POLÍTICAS DE USO RESPONSABLE DE LOS SISTEMAS DE INFORMACIÓN Y COMPUTADORES DEL COLEGIO TILATÁ ESTUDIANTES

1. PROPÓSITO

Este documento tiene como propósito definir las políticas de uso de las herramientas TIC (tecnología de la información y comunicaciones) en el colegio, así como brindar una guía respecto al uso responsable de las mismas.

2. GENERALIDADES

El colegio Tilatá procura brindar las herramientas TIC necesarias para promover el uso de Internet y de la red interna para que los estudiantes, docentes, y empleados en general, realicen trabajos específicos a su función, para que desarrollen habilidades y divulguen su conocimiento en el uso de las mencionadas herramientas.
Los recursos como computadores asignados a cada persona, área y/o sala, los portales (Cibercolegios y Sophia), las redes de cableado estructurados e inalámbricos, entre otros, son herramientas de trabajo y como tal deben ser utilizadas.

Todos los usuarios deben actuar honesta y responsablemente. Cada usuario es responsable por la integridad y seguridad de estos recursos.

Todos los usuarios son responsables del buen uso de la información y de tomar medidas preventivas para protegerla de amenazas como virus, spywares o cualquier tipo de daño o filtración de la misma.

El colegio puede restringir o prohibir el uso de sus recursos informáticos en cualquier caso en el que se demuestre alguna violación de estas políticas o de alguna ley.

3. DEFINICIONES

Para los propósitos de esta política se aplicarán las siguientes definiciones:
a. Comunicaciones electrónicas:
Incluyen todo uso de los sistemas de información para comunicar o publicar material y contenido por medio de servicios como correo electrónico, comunicados, foros de discusión, páginas html, o alguna herramienta similar.
b. Sistemas de información:
Incluye cualquier sistema físico o aplicación de software que sea administrado por la Institución y por los cuales ella sea responsable, como computadores, redes, servidores, enrutadores y aparatos similares junto con sus aplicaciones de red o aplicaciones de escritorio como sistemas operativos, aplicaciones de Internet, portales, etc.
c. Redes:
Incluye varios sistemas electrónicos como redes de datos, voz y dispositivos de almacenamiento.
d. Material no permitido:
Incluye la transmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales.

4. ACCESO

El acceso no autorizado a los sistemas de información de la Institución está prohibido. Todo usuario tiene un nombre de usuario y contraseña para acceder a los diferentes

sistemas de información del colegio, dichos datos son personales e intransferibles, ningún usuario debe utilizar la identificación de otro usuario, o dar a conocer la propia.
Cuando un usuario termina su relación con el Colegio Tilatá, sus datos de acceso para los sistemas de información serán eliminados inmediatamente.
Recomendaciones de acceso:

- No dé a conocer su contraseña a otros usuarios.
- Al terminar una sesión de trabajo siempre desconéctese de la red.
- Cambie sus passwords con regularidad, y no anote los mismos en lugares donde puedan ser fácilmente obtenidos.

5. USO PERMITIDO

a. Los sistemas de información del Colegio Tilatá son una herramienta para el buen desarrollo de actividades académicas.
b. Comunicación e intercambio con la comunidad académica, universitaria u otras instituciones con el fin de tener acceso a los últimos avances relacionados con la especialidad o tareas desempeñadas.
c. Anuncios o servicios nuevos para el uso de los usuarios en general, pero no para publicidad de tipo comercial o personal alguno.
d. Actividades de capacitación por medios virtuales o en línea.

