POLITICAS Y PROCEDIMIENTOS DEL AREA DE TECNOLOGÍA.

UNIVERSIDAD TECNOLÓGICA
INDOAMÉRICA

RESPONSABLE:

Dr. Franklin Tapia Defaz

RECTOR

Ambato, 07 de diciembre de 2018

Contenido

UNIVERSIDAD TECNOLOGICA INDOAMERICA

RECTORADO

CONSIDERANDO:

Que, el Art 14 del Reglamento para Carreras y Programas Académicos en Modalidades en Línea, a Distancia y Semipresencial o de Convergencia de Medios, señala que: *"Los parámetros específicos referentes a los requerimientos de infraestructura tecnológica, se determinarán en el Instructivo que el CES, expida para el efecto".*

Que, el Art. 70 del Reglamento para Carreras y Programas Académicos en Modalidades en Línea, a Distancia y Semipresencial o de Convergencia de Medios indica que: *"Las IES deberán garantizar que para la ejecución de carreras y programas en línea y a distancia cuentan, o tienen acceso garantizado, a una infraestructura de hardware y conectividad, ininterrumpida durante todo el período académico. En el caso de que la infraestructura tecnológica no sea propia de la IES, se deberá evidenciar mediante convenios de uso o contratos específicos la provisión de este servicio. El CES deberá monitorear las características y funcionamiento de esta infraestructura tecnológica antes y durante el desarrollo de las carreras y programas".*

Que, el Art. 71 del Reglamento para Carreras y Programas Académicos en Modalidades en Línea, a Distancia y Semipresencial o de Convergencia de Medios manifiesta que**: "***Todas las IES que oferten carreras y programas en línea y a distancia deberán tener una plataforma tecnológica, mediante la cual el estudiante pueda acceder a las aulas virtuales de las asignaturas, cursos o equivalentes y a otras actividades de interacción entre pares, con sus profesores autores, profesores tutores, técnicos docentes y personal administrativo. Estas plataformas deberán apoyar a la organización del aprendizaje, debiendo facilitar espacios para el desarrollo de las actividades de docencia, de prácticas de aplicación y experimentación y de aprendizaje autónomo, como se establece en el Reglamento de Régimen Académico".*

En uso de sus atribuciones,

RESUELVE:

Expedir las siguientes:

POLITICAS Y PROCEDIMIENTOS DEL AREA DE TECNOLOGÍA

PRIMERA. - Ámbito de aplicación y fines.

Las políticas de seguridad en cómputo tienen por objeto establecer las medidas de índole técnico y de organización, necesarias para garantizar la seguridad de las tecnologías de información: equipos de cómputo, sistemas de información, redes de telemática, voz y datos y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a los usuarios de la Universidad Tecnológica Indoamérica

SEGUNDA. - Políticas de Seguridad, Acceso Físico

a) Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo a los medios de comunicación;
b) El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado, portando una identificación que les será asignado por el área de seguridad del campus;
c) Las visitas internas o externas al área de comunicaciones, podrán acceder siempre y cuando se encuentren acompañadas por un responsable del área o con permiso de la Dirección o Coordinación de Tecnología;
d) Las visitas a las instalaciones físicas de los centros de cómputo, laboratorios o salas de videoconferencia se realizarán en el horario establecido y cumpliendo lo estipulado en este documento;
e) El personal autorizado para movilizar, cambiar o extraer equipos de cómputo de la institución es el técnico responsable del mismo o el superior responsable

a través de identificaciones y formatos de Entrada/Salida, el cual notificará al área de activos y al personal de seguridad;

f) A partir de los procedimientos definidos por la institución, el Departamento Financiero definirá procedimientos para inventario físico, firmas de resguardo para préstamos y usos dedicados de equipos de tecnología de información;

g) El resguardo de los equipos de comunicaciones deberá quedar asignado a la persona que los usa o administra, permitiendo conocer siempre la ubicación física de los equipos;

h) El centro de datos, así como las áreas que cuenten con equipos de misión crítica deberán contar con vigilancia y/o algún tipo de sistema que ayude a recabar evidencia de accesos físicos a las instalaciones;

i) Las puertas de acceso a las salas de cómputo deben ser preferentemente de vidrio transparente, para favorecer el control del uso de los recursos de cómputo;

j) Las instalaciones en las que se encuentra la infraestructura tecnológica de la institución deben:

- Recibir mantenimiento preventivo al menos una vez por semana, que permita mantenerse libre de polvo; estar libre de contactos e instalaciones eléctricas en mal estado; contar por lo menos con dos extinguidores de incendio adecuado y cercano al centro de telecomunicaciones;
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas del área de tecnología deberán recibir mantenimiento anual con el fin de mantener la efectividad del sistema; y,

l) Cada vez que se requiera conectar equipo de cómputo, se deberá comprobar la carga de las tomas de corriente.

