LINEAMIENTOS INSTITUCIONALES DE SEGURIDAD INFORMÁTICA

Contenido

1.0 Justificación

Las tecnologías de la información han originado principalmente el uso masivo y universal del Internet, las instituciones se ven inmersas en ambientes agresivos donde el sabotaje, robo de datos, daño de información, ataques informáticos son cada vez más frecuentes y sofisticados.

Conforme las tecnologías se han esparcido, se han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

La seguridad informática se ha convertido en cuestión de seguridad nacional en algunos países y esta tendencia está siendo adoptada por muchas organizaciones, por ello contar con lineamientos de seguridad informática es imprescindible para proteger los activos de la institución.

Por lo anterior, surge la necesidad de crear Lineamientos Institucionales de Seguridad Informática, los cuales permitirán implementar mecanismos para salvaguardar la información y recursos informáticos de la Universidad Autónoma de Chihuahua.

2.0 Introducción

Los requerimientos de seguridad que involucran las tecnologías de la información en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como lo es Internet, situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Esto ha originado que organizaciones gubernamentales y no gubernamentales desarrollen políticas y recomendaciones que regularicen el uso adecuado de las Tecnologías de Información para aprovechar sus ventajas y beneficios, evitando con ello su uso indebido que ocasiona problemas en los bienes y servicios de las entidades.

De esta manera, los Lineamientos Institucionales de Seguridad Informática de la Universidad Autónoma de Chihuahua emergen como un instrumento para concientizar a sus integrantes acerca de la importancia y sensibilidad de la información y servicios críticos.

El proponer estos lineamientos de seguridad requiere un alto compromiso con la institución, agudeza técnica para detectar fallas y deficiencias, así como constancia para renovar y actualizar dichos lineamientos en función del ambiente dinámico que nos rodea.

3.0 Alcance

Los presentes lineamientos aplican para todos los usuarios y administradores de equipos de cómputo, redes de datos, servicios electrónicos, sistemas de información y cualquier otro tipo de servicio de la plataforma tecnológica de la Universidad Autónoma de Chihuahua, incluyendo a los usuarios de los servicios de Internet de la misma.

4.0 Políticas de seguridad

4.1 Restricciones generales del uso de la plataforma tecnológica de la UACH

4.1.1 Se prohíbe el uso de los recursos tecnológicos de la Universidad Autónoma de Chihuahua para llevar a cabo actos delictivos como fraude, extorsión, suplantación de identidad, amenazas, difamación, actos de corrupción, acoso de cualquier tipo, o cualquier otro acto que atente contra la integridad física y/o moral de cualquier persona, agrupación o institución.

4.1.2 Se prohíbe planear o llevar a cabo cualquier acción que atente contra la integridad, confidencialidad, disponibilidad y/o rendimiento de la plataforma tecnológica de la Universidad Autónoma de Chihuahua o de cualquier otra organización.

4.1.3 Se prohíbe el uso de los recursos tecnológicos para promoción o beneficio personal fuera de los objetivos educativos, de investigación, administrativos y demás fines que de manera clara conforman a la UACh.

4.1.4 Se prohíbe el uso de los recursos tecnológicos para realizar cualquier tipo de acto que implique la violación a derechos de autor.

4.1.5 Se prohíbe el tratar de obtener cuentas de usuario ajenas, o utilizar cuentas de usuario ajenas para acceder a cualquier recurso de la plataforma tecnológica de la Universidad Autónoma de Chihuahua o de cualquier organización sin la autorización debida.

4.1.6 Se prohíbe el desarrollo, uso, distribución y/o promoción de métodos, herramientas, mecanismos, software, hardware y/o técnicas que afecten la integridad, confidencialidad, disponibilidad y/o rendimiento de la plataforma tecnológica de la Universidad Autónoma de Chihuahua o de cualquier otra organización.

4.1.7 Se prohíbe acceder modificar, alterar, sustraer, reemplazar y/o borrar documentos, archivos, programas, bases de datos, código de programación, configuraciones, parámetros o cualquier otro tipo de información y/o datos sin contar con la autorización debida por parte de las autoridades universitarias y/o administradores de dichos recursos.

