POLÍTICAS DE SERVICIO

I. ÁREA

Coordinación de Seguridad en Cómputo

II. DESCRIPCIÓN

Área que proporciona servicios de seguridad informática a la red Universitaria Institucional, implementando medidas de seguridad y acciones orientadas hacia la eliminación de vulnerabilidades informáticas, teniendo en la mira evitar que una amenaza se vuelva realidad.

III. DEFINICIÓN DE TÉRMINOS

Antivirus	Conjunto de programas avanzados que no sólo buscan detectar un virus informático, sino bloquearlo, desinfectar y prevenir una infección de los mismos, y actualmente son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.
SNMP:	Protocolo de administración de equipos de comunicaciones.
Firewall:	Equipo de seguridad utilizado en redes de computadoras para controlar las comunicaciones, para disminuir el riesgo de un incidente de seguridad informático.
Firewall de host:	Conjunto de programas que implementan control de entrada/salida de direcciones de puertos para evitar accesos no autorizados, configurados para permitir, negar o limitar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas definidas por el administrador del programa.
Iptables:	Herramienta de los equipos con SO Linux que permite interceptar y manipular paquetes de red, con lo que se puede implementar un firewall.

IV. SERVICIOS PROVISTOS

Generalidades:

- Estos servicios aplican solamente en estaciones de trabajo, servidores y laptops propiedad de la UACh.
- Para la instalación de software se requiere que el equipo cuente con todos los parches del sistema operativo (service packs) y actualizaciones críticas.
- Todos los equipos propiedad de la UACh que estén conectados a la red Universitaria estarán protegidos de ataques externos por medio de la implementación de seguridad perimetral, para reforzar esta protección, es necesario que sea instalada

una solución de Anti-Virus informáticos en los equipos con sistema operativo Microsoft Windows, para ello se realiza una evaluación de las diferentes soluciones en el mercado, adquiriendose la que mejor se adapte a las necesidades de la UACh, por lo que su instalación no es opcional y no se deberá de desinstalar de los equipos institucionales.

Antivirus Institucional (AVI).
Instalación del programa para la prevención y/o eliminación de virus informáticos.

a) Instalación y configuración de servidor secundario del AVI para actualización de manera local en áreas donde la velocidad de conexión esta limitado ó la cantidad de actualizaciones es excesiva.
Tiempo de respuesta: 5 días laborales a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.

b) Solución a fallas de la instalación y actualización del AVI, servicio proporcionado como soporte usuarios, se revisa por comportamiento anómalo del software.
Tiempo de respuesta: 3 días hábiles a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.

c) Instalación del AVI en estaciones de trabajo o laptops, servicio realizado por personal del DAU, cuando es detectado un equipo que no cuenta con el antivirus institucional.
Tiempo de respuesta: 2 días hábiles.

d) Desinfección de equipos de cómputo, servicio realizado por personal del DAU referente a la solución de problemas ocasionados por virus en los equipos de cómputo.
Tiempo de respuesta: 2 días hábiles.

Seguridad Perimetral.
Es necesario la utilización de un esquema para restringir en acceso entre el exterior (red publica) y la red de la Universidad, se implementa un esquema de control de acceso desde y hacia Internet, esto es utilizando una solución basada en dispositivos de seguridad (firewalls, Proxys, ACL's, etc.) los cuales se encargan de evitar los accesos no autorizados.

a) Soporte de Seguridad Perimetral. Dar solución a problemas de conectividad entre la red de la UACh y la red externa. Los problemas mas comunes en esta categoría son:

- Problemas de conexión hacia un sitio en Internet.
- Bloquear una dirección o puerto siempre y cuando este constituya una amenaza de seguridad informática.

