ACUERDO DE SERVICIO SEGURIDAD PERIMETRAL

1. **NOMBRE DEL SERVICIO**
   Seguridad perimetral (firewall).

2. **DESCRIPCIÓN DEL SERVICIO**
   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, la Coordinación de Seguridad en Cómputo (CSC) implementa un esquema de control de acceso desde y hacia Internet, esto es utilizando una solución basada en equipos conocidos como firewall los cuales se encargan de evitar los accesos no autorizados.

3. **COSTOS**
   No aplica.

4. **SERVICIOS PROVISTOS**
   Liberación del equipo de firewall
   Todos los equipos de la Red Universitaria se encuentran protegidos por esta solución, la cuál se complementa con el software de antivirus institucional (AVI) instalado en cada equipo de cómputo (estación de trabajo o servidor) propiedad de la UACh y que se encuentre conectado a la Red Universitaria.

   En dado caso de que se requiera que un equipo no esté protegido por el esquema de protección perimetral (firewall), es necesario realizar una solicitud expresa, el trámite será el siguiente:
   - La solicitud se realiza por medio del DAU, el cuál dirigirá la solicitud al CGE, indicando la razón por la cuál se requiere que el equipo esté fuera del firewall; la aplicación y los puertos hacia donde se va a realizar la comunicación, la cuál será tramitada como un servicio nuevo y requerirá de su aprobación por parte del CGE.
   - Una vez aprobada la solicitud, será necesario realizar una auditoría de seguridad por parte de la CSC, 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 de la configuración del proxy para navegar en internet.
   - Los equipos a ser expuestos fuera del firewall, deberan de cumplir con los siguientes requisitos mínimos:

     1. Proporcionar nombre del equipo y persona a cargo del equipo.
     2. El Sistema Operativo, deberá de tener instalados los service packs (de acuerdo con lo publicado por el fabricante) y actualizaciones críticas.
     3. 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.
     4. En equipos con SO Windows NT, 2000 y XP, es necesario la utilización de un firewall de host (ver recomendación por la CSC, en la liga: http://antivirus1.uach.mx/soporte/) que debrá estar activo y debidamente configurado.

5. En equipos con SO Unix, es necesario la eliminación de puertos no utilizados y el uso de iptables.
6. El equipo deberá contar con la protección del AVI, el cuál deberá de estar propiamente instalado y actualizado.

- A equipos que hayan sido liberados del firewall la CSC programará una auditoría de seguridad cada tres meses. Salvo en caso de una falla de seguridad del fabricante del SO, lo que ocasionará que el equipo quede protegido por el firewall, por lo cuál el responsable del equipo deberá de actualizar el sistema operativo y avisar a CSC para programar una auditoría, con la que nuevamente podrá liberar el equipo del firewall.

- El resultado de la auditoría se le notificará al solicitante, en caso de que el resultado sea satisfactorio, el equipo será liberado del firewall; en caso que no se cumplan los requisitos, el responsable del equipo será quién se encargue de la instalación y puesta a punto; se reprogramará una nueva auditoría de seguridad.

5. PRIORIDADES DE LLAMADOS

La prioridad de atención a este servicio es igual para todos sin importar el tipo de usuario.
Es considerado como nuevo servicio, por lo que requiere de autorización por parte del CGE, una vez autorizado, la CSC programa la auditoría de seguridad, la cuál tendrá como tiempo de respuesta máximo 5 días hábiles con jornada laboral de 8 horas, una vez completada la auditoría, el resultado se le dará a conocer al usuario, en caso de que el resultado sea satisfactorio, el equipo será liberado del firewall con tiempo de respuesta de 3 dias hábiles; en caso que no se cumplan los requisitos, el responsable del equipo será quién se encargue de la instalación y puesta a punto del equipo, por lo que se reprogramará una nueva auditoría de seguridad.

6. ALCANCE DEL SERVICIO

El nivel que ofrece la CSC al usuario es de tercer nivel, y el horario de servicio será de Lunes a Viernes en el horario de 8:00 am a 4:00 pm. El tiempo de respuesta es variable de acuerdo a la carga de trabajo, el tiempo mínimo de respuesta es de 1 día hábil y un máximo de 8 días hábiles.

7. REPORTES DEL SERVICIO

Número de solicitudes atendidas. (SGAUS)
Formato de auditoría de seguridad FOR 7.5 CSC 06.

8. PROCEDIMIENTO DE ESCALAMIENTO

Para aquellas solicitudes de servicio que hayan excedido el tiempo de respuesta se deberán escalar para el registro correspondiente y solución inmediata:

1. JDAU
2. CGE

9. RESPONSABILIDADES Y LÍMITES

- **DAU:**
  - Registrar las solicitudes de servicio en el SGAU's según lo indica el procedimiento de atención a usuarios.
  - Informar al usuario el status de sus solicitudes de servicio.
  - Verificar con el usuario el cierre de la solicitud de servicio en el SGAU's.

- **CGE**:
  - Recibe la solicitud y el oficio de solicitud de liberación por parte del jefe de departamento o director de área y autoriza o rechaza la solicitud, en caso de ser rechazada se le notifica al DAU para que sea notificado el usuario; en caso de ser aprobada la solicitud se transfiere a la CSC.

- **CSC**:
  - Recibe la solicitud autorizada, se pone en contacto con el usuario para la programación de la auditoría de seguridad.
  - Notifica al usuario del resultado de la auditoría, si cumple con los requisitos mínimos para la liberación del equipo del esquema de protección de seguridad perimetral, procede a la configuración del firewall. En caso que no se cumplan con los requisitos, se informa al usuario, por lo que se reprogramará una nueva auditoría de seguridad.

- **Usuario:**
  - Dirigir las solicitudes de servicio directamente al personal de Helpdesk del Departamento de Atención a Usuarios.
  - Presentar un oficio por parte del jefe de departamento o director de área, dando a conocer los motivos de la solicitud dirigida al CGE.
  - Describir la petición lo más claro posible describiendo todos los datos solicitados por Helpdesk.
  - Verificar que la atención a su solicitud sea de su completa satisfacción y firmar la solicitud de servicio.
  - Es responsabilidad del usuario la puesta a punto del equipo de cómputo en cuanto a parches y actualizaciones críticas del S.O. así como la actualización del AVI y configuración del firewall de host, en caso de que el usuario no esté capacitado/habilitado para ello, deberá de generar una solicitud al DAU.