4.1.8 Todo recurso tecnológico generado y/o adquirido por la Universidad Autónoma de Chihuahua o sus dependencias, es de propiedad exclusiva de la Universidad Autónoma de Chihuahua (incluyendo cualquier tipo de información, datos, archivos, bases de datos, sistemas de información, código fuente, equipos, accesorios y cualquier otro recurso y/o activo), por lo que no puede ser utilizado ni ser respaldado sin la autorización debida por parte de las autoridades universitarias, o bien, por los requerimientos que demande las funciones de los empleados de la Universidad Autónoma de Chihuahua.

4.1.9 Las autoridades universitarias podrán solicitar mediante un oficio dirigido al Coordinador General de Tecnologías de Información la suspensión del acceso total o parcial de cualquier servicio de tecnologías de información a los usuarios sobre los cuales tenga injerencia, cuando lo consideren pertinente bajo razones debidamente justificadas. De igual forma, para restablecer los servicios suspendidos a usuarios, deberá dirigir un oficio al Coordinador General de Tecnologías de Información.

4.2 Uso del servicio de internet

4.2.1 La Coordinación General de Tecnologías de Información es el área responsable de proporcionar el acceso a Internet en las dependencias de la Universidad Autónoma de Chihuahua, por lo cual la Coordinación General de Tecnologías de Información deberá tener identificados todos los puntos de conexión a Internet dentro de las instalaciones de la Universidad Autónoma de Chihuahua.

4.2.2 Todos los enlaces hacia Internet instalados dentro de la Universidad Autónoma de Chihuahua, deben contar con algún mecanismo de seguridad perimetral como firewalls, proxies, etc.

4.2.3 Queda prohibido el acceso a sitios web y/o uso de servicios de Internet afines a pornografía, apuestas, juegos en línea, redes peer-to-peer y todos aquellos que se consideren ilegales por cualquier ley municipal, estatal o federal del país.

4.2.4 Queda prohibido el acceso a sitios web y uso de servicios de Internet para fines personales, de ocio y/o que puedan afectar el rendimiento laboral del personal administrativo o académico.

4.2.5 Queda prohibido el uso de servicios de Internet que de manera arbitraria saturen enlaces de datos o cualquier elemento de la plataforma tecnológica universitaria o de cualquier otra organización.

4.2.6 Queda prohibido el uso de servicios, equipos y/o herramientas informáticas que generen túneles entre equipos de la Universidad Autónoma de Chihuahua y sitios externos, por ejemplo: uso de proxies ajenos a la Universidad Autónoma de Chihuahua, conexiones VPN, sesiones remotas por SSH, telnet, RDP, VNC, etc., a excepción de aquellos que sean para fines educativos, de investigación o que las funciones laborales lo requieran, siendo necesario justificar y dar aviso de la situación al equipo de respuesta a incidentes de seguridad informática (CERT-UACh).

4.2.7 Cualquier servicio de Tecnologías de Información dentro de la Universidad Autónoma de Chihuahua que requiera ser accedido desde Internet, deberá ser notificado y autorizado por la Coordinación General de Tecnologías de Información.

4.2.8 Todos los usuarios de la Universidad Autónoma de Chihuahua podrán acceder a sitios web y servicios de Internet desde las instalaciones de la Universidad Autónoma de Chihuahua con fines educativos, de investigación y aquellos que demanden sus funciones dentro de la institución, tomando en cuenta los puntos anteriores.

4.2.9 Se recomienda no responder encuestas en línea o correos electrónicos de cualquier procedencia (incluyendo si aparentan ser de la propia Universidad Autónoma de Chihuahua o de instancias gubernamentales) que soliciten datos personales, datos institucionales, cuentas de usuario, datos bancarios, etc. En caso de presentarse alguna situación de este tipo, cualquier usuario de la Universidad Autónoma de Chihuahua podrá comunicarse al Departamento de Atención a Usuarios de la Coordinación General de Tecnologías de Información para reportar la situación y pedir asesoría.

4.2.10 Se recomienda no instalar programas que vienen adjuntos en correos electrónicos, o que se descargan de sitios de Internet cuyo origen es desconocido o de dudosa procedencia. En caso de presentarse alguna situación de este tipo, cualquier usuario de la Universidad Autónoma de Chihuahua podrá comunicarse al Departamento de Atención a Usuarios de la Coordinación General de Tecnologías de Información para reportar la situación y pedir asesoría.

4.2.11 Se recomienda nunca dejar sesiones activas de servicios de correo electrónico, redes sociales o de cualquier tipo una vez que el usuario ha terminado de utilizarlos, o cuando se aleja de su equipo de cómputo.

4.2.12 La Coordinación General de Tecnologías de Información podrá llevar a cabo tareas de monitoreo del tráfico de Internet, con la intensión de prevenir y contrarrestar ataques informáticos.

4.3 Equipos de cómputo

4.3.1 Todos los equipos de cómputo propiedad de la Universidad Autónoma de Chihuahua deberán ser utilizados exclusivamente para fines educativos, académicos, de investigación, administrativos y aquellos que exija la función del usuario.

4.3.2 Todos los equipos de cómputo propiedad de la Universidad Autónoma de Chihuahua deberán contar con usuario y contraseña para acceder al ó a los sistemas operativos que tenga instalados. Sólo el administrador del equipo podrá acceder a éste, o bien, otorgar autorización a otros usuarios para acceder a sus recursos.

- *Nombre de usuario*: Al menos 8 caracteres (utilizar caracteres alfabéticos en minúscula y mayúscula, así como caracteres numéricos).
- *Password*: Al menos 8 caracteres (debe ser distinto al nombre de usuario, debe utilizar y combinar caracteres alfabéticos, numéricos y especiales).

4.3.3 Todos los equipos de cómputo propiedad de la Universidad Autónoma de Chihuahua que cuenten con algún sistema operativo de la marca Microsoft versión Windows 2000 o superior, deberán contar con un software antimalware institucional vigente, actualizado y con licencia original.

4.3.4 Todos los equipos de cómputo propiedad de la Universidad Autónoma de Chihuahua deberán contar con los parches y actualizaciones más recientes de sistemas operativos y demás software que tenga instalado.

4.3.5 Todos los equipos de cómputo propiedad de la Universidad Autónoma de Chihuahua deberán contar con licencia original del ó de los sistemas operativos que tenga instalados.

4.3.6 Todos los equipos de cómputo propiedad de la Universidad Autónoma de Chihuahua deberán contar con el licenciamiento original y/o legal pertinente del software instalado.

4.3.7 La Coordinación General de Tecnologías de Información podrá realizar auditorías de seguridad, auditoría de licenciamiento de software y monitoreo de uso sobre todos los equipos de cómputo propiedad de la Universidad Autónoma de Chihuahua, con la finalidad de verificar el cumplimiento de los puntos pertinentes señalados en estos Lineamientos Institucionales de Seguridad.

4.4 Red universitaria

4.4.1 Los usuarios conectados a la red universitaria pueden acceder exclusivamente a servicios de la red local y servicios públicos sobre los cuales tenga autorización debida.

4.4.2 La red universitaria deberá ser utilizada exclusivamente para fines académicos, educativos, de investigación, administrativos, y aquellos que por las funciones y responsabilidades de los usuarios dentro de la organización deban realizar.

4.4.3 Queda prohibido utilizar mecanismos de escaneo y/o monitoreo de tráfico de red y/o de puertos de comunicaciones, a excepción de funciones de mantenimiento autorizadas por los administradores de red y que no tengan la intención de afectar la integridad de los activos de la plataforma tecnológica de la Universidad Autónoma de Chihuahua o de cualquier otra organización.

4.4.4 Se prohíbe la conexión de equipos de telecomunicaciones (routers, switches, puntos de acceso, concentradores, etc.) sin la autorización de la Coordinación General de Tecnologías de Información.

4.4.5 Las tomas de red no utilizadas de manera regular, deben estar deshabilitadas.

4.4.6 La Coordinación General de Tecnologías de Información tiene la facultad de suspender o eliminar, sin previo aviso al usuario, el acceso a los servicios de tecnologías de información a cualquier equipo que lleve a cabo algún ataque informático que afecte o implique un riesgo mayor a la integridad, confidencialidad y disponibilidad de cualquier activo crítico de la plataforma tecnológica de la Universidad Autónoma de Chihuahua.

4.4.7 Las redes LAN inalámbricas que forman parte de la red universitaria, deberán restringir el acceso a los usuarios mediante algún mecanismo de autenticación (excepto aquellas que deban ser redes públicas como wifi_uach), privilegiando el uso de WPA2.

4.4.8 Los usuarios de las redes LAN inalámbricas deberán contar con la autorización de los administradores de la red local para conectarse a dicha red inalámbrica. El administrador de la red proporcionará la clave de acceso al usuario, siempre y cuando lo considere pertinente.

4.4.9 La Coordinación General de Tecnologías de Información podrá realizar tareas de monitoreo del tráfico de la red de datos, con la intensión de prevenir y contrarrestar ataques informáticos.

4.5 Redes públicas (wifi_uach)

4.5.1 Se prohíbe el uso de analizadores de espectro, analizadores de frecuencia, analizadores de tráfico y/o cualquier otro mecanismo de análisis y monitoreo en esta y cualquier otra red de la Universidad Autónoma de Chihuahua.

4.5.2 Se prohíbe el acceso a otras redes de la Universidad Autónoma de Chihuahua, a excepción de aquellos servicios web públicos.

4.5.3 Se prohíbe la implementación de cualquier tipo de servicio por parte de los usuarios en esta red universitaria.

4.5.4 Queda prohibida la conexión de clientes de correo electrónico hacia los servidores del correo universitario. Como opción, los usuarios de correo electrónico de la Universidad Autónoma de Chihuahua pueden utilizar el servicio “Correo” en el sitio web http://www.uach.mx en la sección “Mis Servicios de TI” para la recepción y envío de correos exclusivamente con su cuenta y contraseña personales.

4.5.5 Es altamente recomendable evitar realizar operaciones electrónicas que impliquen transacciones financieras y/o bancarias utilizando redes públicas como “wifi_uach”.

4.5.6 La Coordinación General de Tecnologías de Información podrá realizar tareas de monitoreo del tráfico de datos, con la intensión de prevenir y contrarrestar ataques informáticos.

4.6 Servicios electrónicos y sistemas de información universitarios

4.6.1 Los servicios electrónicos y los sistemas de información que ofrece y/o desarrolla la Universidad Autónoma de Chihuahua deberán utilizar software con licencia original.

4.6.2 Los usuarios de los servicios electrónicos y/o de sistemas de información de la Universidad Autónoma de Chihuahua, sólo podrán acceder a ellos siempre y cuando cuenten con la autorización adecuada, y deben hacerlo exclusivamente con su cuenta de usuario y password asignado por el administrador del servicio y/o sistema universitario.

4.6.3 Se prohíbe a cualquier usuario ejecutar cualquier tipo de mecanismo para recuperar cuentas de usuario y/o password. En caso de perder la cuenta de usuario y/o password, el usuario deberá comunicarse con el Departamento de Atención a Usuarios de la Coordinación General de Tecnologías de Información para reportar la situación.

4.6.4 Los administradores de servicios electrónicos y de los sistemas de información de la Universidad Autónoma de Chihuahua deben contar al menos con bitácoras de usuarios, accesos, cambios y/o actualizaciones realizados en el servicio y/o sistema. Estas bitácoras deberán ser revisadas y analizadas periódicamente por el administrador del servicio y /o sistema de información.

4.6.5 Cualquier servicio electrónico (como páginas web, correo electrónico, FTP, SSH, etc.) o sistema universitario que requiera ser accedido desde fuera de la Universidad Autónoma de Chihuahua, deberá ser reportado al equipo de respuesta a incidentes de seguridad informática (CERT-UACh) para verificar la factibilidad de su publicación.

4.6.6 Se deben eliminar las cuentas por defecto en los servicios electrónicos y sistemas universitarios.

4.6.7 En la medida de lo posible, no deben utilizarse puertos de comunicación por defecto en aplicaciones y/o servicios electrónicos.

