I. ÁREA

Coordinación de Seguridad en Cómputo

II. DESCRIPCIÓN

La Coordinación de Seguridad en Cómputo es la responsable de implementar y mantener funcionando correctamente la infraestructura de seguridad informática de la Universidad Autónoma de Chihuahua, así como la administración de la red WAN universitaria.

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.
Carrier	Proveedor de servicios de voz, video y datos.
Conectividad	Conexión a la red de datos de la UACH.
Disponibilidad	Porcentaje de tiempo en que un equipo permanece conectado a la red de datos de la UACH.
DNS	Servicio de resolución de nombres, utilizado para acceso a equipos y sitios de internet.
Filtrado de paquetes	La acción de filtrar paquetes es bloquear o permitir el paso a los paquetes de datos de forma selectiva, según van llegando a una interfaz de red.
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 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.
Latencia	Tiempo promedio que tarda un paquete de datos en ir y regresar desde una computadora o equipo origen hacia otra computadora o equipo destino.
Mbps	Megabits por segundo.
Proxy	Servicio de administración y control de los accesos a Internet, el cual es usado por todos los equipos de la UACh que utilizan el servicio de navegación a Internet.
SNMP:	Protocolo de administración de equipos de comunicaciones.
WAN	Término que define a un tipo de red cuya cobertura se extiende por varias poblaciones. Se entiende por WAN a la interconexión de varias redes locales dispersas geográficamente, y que pertenecen a una misma organización.

IV. SERVICIOS PROVISTOS

Servicio de Vigilancia de Conectividad a la Red

Es un mecanismo de control para detectar y solucionar problemas; para conocer el estado de los equipos de telecomunicaciones, el tiempo de respuesta y de disponibilidad.

- Este servicio será proporcionado únicamente para el personal de la Coordinación de Tecnologías de Información.
- El equipo (s) que se requiere monitorear debe ser relevante dentro el funcionamiento de la red universitaria
    - Servidores de Sistemas Universitarios.
    - Servidores de Correo, proxy, DNS, Internet, etc.
    - Equipos de telecomunicaciones del Backbone de la red

- El solicitante debe apegarse a las cláusulas del Acuerdo de Servicio de Vigilancia de Conectividad a la Red (**DOC 7.2 CSC 07**) que se encuentra publicado en el Sistema UNIQ **http://uniq.uach.mx.**

- El tiempo de respuesta es de 32 horas hábiles

Servicio de Atención a Fallas de enlaces e Internet

Se refiere a la solución de problemas relacionados con fallas de conectividad hacia las diferentes dependencias universitarias. Así como las fallas relacionadas con el servicio de Internet.

- El tiempo de respuesta para este servicio es de 32 horas hábiles.
- Este servicio será proporcionado a toda la comunidad universitaria.

Servicio de Antivirus Institucional

Instalación del programa para la prevención y/o eliminación de virus informáticos.
Este servicio abarca las siguientes categorías:

- **Instalación y configuración de servidor secundario del AVI**, para actualización de manera local en áreas donde la velocidad de conexión está limitado o la cantidad de actualizaciones es excesiva.
  - El tiempo de respuesta es de 40 horas hábiles, a partir de que se escala la solicitud de servicio a la CSC en el SGAU´s.
  - Este servicio será proporcionado para los responsables de cómputo de las diferentes unidades académicas.

- **Solución a fallas de la instalación y actualización del AVI**, servicio proporcionado como soporte a usuarios, se revisa por comportamiento anómalo del software.
  - El tiempo de respuesta es de 24 horas hábiles, a partir de que se escala la solicitud de servicio a la CSC en el SGAU´s.
  - Este servicio será proporcionado para los responsables de cómputo de las diferentes unidades académicas.

- **Instalación del AVI en estaciones de trabajo o laptops,** cuando es detectado un equipo que no cuenta con el antivirus institucional.
  - El tiempo de respuesta es de 16 horas hábiles
  - Este servicio será proporcionado para usuarios de unidad central

- **Desinfección de equipos de cómputo**, referente a la solución de problemas ocasionados por virus en los equipos de cómputo.
  - Tiempo de respuesta: 16 horas. hábiles.
  - Este servicio será proporcionado para usuarios de unidad central

Servicio de Seguridad Perimetral.

