanas de mantenimiento con una duración definida para la ejecución de los cambios en las aplicaciones de software;
- d) Coordinar la implementación de actualizaciones a las aplicaciones de software en el ambiente de producción;
- e) Instalar las modificaciones, controlando previamente la recepción de las pruebas validadas y autorizadas; y,
- f) Validar la actualización de la documentación en los manuales de usuario de los cambios implementados en las aplicaciones de software.



# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

**Art. 39- De la seguridad en el código fuente de las aplicaciones de software.-** Se establecerán procedimientos para el acceso al código fuente de las aplicaciones de software de la UPEC.

En consecuencia, la Dirección de TIC deberá:

- a) Asignar un responsable del código fuente de las aplicaciones de software; y,
- b) Realizar el mantenimiento del código fuente de las aplicaciones de software en base a procedimientos de control de cambios.

## CAPÍTULO XI

### CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS

**Art. 40.- De la gestión de la continuidad en los servicios informáticos institucionales.-** Se garantizará la continuidad de las operaciones en los servicios informáticos de la UPEC frente a posibles incidencias y amenazas que pongan en riesgo la disponibilidad de los servicios informáticos. En consecuencia, la Dirección de TIC coordinará y supervisará la implantación del Plan de continuidad de los servicios informáticos de la UPEC.

## CAPÍTULO XII

### DEL CUMPLIMIENTO Y SANCIONES

En caso de existir incumplimiento de la presente política de Seguridad de la Información por parte de un miembro de la comunidad universitaria, se comunicará a la Dirección Administrativa para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas




# UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 · Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

institucionales y demás responsabilidades civiles y penales a que hubiera lugar.

**DISPOSICION FINAL.-** Las políticas de Seguridad de la Información entrarán en vigencia a partir de su aprobación por el Consejo Superior Universitario Politécnico.

Dada, en la Sala de Sesiones del Consejo Superior Universitario Politécnico de la Universidad Politécnica Estatal del Carchi, en Tulcán a los 30 días del mes de agosto del 2019.



Dr. Hugo Rúa Enriquez.

**PRESIDENTE DEL CONSEJO SUPERIOR  
UNIVERSITARIO POLITÉCNICO**

**CERTIFICO.-** Que la presente Resolución fue aprobada en sesión ordinaria del viernes treinta de agosto del dos mil diecinueve.



Dr. Juan Carlos Villacreses E.

**SECRETARIO**

**CONSEJO SUPERIOR UNIVERSITARIO POLITÉCNICO**