4.6.8 Los usuarios deben reportar al Departamento de Atención a Usuarios de la Coordinación General de Tecnologías de Información cualquier falla, error, vulnerabilidad o defecto que encuentre en aplicaciones, servicios electrónicos y/o sistemas universitarios. El Departamento de Atención a Usuarios de la Coordinación General de Tecnologías de Información debe canalizar estas situaciones a las áreas correspondientes para su debida atención.

4.6.9 Las bases de datos de información institucional sólo podrán ser accedidos por los administradores autorizados por la Coordinación General de Tecnologías de Información. Cualquier otro usuario tiene prohibido el acceso a esa información.

4.6.10 Es obligación de los administradores de servicios electrónicos y/o sistemas de información que manejan información crítica e institucional, mantener el respaldo correspondiente de la misma ya que se considera un activo de la institución que debe preservarse.

4.6.11 Se prohíbe la distribución por cualquier medio electrónico de información irrelevante, publicidad externa a las funciones universitarias y/o información basura, tanto hacia dentro de las instalaciones de la Universidad Autónoma de Chihuahua, como al exterior de la misma.

4.7 Servidores

4.7.1 Todos los servidores instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua, deberán ser administrados por personal de la misma, y sólo este administrador podrá acceder a sus recursos, o bien, autorizar a otras personas que puedan realizar tareas sobre el servidor.

4.7.2 Todos los servidores instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua, deberán mantener una bitácora de usuarios, accesos (hora y fecha de entrada, origen, hora y fecha de salida), eventos importantes. Es recomendable que dicha bitácora se registre y almacene en otro equipo. Estas bitácoras deberán ser revisadas y analizadas periódicamente por el administrador del servidor.

4.7.3 Todos los servidores instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua, deberán contar con cuentas de usuario y contraseñas fuertes, evitando utilizar la cuenta de administrador, root y/o superusuario. Todas las cuentas de usuario incluidas por defecto deben deshabilitarse.

4.7.4 Todos los servidores Microsoft Windows instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua deberán contar con un software antimalware institucional, firewall activo, actualizado y con licencia original y legal.

4.7.5 Todos los servidores instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua, deberán contar con el licenciamiento original del o los sistemas operativos y demás software instalado.

4.7.6 Todos los servidores instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua, deberán contar con los parches y actualizaciones más recientes de los sistemas operativos y demás software instalado.

4.7.7 Todos los servidores instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua deberán mantener todos sus puertos de comunicaciones cerrados a cualquier acceso, a excepción de aquellos que requiera utilizar de manera obligada para brindar los servicios para los que está destinado.

4.7.8 Se recomienda que los puertos que comunicación utilizados por los servidores, no sean los puertos por defecto que emplean en aplicaciones y software instalados.

4.7.9 Todos los administradores de servicios y/o equipos que permitan cualquier tipo de acceso a usuarios remotos deberán seguir las siguientes medidas:

4.7.9.1 Contar con capacitación adecuada para la administración del servicio y de medidas de seguridad pertinentes al uso del servicio y/o equipo, incluyendo la seguridad física.

4.7.9.2 Implementar un control de accesos al servicio y servers.

4.7.9.3 Implementar un mecanismo de actualizaciones constantes.

4.7.9.4 Realizar un monitoreo constante de los servicios y de los servidores.

4.7.9.5 Evitar uso de herramientas catalogadas como altamente vulnerables (ejemplos: Joomla, telnet, etc.).

4.7.9.6 Mantener una bitácora de eventos de manera remota.

4.7.9.7 Evitar utilizar puertos de comunicación por defecto.

4.7.9.8 Bajo ninguna circunstancia se deberá utilizar cuentas de usuario por defecto en servicios públicos y servidores de Tecnologías de Información.

4.7.9.9 Para el login de acceso a equipos y a la administración del servicio, seguir el siguiente esquema:

- *Nombre de usuario*: Al menos 8 caracteres (utilizar y combinar caracteres alfabéticos, numéricos y especiales).
- *Password:* Al menos 8 caracteres (debe ser distinto al nombre de usuario) utilizar y combinar caracteres alfabéticos, numéricos y especiales).

4.7.9.10 De ser posible, implementar un número de intentos fallidos para romper las conexiones que intentan ingresar al equipo, servicio y/o configuración.