TERCERA. - De los Respaldos

a) Las Base de Datos de la Universidad serán respaldadas periódicamente diariamente en forma automática y/o manual;

b) Los respaldos deberán ser almacenados en un lugar seguro y distante del sitio de trabajo;
c) Respaldar la información de los usuarios, bajo su criterio, de los discos duros dependiendo de la importancia y frecuencia del cambio de la misma;
d) Los administradores no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena; y,
e) Para reforzar la seguridad de la información de la cuenta, el usuario conforme su criterio deberá hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma. Los respaldos serán responsabilidad absoluta de los usuarios.

CUARTA. - Políticas De Seguridad Lógica De La Red.

a) La Red de la Universidad tiene como propósito principal servir en la transformación e intercambio de información dentro de la entidad con estudiantes, docentes, técnicos, administrativos y con entidades nacionales e internacionales, con el fin de generar conexiones con otras redes;
b) La responsabilidad por el tráfico de la información que circula en la red de datos de la institución recae directamente sobre el usuario que los genere o solicite;
c) Se prohíbe ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo;
d) No se permite interferir o interrumpir las actividades de los demás usuarios por cualquier medio o evento salvo que las circunstancias así lo requieran, como casos de contingencia, los cuales deberán ser reportados en su momento a sus superiores correspondientes;
e) Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la Universidad y se usarán exclusivamente para actividades relacionadas con la institución;

f) Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario;

g) El uso de analizadores de red es permitido única y exclusivamente por el personal de Informática, para monitorear la funcionalidad de la Red, contribuyendo a la consolidación del sistema de seguridad bajo las políticas y normatividades de la institución;

h) Cuando se detecte fraude de datos, se cancelará la cuenta o se desconectará temporalmente al usuario.;

i) El Director de Tecnología debe llevar un control total y sistematizado de los recursos tecnológicos;

j) Los encargados del área de tecnología son los responsables de la planificación y organización del personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo; y,

k) El Departamento de Recursos Humanos deberá reportar al departamento de Tecnología cuando un usuario deje de laborar o de tener una relación con la institución.

QUINTA. - Políticas de acceso a la base de datos

a) De las claves de acceso a la base de datos como administrador:

1.- La base de datos del Sistema de Gestión Académica y Financiera (SGA), deberá ser manejada por dos personas designadas por el Canciller de la Universidad, pudiendo ser internas o externas a la institución y serán las únicas responsables del control total de la base de datos;

2.- Los programadores deben trabajar sobre la base de datos con un perfil especialmente diseñado para garantizar la estructura y confiabilidad de la información, para lo que se recomienda:

- Acceso solo de lectura para las tablas críticas de manejo de la información como son las tablas de notas, asistencias, pagos y deudas de los estudiantes; y,

- Tablas lógicas de logs (registro de sucesos dentro de la base de datos y sistema operativo) este perfil deberá ser creado por el administrador de la base de datos designado por el Canciller.

3.- Los programadores deben trabajar sobre un ambiente de pruebas que no esté directamente en producción en el cual tendrán acceso total a la base de datos para realizar su trabajo.

4.- De ser necesario la restructuración de la base de datos solamente lo podrán las personas autorizadas y designadas para tales fines por parte del Canciller.

SEXTA. - Políticas de uso de los usuarios

a) Deberán ser afines al trabajo desarrollado;
b) Los recursos tecnológicos asignados al usuario son intransferibles y no deberán ser utilizados para fines personales;
c) Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios;
d) El correo electrónico no se deberá usar para envío masivo, ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social;
e) Queda estrictamente prohibido copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor;
f) Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de la institución, de acuerdo con las políticas que en este documento se mencionan; y,
g) Los usuarios deberán solicitar apoyo ante cualquier duda en el manejo de los recursos de cómputo de la institución.