6. USO NO PERMITIDO DE COMPUTADORES Y REDES.

El uso indebido de sistemas de información está prohibido. Este uso indebido incluye:

a. Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
b. Acceder sin la debida autorización, mediante computadores, software, información o redes de la Institución, a recursos externos o que pertenezcan al Colegio Tilatá.
c. Uso personal de cualquier sistema de información de la Institución para consulta y/o, visita a páginas sociales, de chat, juegos, emisoras en línea, o cualquier página pueda representar peligro para la seguridad de la red del colegio.
d. Uso personal de cualquier sistema de información de la Institución para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material obsceno.
e. Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
f. Utilizar los sistemas de información para propósitos ilegales o no autorizados.
g. Enviar cualquier comunicación electrónica fraudulenta.
h. Violar cualquier licencia de software o derechos de autor, incluyendo la instalación, copia o distribución de software protegido legalmente sin la autorización escrita del propietario del software. Esto incluye copia de programas, Cd´s musicales, libros, etc.
i. Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.
j. Usar las comunicaciones electrónicas para acosar o amenazar a los usuarios de la Institución o externos, de alguna manera que sin razón interfiera con el desempeño de los empleados.
k. Usar las comunicaciones electrónicas para revelar información privada sin el permiso explícito del dueño.
l. Leer la información o archivos de otros usuarios sin su permiso.
m. Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los registros de la Institución o cualquiera externo (incluyendo registros computarizados, permisos, documentos de identificación, u otros documentos o propiedades.)
n. Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
o. Lanzar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva.

p. Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Institución.
q. Transportar o almacenar material con derechos de propiedad o material nocivo usando las redes de la institución.
r. Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.
s. Comer o beber mientras cerca del equipo de cómputo, cualquier partícula ó líquido puede dañarlo seriamente.
t. Dejar encendidos los equipos por más de un día de trabajo, esto disminuye la vida útil del mismo.

7. PRIVACIDAD

a. La privacidad de los usuarios no está garantizada. Cuando un usuario trabaja en los computadores del colegio siguiendo las políticas de acceso establecidas, puede confiar en la privacidad de sus datos, sin embargo, los usuarios deben estar conscientes de que ningún sistema de información es completamente seguro, que personas dentro y fuera de la institución pueden encontrar formas de tener acceso a la información. De acuerdo con esto, el colegio no puede, y no garantiza la privacidad de los usuarios.

b. Respuesta al uso indebido de computadores y sistemas de información. En caso de encontrar algún tipo de uso indebido de los sistemas de información del Colegio, la Administración de la Institución puede acceder cualquier cuenta, datos, archivos, o servicio de información perteneciente a los involucrados en el incidente, para investigar y aplicar las sanciones correspondientes. Todos los miembros del departamento de Sistemas están en la obligación de monitorear constantemente los sistemas de información de la Institución a través de los medios correspondientes para responder oportunamente a cualquier acción que atente contra la integridad, disponibilidad, seguridad, o desempeño correcto de los mismos mediante la negación, restricción de acceso a usuarios o sistemas, aislamiento o desconexión de equipos o servicios. Los incidentes deben ser informados a la Rectoría o quien haga sus veces con la mayor cantidad de evidencia posible, para tomar las medidas correspondientes.

c. Acceso a la información de los empleados en lo referente a las operaciones de la Institución.

Los empleados de la Institución llevan a cabo las tareas administrativas y académicas con los sistemas de información de la misma. Cada empleado controla el acceso a información particular almacenada en los sistemas de información. Sin embargo, si un empleado no estuviere disponible, se encontrare incapacitado o se negare a proveer información necesaria para llevar a cabo cualquier operación académica o administrativa de la Institución, previa autorización por parte de la Rectoría o quien haga sus veces, el departamento de sistemas puede tener acceso a estos archivos, datos, o partes individuales de los sistemas de información.

8. CORREO ELECTRÓNICO

a. Aplicabilidad. Todas las políticas incluidas en este documento son aplicables al correo electrónico.

b. Uso. El colegio provee de un correo institucional a cada uno de sus empleados, debe usarse para fines laborales, de manera profesional y cuidadosa porque éste está representando a la institución.