4.7.9.11 La Coordinación General de Tecnologías de Información podrá auditar la seguridad, auditar el licenciamiento de software, auditar las bitácoras indicadas en el punto 4.7.2 y monitorear las actividades de todos los servidores instalados dentro de la infraestructura de telecomunicaciones de la Universidad Autónoma de Chihuahua, con la intención de reducir las amenazas informáticas sobre los servidores y los servicios que proporcionan.

4.8 Equipos de telecomunicaciones

4.8.1 Los equipos de telecomunicaciones de la Universidad Autónoma de Chihuahua solo pueden ser administrados por empleados de la misma cuya función lo permita. En caso de requerirse, podrá apoyarse por personal externo a la Universidad Autónoma de Chihuahua, siempre y cuando sea bajo estricta supervisión y control de las tareas a realizar por parte del administrador.

4.8.2 La instalación de cualquier equipo de telecomunicaciones debe ser autorizada por la Coordinación General de Tecnologías de Información.

4.8.3 Todos los equipos de telecomunicaciones deberán contar con control de acceso a su configuración. Las cuentas de usuario y contraseñas por defecto, deben ser deshabilitadas.

4.8.4 El software de administración de los equipos de telecomunicaciones debe contar con las actualizaciones de seguridad adecuadas.

4.8.5 Se debe contar con una bitácora de los accesos y cambios realizados en la configuración de equipos de telecomunicaciones.

4.8.6 Las interfaces, puertos y/o servicios que no se estén utilizando en los equipos de telecomunicaciones, deben estar deshabilitados.

4.8.7 Los administradores de equipos de telecomunicaciones deben tener identificada la ubicación, la configuración, los parámetros y demás componentes de dichos equipos.

4.8.8 Todo equipo de telecomunicaciones instalado dentro de la plataforma tecnológica de la Universidad Autónoma de Chihuahua, debe ser compatible con los protocolos de comunicación Ipv4 e Ipv6.

4.8.9 Todos los equipos de telecomunicaciones son sujetos a auditorías de seguridad y monitoreo por parte de la Coordinación General de Tecnologías de Información, con la finalidad de verificar el cumplimiento con los puntos pertinentes de estos Lineamientos Institucionales de Seguridad.

4.8.10 La Coordinación General de Tecnologías de Información podrá desconectar de la red universitaria, apagar y/o bloquear cualquier equipo que represente una amenaza para la integridad, confidencialidad, disponibilidad y/o rendimiento de los activos de la plataforma informática de la Universidad Autónoma de Chihuahua.

4.9 CENTROS DE CÓMPUTO

4.9.1 Todo centro de cómputo debe contar con un administrador que vigile el cumplimiento de estos lineamientos por parte de los usuarios y equipos dentro del centro de cómputo.

4.9.2 Todo centro de cómputo debe contar con políticas internas que definan el uso correcto de los equipos y software instalado, así como el uso de cualquier recurso de la plataforma tecnológica de la Universidad Autónoma de Chihuahua. Dichas políticas deben contemplar los puntos señalados en estos Lineamientos Institucionales de Seguridad.

4.9.3 El administrador del centro de cómputo debe tener un inventario actualizado del equipamiento y software instalado en dicho centro de cómputo, así como el control de la configuración, lista de usuarios, respaldos, identificación física de equipo y licenciamiento de software.

4.9.4 El uso de software y/o cualquier dispositivo conectado a la plataforma tecnológica de la Universidad Autónoma de Chihuahua, debe ser autorizado y supervisado por el administrador del centro de cómputo.

4.9.5 Sólo el administrador del centro de cómputo debe instalar software en las computadoras, realizar cualquier tarea administrativa del equipo de cómputo y/o llevar a cabo actualizaciones de hardware y software.

4.9.6 Queda prohibido el uso de sistemas de información administrativos y/o financieros universitarios en los centros de cómputo sin la supervisión estricta del administrador y/o del personal de la Coordinación General de Tecnologías de Información.

4.9.7 Queda prohibido realizar operaciones electrónicas que implique transacciones financieras en equipos del centro de cómputo.