SEPTIMA- De los servidores de la Red de la UTI.

a) Departamento de Tecnología tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red;

b) La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad del Departamento de Tecnología;

c) Durante la configuración del servidor el Departamento de Tecnología debe normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios;

d) Los servidores que proporcionen servicios a través de la RED e Internet deberán:

   1. Funcionar las 24 horas del día y los 365 días del año;
   2. Recibir mantenimiento preventivo mínimo dos veces al año que incluya depuración de bitácoras; y,
   3. Deberán ser monitoreados por el departamento de Tecnología y por el Centro de Operaciones de la Red de la institución con el fin de evitar interrupciones en el servicio;

e) Los servicios institucionales de Internet sólo podrán proveerse a través de los servidores autorizados por el Departamento de Tecnología;

f) Los servidores deberán ubicarse en un área física que cumpla las normas para un centro de telecomunicaciones como:

   1. Acceso restringido;
   2. Temperatura adecuada para los equipos;
   3. Protección contra descargas eléctricas; y,
   4. Mobiliario adecuado que garantice la seguridad de los equipos;

h) El Centro de Operaciones de la Red se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra;

i) Para efecto de asignarle su cuenta de correo a los docentes y administrativos de la institución, éste deberá llenar una solicitud en formato libre y entregarlo al departamento de Recursos Humanos, con su firma y la del Director del área, con el siguiente formato: nombreprimerapellido@uti.edu.ec

j) Una vez matriculado el estudiante el Departamento de Tecnologías proveerá una cuenta de correo con el siguiente formato; y,

k) nombreprimerapellido@indoamerica.edu.ec. En caso de existir nombres repetidos se tomará el segundo apellido.

OCTAVA. - De los Sistemas Institucionales de Información

a) El Administrador de Base de datos tendrá acceso a la información para:
   1. La obtención de los respaldos de la Base de Datos;
   2. Diagnóstico o monitoreo;
   3. Solucionar problemas que el usuario no pueda resolver;

b) El Administrador de la Base de Datos no deberá eliminar ni manipular la información del sistema, al menos que esté dañada o ponga en peligro el buen funcionamiento del sistema; y,

c) El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el acceso a la información.

NOVENA. - Políticas De Seguridad Lógica para Administración de los Recursos de Cómputo.

a) El Departamento de Tecnología es el encargado de suministrar medidas de seguridad adecuadas contra hackers o daños a la información almacenada en los sistemas, así como la instalación de las herramientas, dispositivos o software; y,

b) El Departamento de Tecnología debe mantener informados a los usuarios y poner a disposición software que elimine de ataques a los sistemas de cómputo.

DÉCIMA. - Administración de Tecnologías de Información

a) El Administrador de Tecnología, podrá suspender las cuentas de los usuarios, en los siguientes casos:
   1. Si la cuenta no es utilizada con fines institucionales;
   2. Si pone en peligro el funcionamiento de los sistemas; y,

3. Si se verifica que un usuario ajeno está usando una cuenta de la institución;

b) Para la solución de problemas técnicos, deberá ingresar de forma remota única y exclusivamente y bajo solicitud explícita del propietario del equipo de cómputo;

c) Una vez que se adquiera o instale un software se actualizará la información de los equipos de cómputo;

d) Registrar los equipos de cómputo en el inventario y la red de la institución; y,

e) Reportar los incidentes de violación de seguridad de los sistemas de cómputo, argumentando fundamentada mente con los respaldos que permita eliminar riesgos.

DÉCIMA PRIMERA. - Políticas de Renovación de Equipos

Se definen los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

El ciclo de vida útil de los equipos varía según su función y el deterioro que estos sufran, se define como el tiempo durante el cual son útiles a la institución evitando pérdidas de tiempo laboral y académico. Según la naturaleza de los equipos, su ciclo de vida puede estar determinado por el tiempo de vigencia de la garantía, el tiempo que el fabricante le brinde soporte y repuestos, la capacidad del equipo para utilizar determinadas herramientas informáticas, para prestar ciertos servicios o la carga de trabajo del mismo, y por condiciones ajenas a la institución.