Es necesario la utilización de un esquema para restringir el acceso entre el exterior (red pública) 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.
Este servicio abarca las siguientes categorías:

- **Soporte de Seguridad Perimetral,** para dar solución a problemas de conectividad entre la red de la UACh y la red externa. Los problemas más 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.

    - El tiempo de respuesta es de 40 horas. hábiles, a partir de que se escala la solicitud de servicio a la CSC en el SGAU´s.
    - Este servicio será proporcionado para usuarios de estaciones de trabajo y laptops propiedad de la UACh.

- **Red Privada Virtual (VPN),** debido a que es necesario acceder a equipos de la red universitaria desde Internet, es necesario ofrecer un servicio de conexión a través de un esquema seguro.

    - El tiempo de respuesta es de 40 horas hábiles
    - Este servicio será proporcionado a el personal administrativo y docente, escuelas incorporadas a la UACh, dependencias de la UACh y eventos especiales donde se requiera.

- **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: 40 hrs. hábiles a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.
- Este servicio será proporcionado para los responsables de cómputo de las diferentes unidades académicas.

Servicios generales de seguridad en cómputo.

Implementación de soluciones que proporcionen un ambiente seguro para el uso de las Tecnologías de Información. Así como la asignación de direccionamiento IP para equipos de la red UACh.
Este servicio abarca las siguientes categorías:

- **Implementación de medidas de seguridad en cómputo**, establecer mecanismos para la protección de los equipos de cómputo.
  - El tiempo de respuesta es de 64 horas hábiles, a partir de que se escala la solicitud de servicio a la CSC en el SGAU´s.
  - Este servicio será proporcionado para toda la comunidad universitaria.
- **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 o Confidencialidad.
  - Tiempo de respuesta: 64 horas hábiles a partir de que se escala la solicitud de servicio a la CSC en el SGAU's.
  - Este servicio será proporcionado para toda la comunidad universitaria.
- **Direccionamiento IP**
  Consiste en la asignación de direcciones IP para equipos de la red UACH (148.229.0.0).
  - Este servicio será proporcionado a toda la comunidad universitaria.
  - El tiempo de respuesta es de 32 horas hábiles
  -

Generalidades:

- *Todos los servicios de seguridad aplican solamente a estaciones de trabajo, servidores y laptops propiedad de la UACh.*
- *Para instalación de software se requiere que el equipo cuente con todos los parches del sistema operativo (service pack) y actualizaciones criticas.*
- 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, adquiriéndose 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.

V. SERVICIOS EXCLUIDOS

Atención de fallas en los siguientes casos:

- La instalación del Sistema Operativo, service packs 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.
- Fallas de energía eléctrica.
- Falla de red o de acceso a Internet en una sola computadora.
- Fallas en el DNS, páginas web, correo electrónico, plataforma de educación virtual, checador, cajas únicas y en general, cualquier servicio electrónico ó sistema universitario.
- Configuración presencial del direccionamiento IP en computadoras y servidores.

VI. INCIDENTES CRITICOS

1.- Fallas de conectividad hacia:

Toda la red universitaria

Rectoría (Debido a los sistemas universitarios se resguardan en ese sitio)

Todo el campus nuevo (Debido a la gran cantidad de usuarios afectados)

Todo el campus I (Debido a la gran cantidad de usuarios afectados)

** El tiempo para iniciar la corrección de la falla después de detectarla es de 1 hora.
** El tiempo de resolución es de 4 horas.

2.- Fallas del servicio de Internet Empresarial

** El tiempo para iniciar la corrección de la falla después de detectarla es de 30 minutos.
** El tiempo de resolución es de 4 horas en aspectos que la CSC controle directamente. En caso de que la falla sea atribuible al proveedor del servicio, éste definirá el tiempo de restablecimiento.

3.- Incidencia de Virus

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

Los resultados de la evaluación de servicios y respuesta oportuna a solicitudes de servicio deberán cumplir con lo definido en las políticas, objetivos e indicadores generales de la CGTI