UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA
Coordinación General de Tecnologías de Información
Coordinación de Seguridad en Cómputo

Manual de Políticas de Seguridad en Cómputo

Introducción

La Política de Seguridad en Cómputo (PSC) sirve para crear un ambiente que ayude a proteger a todos los usuarios miembros de la comunidad universitaria que utilicen los servicios de Tecnologías de Información (TI) de la Universidad Autónoma de Chihuahua (Uach) de las amenazas internas y externas que podrían comprometer la privacidad, productividad, la reputación o los derechos intelectuales.

La PSC reconoce el papel tan importante que la información representa en la Universidad: la docencia, la investigación, la extensión, y las funciones administrativas; así como la importancia de tomar las medidas necesarias para proteger la información en todas las formas actualmente conocidas.

Mientras que más información es utilizada y compartida por los estudiantes, docentes, investigadores, la administración de las Unidades Académicas (UA) y la administración central; mejores deben de ser los esquemas de protección, vigilancia y monitoreo, para salvaguardar y proteger la información generada.

La PSC sirve para proteger recursos de la información contra amenazas dentro y fuera de la UACh estableciendo responsabilidades, pautas, y prácticas las cuales ayudarán a la comunidad universitaria para prevenir, disuadir, detectar, responder, y recuperarse de incidentes ocurridos a estos recursos; así como para fomentar un ambiente de la difusión segura de la información.

La PSC de la UACh es establecida por la Coordinación General de Tecnologías de Información (CGTI) a través de la Coordinación de Seguridad en Cómputo (CSC), quién debe implementar, fomentar, difundir y vigilar su ejecución.

1. Criterios.

Los criterios utilizados en esta política esta basada en los siguientes principios:

1.1. Ayuda en la misión universitaria. La PSC está diseñada para apoyar la misión de la UACh, protegiendo los servicios y recursos de TI, la información institucional, la reputación, la posición legal, y la capacidad de conducir las operaciones propias de la UACh. Esta política se crea para facilitar las actividades que son importantes para la Universidad.

1.2. Apropiada y costeable. No todos los recursos de la información requieren el mismo nivel de mecanismos de seguridad o de protección. Los requisitos de la PSC fueron formulados con el objetivo de que el uso de las medidas de seguridad sea establecido con la sensibilidad y el valor de los recursos de la información y de las amenazas reales a esos recursos.

La intención no es dictar requisitos que la puesta en práctica, impondría costos innecesarios, sino ayudar a evitar la pérdida de información y el gasto en recuperarse en caso de que ocurra un Incidente de Seguridad en Cómputo (ISC).

1.3. Responsabilidad compartida. Todos los miembros de la comunidad universitaria poseen la responsabilidad de proteger los recursos de la información a los cuales tienen acceso. La PSC reconoce que la comunidad necesitará la información, el entrenamiento, y las herramientas adecuadas para ejercer sus responsabilidades y que estas responsabilidades se deben hacer explícitas.

1.4. Flexible y adaptable. La política define procedimientos y prácticas específicas, solamente cuando sea necesario para proporcionar la protección adecuada. La meta es que los miembros de la comunidad universitaria puedan determinar a su discreción y mejor juicio el decidir cómo proteger la información de la cual son responsables, conforme a las obligaciones legales y otras emitidas por la UACh.

1.5. Estado de preparación en caso de emergencia. No es posible prevenir todos los incidentes de seguridad. La PSC se diseña para asegurarse de que las medidas apropiadas están tomadas para los posibles incidentes, incluyendo la puesta en práctica de de medidas para la continuidad de la operación así como proteger los sistemas, servicios y procesos críticos que contengan información.

2. Alcance

2.1. Equipos. La PSC cubre todos los recursos y servicios de TI que sean propiedad de la UACh o utilizados por la Universidad bajo licencia o contrato. Esto incluye la información registrada en todos los tipos de medios (análogos, digitales, hardware, software, en papel y de sistemas de telefonía). La PSC protege contra los actos intencionales y no intencionales que podrían comprometer el secreto, la integridad, o la disponibilidad de los servicios y recursos de la información universitaria.
La PSC se crea para tratar amenazas internas y externas; pero no se limita a: error, fraude, malversación, acceso no autorizado, spamming, hurto, sabotaje, terrorismo, extorsión, violaciones a la privacidad, interrupción del servicio, y desastres naturales.