Para la renovación de los equipos de cómputo y telecomunicaciones se considera la siguiente clasificación:

a) Equipos en condición Verde: Son los equipos que permiten desarrollar el trabajo académico y administrativo con el fin de conseguir los objetivos institucionales. Su ciclo de vida útil es menor o igual a 3 años;

b) Equipos en condición Amarilla: Son los equipos que permiten desarrollar el trabajo académico y administrativo con el fin de conseguir los objetivos

institucionales. Su ciclo de vida útil es mayor a 3 años y menor a 5 años, estos equipos deberán ser repotenciados de acuerdo al avance tecnológico vigente; y,

c) Equipos en condición Roja: Debido al cumplimiento de su ciclo de vida útil que es mayor a 5 años los equipos que se encuentren en estas condiciones deben ser renovados por la institución.

El Departamento de Tecnologías llevará el control adecuado de cada equipo de los diferentes campos que identifique los tiempos de vida útiles señalados anteriormente con el fin de dar cumplimiento estricto a la política de renovación de equipos.

DÉCIMA SEGUNDA. - Uso de los Servicios de red por los usuarios

a) El usuario deberá definir su contraseña y será responsable de la confidencialidad de la misma;
b) El usuario deberá notificar al Departamento de Tecnología en los siguientes casos: si observa un comportamiento anormal en el servicio: mensajes extraños, lentitud y situación inusual en el servidor; y,
c) Si un usuario viola las políticas de uso de los servidores, el Departamento de Tecnología podrá cancelar la cuenta de acceso a los servidores.

DÉCIMA TERCERA. - Políticas De Seguridad Lógica Para El Uso Del Antivirus Institucional

a) Todos los equipos de cómputo de la institución deberán tener instaladas un programa Antivirus que permita mantener la información con un nivel de seguridad elevado;
b) Todos los días se efectuará el monitoreo en los equipos de cómputo y en la red para ejecutar la actualización de las firmas antivirus proporcionadas:
c) El Departamento de Tecnología será el responsable de:
   - Implementar la Solución Antivirus en los equipos de cómputo en las diferentes áreas de la institución;

d) Solucionar contingencias presentadas en la detección del analizador de red, ante el surgimiento de virus;
e) El administrador de la Red aislará el equipo o red, cuando la contingencia del virus no sea controlada, con el fin de evitar la propagación en otros equipos y redes;
f) El usuario no deberá desinstalar el programa antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus;
g) Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por el programa antivirus en el equipo de cómputo del usuario o por el equipo designado para tal efecto;
h) El usuario deberá comunicarse con El Departamento de Tecnología en caso de problemas de virus para buscar la solución;
i) El usuario será notificado por El Departamento de Tecnología en los siguientes casos:
    1. Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia;
    2. Cuando sus archivos resulten con daños irreparables por causa de virus; y,
    3. Cuando viole las políticas antivirus.

DÉCIMA CUARTA. - Sanciones

Cuando las acciones que vayan en contra de las políticas de seguridad en los equipos de cómputo y la red de la institución, deben ser sancionadas con la suspensión de los servicios, por un período de 90 días, determinados por los Departamentos de Tecnología y Talento Humano en una primera ocasión previa notificación al usuario y de manera indefinida en caso de reincidencia.

DISPOSICION DEROGATORIA

Única. - En virtud de las presentes Políticas y Procedimientos del Área de Tecnología de la Universidad Tecnológica Indoamérica, quedan derogadas las anteriores que se expidieron el 21 de junio de 2016.

DISPOSICIONES FINALES

Primera. - Las presentes Políticas y Procedimientos del Área de Tecnología de la Universidad Tecnológica Indoamérica, entrarán en vigencia a partir de la fecha de su expedición.

Segunda. - En todo lo no contemplado en el presente documento, se aplicarán las disposiciones estatutarias y reglamentarias de la Universidad.

Comuníquese y cúmplase.

Ambato, 07 de diciembre de 2018.

UNIVERSIDAD TECNOLOGICA INDOAMERICA RECTOR

Dr. Franklin Tapia Defaz
RECTOR
UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

Ambato, 07 de diciembre de 2018.

Certifico:

UNIVERSIDAD TECNOLOGICA INDOAMERICA SECRETARIA PROCURADURIA

Dr. Marisol Álvarez de Guerrero
SECRETARIA GENERAL PROCURADORA
UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA