POLÍTICAS DE SEGURIDAD

ENERO – MAYO 2012

DISPOSICIONES GENERALES

ARTÍCULO 1. ÁMBITO DE APLICACIÓN Y FINES

Las políticas de seguridad computacional tienen por objeto establecer los lineamientos en los cuales deben conducirse los usuarios en el uso de recursos computacionales, de manera que permita garantizar la seguridad en las tecnologías de información.

ARTÍCULO 2. DEFINICIONES

- **ITESM CQ**: Instituto Tecnológico y de Estudios Superiores de Monterrey,
- Campus Querétaro.
- **GSC:** Grupo de Seguridad Computacional del ITESM CQ. Se encarga de definir esquemas y políticas de seguridad en materia de cómputo.
- **USUARIO:** Cualquier alumno activo que haga uso de los servicios computacionales, equipos de cómputo, sistemas de información, redes y telecomunicaciones.
- **D I :** Departamento de Informática.
- **RECURSO INFORMÁTICO:** Cualquier componente físico o lógico de un sistema de información.
- **VIRUS INFORMÁTICO:** Pieza de código ejecutable con habilidad de reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.
- **SOLUCIÓN ANTIVIRUS:** Recurso informático empleado para solucionar problemas con virus. El Norton Antivirus Corporate Edition es el antivirus oficial del Sistema ITESM.
- **CONTRASEÑA:** Conjunto de caracteres que permite el acceso de un usuario a un recurso informático.

ARTÍCULO 3. FRECUENCIA DE EVALUACIÓN DE LAS POLÍTICAS.

Se evalúan las políticas del presente documento, con una frecuencia semestral y cuando el GSC-ITESM CQ lo determine.

POLITICAS DE USO ACEPTABLE

ARTÍCULO 4. GENERALES

- El ITESM CQ no es responsable por el contenido de datos ni por el tráfico que en su red circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- Nadie puede ver, copiar, alterar o destruir la información de un usuario sin el consentimiento explícito del afectado.
- No se permite el uso de los servicios de la red cuando provoquen una carga excesiva sobre recursos escasos.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad del ITESM CQ y se usarán exclusivamente para actividades académicas relacionadas con la institución.
- Todas las cuentas de acceso a los sistemas y recursos de cómputo son personales e intransferibles, se permite su uso única y exclusivamente a los propietarios de las mismas.
- Cuando se detecta un uso no aceptable de la red, se cancela la cuenta o se desconecta temporal o permanentemente al usuario involucrado. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

ARTÍCULO 5. GRUPO DE SEGURIDAD COMPUTACIONAL

- El GSC es el encargado de suministrar medidas de seguridad razonables contra la intrusión o daños a la información almacenada en los sistemas, como la instalación de cualquier herramienta, dispositivo o versión de software que refuerce la seguridad de los sistemas.
- El GSC debe poner a disposición de los usuarios e informar del software que refuerce la seguridad de los sistemas computacionales del ITESM CQ.
- El GSC es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de determinar y solucionar anomalías, usos indebidos o cualquier falla que provoque problemas de comunicación.

ARTÍCULO 6. USUARIOS

Los recursos de cómputo empleados por el usuario:

- Deben tener fines académicos.
- No deben ser proporcionados a personas ajenas.
- No deben ser utilizados para fines personales.
- Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.
- Todo usuario debe apegarse a las Políticas dispuestas para el uso del correo electrónico.
- Para reforzar la seguridad de la información de su cuenta, el usuario debe hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma.
- Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.
- Los usuarios deben cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red del ITESM CQ, de acuerdo con las políticas que en este documento se mencionan.
- Los usuarios deben solicitar apoyo al DI ante cualquier duda en el manejo de los recursos de cómputo de la institución.

ARTÍCULO 7. DEPARTAMENTO DE INFORMÁTICA

La DI puede remover información de las cuentas de los usuarios, en los siguientes casos:

- Si la información no es de carácter académico.
- Si pone en peligro el buen funcionamiento de los sistemas.
- Si se sospecha de algún intruso utilizando una cuenta ajena.
- Cuando el usuario se lo solicite mediante un documento explícito

POLITICAS ANTIVIRUS

ARTÍCULO 8. POLÍTICAS ANTIVIRUS GENERALES

- Se recomienda a los usuarios que cuenten con equipos de cómputo portátil instalar y configurar la Solución Antivirus Oficial del Sistema ITESM.
- Para aquellos equipos que cuenten con la Solución Antivirus Oficial del Sistema, diariamente se realiza un rastreo automático mediante la Solución

Antivirus para detectar y eliminar virus de documentos, archivos ejecutables, correos recibidos y páginas Web mientras se encuentre conectado a la red del Campus.

- En caso de que el equipo portátil de los usuarios se vea afectado por la presencia de algún virus, deberá acudir a CASTI para solicitar asesoría en la limpieza de su equipo en los horarios correspondientes
- (Sala de Alumnos 8:00 a 14:00 y de 16:00 a 18:00 horas; CASTI Prepa 7:00 a 18:00 horas.).

ARTÍCULO 9. USUARIOS DE LA RED DEL ITESM CQ

- El usuario no debe desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
- Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.
- El usuario que cuente con una computadora con recursos limitados, debe contar con la versión ligera de la Solución Antivirus Institucional.
-

SANCIONES

ARTÍCULO 10. GENERALES

- Cualquier acción que vaya en contra de las políticas de seguridad computacional del ITESM CQ será sancionada con la suspensión de los servicios de cómputo y red por el período que le corresponda según sea el caso:
    a. Infracción al Reglamento de uso de Equipos Computacionales
        - Primer aviso, suspensión del servicio por 3 días hábiles
        - Segundo aviso, suspensión del servicio por 5 días hábiles
        - Tercer aviso, suspensión del servicio por el tiempo restante del semestre.

Si el usuario ha recibido más de tres avisos, se le suspenderá el servicio para el siguiente período semestral, además se le notificará al Director de carrera del programa correspondiente y al Departamento de Desarrollo Estudiantil.