2.2. Personas. Esta política se aplica a toda la comunidad universitaria (estudiantes, personal académico y administrativo), contratistas, consultores, empleados temporales, huéspedes, voluntarios, incluyendo los que sean afiliados con terceros, y que tienen acceso a los servicios y equipos de TI e información universitaria.

2.3. Recursos de Información. Esta política se aplica a todos los recursos y servicios de información universitaria, incluyendo los usados por la UACh bajo licencia o contrato.
Los recursos de información incluyen la información en cualquier forma y almacenada en cualquier medio de información, todos los equipos de cómputo (servidores y estaciones de trabajo), equipo y software de comunicaciones.

3. Clasificación de la información

Toda la información cubierta por la PSC se le asigna una de las tres clasificaciones dependiendo del nivel de seguridad requerido.

En orden descendente, de acuerdo a la importancia, estas clasificaciones son:

- Confidencial.
- Uso interno.
- Sin restricción.

3.1. Información confidencial. Esta clasificación cubre la información importante sobre los individuos e información sensible sobre la UACh. La información que recibe esta clasificación requiere un alto nivel de protección contra el acceso, modificación, destrucción y el uso no autorizado.
Dentro de esta clasificación está:

a) La información de los empleados actuales, anteriores, y anticipados, incluyendo el empleo, la paga, los datos, las prestaciones y otra información del personal.
b) Información de operaciones de negocio universitaria, finanzas, asuntos legales, u otras operaciones de una naturaleza particularmente sensible.
c) Los datos de la seguridad de información, incluyendo contraseñas, información sobre incidentes seguridad, esquemas y mecanismos de protección, direccionamiento IP, monitoreo de la red universitaria.
d) Otros datos que sean considerados por las autoridades universitarias que pertenezcan a esta clasificación.

3.2. Uso Interno. Esta clasificación cubre la información que requiere la protección contra acceso, la modificación, la destrucción, y el uso no autorizado, pero la sensibilidad de la información es menos que la información confidencial. Los ejemplos de información de uso interno son notas internas, correspondencia (electrónica y convencional) y otros documentos.

3.3. Información sin restricción (pública). Esta clasificación cubre la información dentro de la cual puede ser divulgada a cualquier persona o dentro y fuera de la UACh. Aunque los mecanismos de seguridad no son necesarios para controlar el acceso y la difusión, se requieren para protegerla contra la modificación y la destrucción no autorizada de la información.
Los ejemplos de este tipo de información son las publicaciones realizadas en el portal universitario, avisos, circulares, etc.

4. Responsabilidades

Todos los miembros de la comunidad universitaria comparten la responsabilidad de proteger los recursos de información a los cuales tienen acceso. Todas las responsabilidades dispuestas en esta sección se asignan a cuatro grupos:

- Usuario.
- Administrador.
- Responsable administrativo.
- Responsable técnico.

4.1. ***Usuario***. Todos los miembros de la comunidad universitaria que utilicen los recursos de información se encuentran en la clasificación de usuarios. Los usuarios incluyen, por ejemplo, a alumnos, catedráticos, al personal administrativo, contratistas, consultores y empleados temporales. Los usuarios son responsables de proteger los recursos de la información a los cuales tienen acceso. Sus responsabilidades cubren los dispositivos automatizados y no

automatizados de información y de tecnología de información (papel, informes, libros, películas, computadoras, discos, impresoras, teléfonos, máquinas de fax, etc.) que estén en su cuidado o posesión.
Seguirán las prácticas de la seguridad de la información enumeradas abajo, así como cualquier práctica aplicable local departamental u otra específica de la seguridad de la información.

4.2. ***Administrador***. Los administradores son aquellos miembros de la comunidad universitaria que tienen la responsabilidad primaria de la información y equipo, un usuario adquiere la categoría de administrador por designación o en virtud de los recursos desarrollados, o creados de la información para los cuales nadie más tiene acceso, dicho usuario deberá de tener los conocimientos y competencias para realizar esta actividad.
Toda la información cubierta bajo esta política deberá de ser asignada a un administrador.
El término de administrador utilizado aquí no implica propiedad en ningún sentido legal.
Los administradores tienen las responsabilidades como administrador y usuario de su información ya que además, son responsables de lo siguiente:

a) Hacer cumplir las políticas y procedimientos de la seguridad.
Los administradores pueden establecer políticas locales y procedimientos específicos de la seguridad para la información bajo su resguardo cuando sea apropiado. Los administradores son responsables de los procedimientos relacionados con la creación, la retención, la distribución y la disposición de la información. Los administradores pueden imponer los requisitos adicionales que realzan la seguridad de la información.

b) Asignar clasificaciones y marcar la información.
Los administradores son responsables de determinar la clasificación de su información y de cualquier requisito específico del manejo de la información que vayan más allá de esta política. La información que es confidencial o de uso interno será marcada como tal cuando se presente o se distribuye a los usuarios. Las notas adicionales que especifican requisitos del manejo y de la distribución pueden ser agregadas.

c) Determinación de autorizaciones.
Los administradores determinan quién esta autorizado para tener acceso a su información. Se cerciorarán de que ésos que acceden tengan una necesidad de saber la información y de saber los requisitos de la seguridad para esa información.

d) Llevar un registro.
Los administradores guardarán expedientes que documentan la creación, la distribución, y la disposición de la información confidencial.

e) Reporte de incidentes.
Los administradores deberán de reportar los incidentes que se presenten en los equipos bajo su resguardo a la CSC. Los incidentes serán tratados como confidencial a menos que haya una necesidad de emitir información específica.

f) Actualizaciones.
Los administradores serán los responsables de la instalación de las actualizaciones de los parches de seguridad del software instalado en los equipos bajo su resguardo.
Se considera a los alumnos los administradores de su propio trabajo.

4.3. ***Responsable administrativo***. El responsable directo tanto del equipo, así como de cualquier tipo información almacenada en el mismo, es aquella persona que haya firmado por el resguardo del equipo.

a) El responsable administrativo puede ser administrador y usuario.
b) El responsable administrativo será el responsable físico y lógico del equipo, así como también del resguardo de la cuenta de administración del equipo a su cargo, la cual deberá ser única y deberá ser proporcionada solo a personal autorizado (responsable técnico, administrador, auditor o personas que estén autorizadas por su jefe inmediato) y sólo para elaborar actividades de mantenimiento preventivo y/o correctivo, así como auditorias de seguridad.

Si el responsable administrativo del equipo no cuenta con el conocimiento necesario para proteger su equipo y la información, deberá asignar a un responsable técnico.

4.4. ***Responsable técnico***. El responsable técnico es aquella persona designada por el responsable administrativo para dar mantenimiento preventivo y/o correctivo a los equipos.
El responsable técnico sólo puede ser aquella persona que tenga el conocimiento requerido para ello. Este puede ser designado por la autoridades competentes en cada área.
Si no existe un responsable técnico en su área, el responsable técnico será el DAU mediante solicitud previa levantada por el responsable, el DAU atenderá la solicitud según los acuerdos de servicio publicados.

5. Políticas

5.1. ***Familiaridad con las políticas universitaria.*** Se espera que los usuarios implementen todas las políticas universitaria y ejerciten el buen juicio en la protección de los recursos de la información. Deben de familiarizarse con esta política con respecto al acceso y a la privacidad. Deben estar enterados que el no seguir esta política podría conducir a una acción disciplinaria.

5.2. ***Seguridad física***. Los usuarios proporcionarán la seguridad física para sus dispositivos de la tecnología de información. Las puertas serán cerradas con seguro para proteger el equipo cuando las áreas que las contienen son desatendidas. Los dispositivos de seguridad externos serán desplegados en las áreas que no se pueden proteger con eficacia por otros medios. El equipo portátil tal como laptop, PDAs, y teléfonos portátiles se debe proteger por programas antirrobo. El cuidado particular en casa es necesario para proteger estos dispositivos.

5.3. ***Almacenamiento de la información.*** La información que esta clasificada como confidencial se debe mantener en un lugar que proporcione un alto nivel de protección contra el acceso no autorizado y no llevarla fuera universitaria a menos que pueda ser protegida de manera adecuada. En general, esto significa almacenar la información detrás de una cerradura física o electrónica, por ejemplo, en una oficina, o el escritorio que se mantendrá cerrado cuando el usuario no está presente, o en una computadora que proporcione controles de acceso adecuados. Se recomienda la encriptación para la información almacenada electrónicamente en todas las computadoras, especialmente dispositivos portátiles tales como laptop o ayudantes personales digital (PDAs) que sean vulnerables al hurto o a la pérdida.