9. SEGURIDAD

Todos los usuarios de los sistemas de información del colegio Tilatá deben velar por el cuidado de la información, lo que incluye:

a. Contraseñas:

Las contraseñas que se entregan por primera vez a cada usuario son temporales y deben ser modificadas inmediatamente.
Cada usuario es responsable de mantener en privado sus datos de acceso a los sistemas de información del Colegio.
Las contraseñas de redes serán modificadas anualmente o cuando el cambio de algún miembro del personal del Departamento de Sistemas así lo amerite.
b. Sesiones: cuando un usuario inicia sesión en un sistema de información del colegio, está dando acceso a información que solamente él debe manejar, el dejar la sesión de uno de estos sistemas abierta en su ausencia, deja disponible abiertos a otros usuarios los datos con los que está trabajando.
c. Prevención: todos los usuarios del Colegio Tilatá son responsables de prevenir la filtración y/o daño de la información mediante el cuidado de los dispositivos de almacenamiento.
Todos los usuarios deben revisar con un antivirus sus medios extraíbles para prevenir contagio de virus, software espía, entre otros.
d. Redes y equipos: harán parte del dominio del Colegio Tilatá, solamente los equipos que pertenezcan a este.
Los usuarios deben utilizar las herramientas que el colegio les brinde, siguiendo las políticas de uso que aplica para cada una de ellas.
Los usuarios que requieran del servicio de Internet en sus computadores portátiles personales, deben inscribirse para obtener dicho servicio, para estos casos también aplica esta política.
El colegio Tilatá no se hace responsable por daños que presente un equipo en las instalaciones del colegio. Cada usuario es responsable de la seguridad de su computador personal.

e. Páginas web:
El servidor bloqueará y evitará la visita de páginas en la red dedicadas a áreas que no sean de interés investigativo, capacitación, legal, o del área de competencia.
Los usuarios que requieran de videos o presentaciones en línea deben traerlas listas, es posible que las páginas desde las que se transmite dicho material estén bloqueadas por representar riesgos de seguridad para la red del colegio.

10. SOPORTE
El personal del Departamento de Sistemas del Colegio Tilatá brindará soporte en temas relacionados con los sistemas de información del colegio.
El soporte a computadores, programas u otros dispositivos que no pertenezcan al colegio está prohibido.
a. Requerimientos:
Deben ser entregados por escrito bien sea en papel, vía correo electrónico o por comunicado a la Dirección del Departamento de Sistemas. Una vez recibidos se priorizarán y asignarán a un miembro del equipo.
Se entiende como requerimiento: La falla de un equipo, de internet, de la red, la necesidad de instalar software, el resolver inquietudes, etc.

12. SANCIONES
Los usuarios que no cumplan con las políticas aquí establecidas, tendrán sanciones que repercutirán en la pérdida del servicio así:
a. Si el computador pertenece al colegio:
- Primera vez: amonestación verbal
- Segunda vez: amonestación escrita con copia al jefe inmediato

- Tercera vez: amonestación escrita con copia al jefe inmediato y pérdida del servicio por un mes.

b. Si el computador pertenece al usuario:

- Primera vez: El usuario pierde el acceso a internet por un mes.
- Segunda vez: El usuario pierde el acceso a internet por dos meses.
- Tercera vez: usuario pierde el acceso a internet por el resto del año escolar y tendrá que firmar un compromiso de buen uso para que se le habilite el servicio para el siguiente año escolar.

13. NOTIFICACIÓN

Está política debe adicionarse al procedimiento correspondiente, adicionalmente debe ser publicada en Cibercolegios y en la carpeta de documentos Tilatá para notificar a los usuarios de su existencia.

14. APLICACIÓN Y CUMPLIMIENTO

Esta política aplica a todos los integrantes del Colegio Tilatá.

He leído y acepto la política de uso de los Sistemas de Información del Colegio Tilatá

_____ _____

Nombre y Firma del Estudiante Fecha

Está política ha sido diseñada y adaptada por el Departamento de Sistemas del colegio Tilatá, apoyándose en estándares preestablecidos para la sistemas de los información de instituciones educativas.

Fuentes de información:

- http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Como-implantar-una-politica-para-uso-de-la-Internet-en-las-Empresas.php
- http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/contenidos-seguridad-virus-antivirus.php
- http://www.colpos.mx/politicas/
- http://sgsi-iso27001.blogspot.com/2008/04/poltica-de-uso-de-internet.html
- http://www.unicah.edu/servicios/CTIT/politicas.htm