Tiempo de respuesta: 5 días hábiles a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.

b) Liberación de equipos del firewall, debido a ciertas operaciones es necesario que los equipos sean permitidos para accesar directamente a Internet, por lo que es necesaria la configuración en los equipos de seguridad perimetral para este efecto. En la solicitud se deberá indicar la ubicación física,la aplicación que se va a utilizar la dirección IP del equipo origen, la dirección destino a donde se requiere liberar, los puertos TCP/UDP que van a ser utilizados, asi como su uso. Esta información deberá de ser obtenida por el solicitante y/o responsable de cómputo. Cuando se desconose alguno de estos datos ó trate de la liberacion de un rango amplio de dirrecciones debera de ser acompañada de un oficio responsivo por parte del director de la UA donde se debe justificar el porqué de su liberación.

Los requisitos para la liberación de equipos son:

- El sistema operativo deberá de estar actualizado con todos los parches de seguridad al día de la solicitud.
- El Sistema operativo deberá de contar con mecanismos de autenticación nativos y en operación, utilizando esquemas robustos de contraseña.
- El equipo deberá de tener instalado y configurado un firewall de host que permita el control de puertos de entrada/salida.
- Si se trata de equipos son sistema operativo de Microsoft, deberá de estar instalado y en operación el AVI.

Tiempo de respuesta: 5 días hábiles a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.

<u>Servicios generales de seguridad en cómputo.</u>
Implementación de soluciones que proporcionen un ambiente seguro para el uso de las Tecnologías de Información.

a) Implementación de medidas de seguridad en cómputo, establecer mecanismos para la protección de los equipos de cómputo
Tiempo de respuesta: 8 días hábiles a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.

b) Respuesta de incidentes de seguridad en cómputo, dar solución y seguimiento a problemas de seguridad en cómputo propiedad de la UACh. Este servicio puede ser originado por:

- Accesos no autorizados vía electrónica a equipos conectados a la red de la UACh.
- Propagación masiva de virus en equipos de la red la UACh.
- Amenazas de posibles atentados en equipos e información de la UACh que pongan en peligro la Disponibilidad, Integridad ó Confidencialidad.

Tiempo de respuesta: 8 días hábiles a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.

V. SERVICIOS EXCLUIDOS

Servicios no proporcionados por el área:

- La instalación del Sistema Operativo, los service packs (de acuerdo con lo publicado por el fabricante) y actualizaciones críticas en el equipo del usuario solicitante de un servicio de liberación de equipo del firewall.
- Equipos con SO Windows 95, 98, ME y XP home no serán liberados del firewall, debido a que no cuentan con esquemas de seguridad nativos del SO.
- La instalación de un firewall de host en equipos con SO Windows XP pro, cuando se solicite la liberación del equipo de la seguridad perimetral.
- La configuración de equipos con SO Unix, es necesario la eliminación de puertos no utilizados y el uso de iptables, lo cual será responsabilidad del usuario solicitante del servicio de seguridad perimetral.
- La dirección IP y los puertos de origen/destino, para la liberación de equipos del firewall.

VI. INCIDENTES CRÍTICOS

En caso de que se presente una incidencia de virus que no sea detectada por la solución actual de AVI, se procederá a recolectar una copia del archivo infectado, el cual se enviará por los medios adecuados al fabricante de la solución para que sea incluida en su lista de definiciones.

El tiempo de respuesta se encuentra dado por el fabricante sin embargo se dará respuesta en 48 horas hábiles para la implementación.

Sin embargo se realizarán acciones pertinentes como el bloqueo de puertos y direcciones en los equipos de frontera, para evitar las propagaciones hacia y desde Internet.

VII . MÉTRICAS DEL SERVICIO

- Se medirá el número de solicitudes atendidas en tiempo y forma; se contempla una meta > 85% mensual.
- Se medirá la disponibilidad de los servicios mediante el monitoreo de los servidores, el cual será obtenido mediante la interrogación del sistema con SNMP, con una meta > 85%:
    - Servidor de Antivirus Institucional (avi.uach.mx)
    - Servidor de licencias de Windows Vista (kms.uach.mx)
    - Servidor de windows update (wsus.uach.mx)
    - Firewalls.
    - Proxy's
    - Equipos de comunicaciones de frontera.