5.4. ***Destrucción y disposición de la información y de los dispositivos***. La información confidencial se debe destruir de tal manera que no pueda ser recuperada por personas no autorizadas. Para los documentos físicos las trituradoras de papel se recomiendan altamente, pero por lo menos, los documentos no deben ser puestos en los compartimentos de reciclaje.
Para donar, vender, transferir o disponer de las computadoras o de los medios desprendibles (tales como diskettes, discos duros, etc.), se debe tener cuidado para asegurarse de que los datos confidenciales son ilegibles.

5.5. ***Contraseñas.*** Acceso a las computadoras, usos del software, y la información electrónica se controla mediante identificadores y contraseñas de usuario. Los usuarios son responsables de generar y proteger las contraseñas que les conceden el acceso a los recursos. Debido a que las contraseñas compartidas y los identificadores presentan un riesgo importante de la seguridad, los identificadores y las contraseñas del usuario nunca deben ser compartidos.

Las contraseñas que proporcionan el acceso a los recursos de la red universitaria no se deben almacenar en las estaciones de trabajo y no se deben exhibir en notas (post-it,etc) cerca de las computadoras.
Las contraseñas deben ser de 8 o más caracteres de largo. Incluir letras, números, y caracteres de puntuación (donde sea posible). No deben de ser nombres, palabras que se encuentren publicadas en diccionarios, permutaciones de datos personales (fechas de nacimiento, los números de Seguro Social, etc.).

5.6. ***Seguridad de la Computadora.*** Los usuarios deben tomar medidas para proteger las estaciones de trabajo, computadora portátil y/o PDA's contra intrusos. Es responsabilidad del usuario asegurarse de que los parches de seguridad estén aplicados en sus equipos (programas que corrigen vulnerabilidades de la seguridad del software, distribuido a por el fabricante).
Deben cooperar con y servirse de cualquier servicio que la CGTI proporcione para la ayuda y/o la revisión de estas actividades.

5.7. ***Acceso remoto.*** Muchos sistemas operativos se pueden configurar para permitir el acceso a través de Internet y de otras redes. Los usuarios deben tomar las precauciones y extremo cuidado para asegurarse de que sus sistemas están configurados para prevenir el acceso no autorizado. En determinado caso cuando se tenga que permitir el acceso remoto, se debe tomar especial cuidado para seleccionar opciones seguras y asegurarse de configurar correctamente los servicios aplicando restricciones y otros controles de acceso. Al permitir el acceso remoto a una computadora o a un dispositivo particular en la red universitaria puede tener como consecuencia que permita el acceso, autorizado e ilícito, a otras computadoras y recursos de la red, así que se pone en riesgo más que el equipo que está siendo afectado.

5.8. ***Terminar sesión.*** Los usuarios deberán de terminar la sesión de las aplicaciones, de computadoras y de redes cuando hayan terminado su trabajo. Si las estaciones de trabajo están situadas en oficinas o laboratorios seguros, los usuarios no dejarán los equipos desatendidos con sesiones abiertas sin asegurar las puertas de la oficina. Si las computadoras están situadas en un laboratorios abiertos o compartidos, los usuarios entonces terminarán su sesión completamente.
Se recomienda el uso de contraseñas para iniciar el sistema operativo o el arranque de la máquina en ambientes donde las personas no autorizadas pueden tener acceso físico a las computadoras. El apagar el monitor de la computadora cuando no este en uso puede también desalentar a tales personas de intentar entrar a las computadoras. Así como también se recomienda el uso de contraseña en el screensaver, donde se aplique.

5.9. ***Protección contra virus y codigo malicioso***. Los usuarios se cerciorarán de que sus equipos de trabajo empleen los mecanismos que protegen contra virus y otras formas de código malicioso, que se pueden distribuir con E-mail o la red local. La UACh cuenta con licencias de software AntiVirus Institucional (AVI). La cual debe de estar instalada en todos los equipos de cómputo propiedad de la UACh. En caso que por alguna circunstancia el usuario se percate que en el equipo en el cual se este trabajando no cuente con la protección del AVI, se deberá de realizar la solicitud para su instalación. La actualización del AVI se realiza de manera automática, la cual no puede ser interrumpida por el usuario.
Los usuarios deben de tomar precauciones en archivos que descargan de la red, así como de correos electrónicos, y deben de asegurarse de no ejecutar archivos sospechosos o de dudosa procedencia.
Si se detecta un virus, este debe ser eliminado inmediatamente.