4.9.8 Es altamente recomendable que los centros de cómputo eviten el uso de medios de almacenamiento removibles en los equipos de cómputo.

4.9.9 La Coordinación General de Tecnologías de Información podrá realizar auditorías de seguridad, auditorías de licenciamiento de software y monitoreo de tráfico con la finalidad de verificar el cumplimento de esta política de seguridad.

4.10 CONSIDERACIONES GENERALES

4.10.1 Las cuentas de usuario deben contener al menos 8 caracteres (entre alfabéticos y numéricos).

4.10.2 Las contraseñas de las cuentas de usuario deben contener al menos 8 caracteres, entre los cuales debe haber caracteres especiales (“#”, “!”, “&”, “$”, “.”, “?”, “+”, “*”), números y combinación de letras minúsculas y mayúsculas.

4.10.3 Las cuentas de usuario y contraseñas para acceder a equipos de cómputo, servicios electrónicos, sistemas de información o cualquier otro servicio, no deben estar al alcance de otras personas, ni almacenadas en otros dispositivos electrónicos. El usuario debe considerar estos datos como confidenciales.

4.10.4 Es recomendable que el usuario realice respaldos periódicos de la información que considere importante.

4.10.5 Se recomienda que el usuario cierre las sesiones de cualquier aplicación, sistema de información y/o servicio de internet (como correo electrónico, redes sociales, etc.) en el momento en que deje de utilizar dichos servicios.

4.10.6 El usuario debe bloquear con contraseña el acceso a su equipo de cómputo cuando se aleje de él. En caso de requerir alejarse de su equipo de cómputo por un período mayor a 30 minutos, deberá apagarlo completamente.

4.10.7 Es recomendable que los usuarios de otros dispositivos móviles como smartphones y/o tablets, instalen software antivirus en dichos dispositivos.

4.10.8 Solo el personal de la Coordinación General de Tecnologías de Información tiene acceso a los Sites principales de la Universidad Autónoma de Chihuahua (en el edificio de la Coordinación General de Tecnologías de Información en el Campus I, y en el Site de la Coordinación General de Tecnologías de Información en el Campus II). Ningún otro usuario podrá ingresar a ellos sin la autorización y estricta supervisión del personal de la Coordinación General de Tecnologías de Información.

4.10.9 Lo no previsto en este documento, será resuelto por el Coordinador General de Tecnologías de Información.

5.0 Medidas de contención.

Con independencia de la responsabilidad universitaria, civil o penal a que haya lugar, se podrán tomar medidas de contención que pueden llegar hasta la suspensión definitiva del servicio, dependiendo de la gravedad de la falta y de la intensión de ésta, pudiendo ser de la siguiente manera:

FALTAS NO GRAVES:

Son aquellas faltas a puntos de estos Lineamientos Institucionales de Seguridad que no representen un peligro de consideración hacia los activos críticos de la Universidad Autónoma de Chihuahua o de otras organizaciones. Las medidas de contención a este tipo de faltas pueden incluir las siguientes acciones:

- Reporte mediante oficio al infractor.
- Reporte mediante oficio al jefe inmediato, coordinador administrativo o coordinador académico, según corresponda.
- Suspensión temporal de los servicios de la plataforma tecnológica de la Universidad Autónoma de Chihuahua.

FALTAS GRAVES:

Son aquellas faltas que atenten contra la integridad, confidencialidad y/o disponibilidad de los activos críticos de la Universidad Autónoma de Chihuahua o de otras organizaciones, de manera intencional. Las medidas de contención a estas faltas pueden incluir las siguientes acciones:

- Reporte mediante oficio al infractor.
- Reporte mediante oficio al jefe inmediato, coordinador administrativo o coordinador académico, según corresponda.
- Reporte mediante oficio al Director de la unidad académica, Director de Área o Coordinador General, según corresponda.
- Reporte mediante oficio al Departamento de Recursos Humanos de la Universidad Autónoma de Chihuahua.
- Reporte mediante oficio al Despacho del Abogado General de la Universidad Autónoma de Chihuahua.
- Suspensión indefinida de los servicios de la plataforma tecnológica de la Universidad Autónoma de Chihuahua.