5.10. ***Respaldos.*** La información que se genera por parte de los empleados de la UACh en las estaciones de trabajo se considera como información Institucional, por lo que deberá de ser respaldada conforme a lo establecido en la instrucción de trabajo general de Respaldo de Información Institucional (ITR 7.5 CSC 01) del Sistema de Gestón de Calidad (SGC) de la CGTI.

En el caso de los alumnos, ellos serán los responsable de respaldar su información.

5.11. ***Acceso a Internet.*** Los equipos de cómputo propiedad de la UACh que se encuentren conectados a la red Universitaria tendrán conexión hacia Internet a través del sistema de Proxy Institucional y estarán bajo la protección perimetral. Para el uso de Internet se deberá de configurar en el navegador el proxy, esto deberá de ser realizada por el responsable técnico (ver 4.4).

5.12. ***Protección perimetral.*** Debido a que cada día se presentan más problemas de virus informáticos, ataques y robos de información en Internet, es necesario la utilización de un esquema para restringir en acceso desde el exterior hacia la red de la Universidad, aunado al hecho que el ancho de banda es un recurso limitado, es necesaria la implementación de un esquema de control de acceso desde y hacia Internet, esto es utilizando una solución basada en equipos firewall (FW), sistema de detección de intrusos (IDS) y el sistema de proxy, el primero es el que se encarga de evitar los accesos no deseados, el segundo de auxiliar en la detección de intrusos en la red y el tercero de proveernos de un uso adecuado del ancho de banda así cómo de proporcionar un caché de memoria de las páginas web accesadas por los usuarios de la red Universitaria.

Bajo este esquema todos los equipos de la Red Universitaria se encuentran protegidos por esta solución, la cual se complementa con el software de antivirus institucional instalado en cada equipo.

En dado caso de que se requiera que un equipo no esté protegido por el firewall, es necesario realizar una solicitud expresa. Dicha solicitud deberá de ser oficial, por escrito y dirigida al Departamento de Atención a Usuarios (DAU), indicando la razón por la cual se requiere que el equipo esté fuera del firewall; la aplicación y los puertos hacia donde se va a realizar la comunicación; el nombre del usuario, del responsable administrativo y del responsable técnico, con estos datos se levantará una solicitud de servicio nuevo la cual requiere de la autorización del CGE, una vez aprobada se turnará hacia la CSC, será necesario realizar una auritoría de seguridad, para verificar que el equipo cumple con los requisitos mínimos para su uso fuera del firewall, tomando en cuenta que el hecho que un equipo que esté fuera del firewall no implica que no se requiere del proxy para navegar en Internet.

Los equipos a ser expuestos fuera del firewall, deberan de cumplir con los siguientes requisitos:

a) El Sistema Operativo (SO), deberá de tener instalados los últimos parches de seguridad:
   - Equipos con SO Windows 95, 98 y ME no serán puestos fuera del firewall, debido a que no cuentan con esquemas de seguridad nativos del SO.
   - En equipos con SO Windows NT, 2000 y XP, es necesario la utilización de un firewall de host (consultar seguridad.uach.mx para la recomendación de FW disponibles).
   - En equipos con SO Unix (Linux, Solaris, MacOS), es necesario la eliminación de puertos no utilizados y el uso de iptables.

b) Software de AVI, deberá de tenerlo propiamente instalado y actualizado.

c) La frecuencia de las auditorías será trimestral, salvo en caso de una falla de seguridad del fabricante del SO, lo cual ocasionará que el equipo sea protegido por el esquema de seguridad perimetral, por lo que el responsable del equipo deberá de actualizar el SO y solicitar al DAU el servicio de liberación de equipo del FW, para volver a desproteger el equipo.

5.13. ***Equipos móviles.*** Los equipos portátiles propiedad de la UACh debido a que se pueden conectar a otras redes (por Dial-Up, cable, GSM, etc.), de las cuales la Universidad no es responsable, estos equipos deberán de cumplir lo establecido en el apartado 5.12. El equipo solo podrá ser utilizado para actividades relacionadas con la universidad. No podrá tener programas instalados ajenos a este propósito como pueden ser: Chats, mensajería instantánea, compartición de archivos(música,juegos,video,etc.).

El equipo podrá ser auditado por la CSC en cualquier momento, si el equipo no cumple con las características el equipo podrá ser reasignado.