ACUERDOS Y POLITICAS DEL SERVICIO DE SEGURIDAD INFORMATICA

1.0 Propósito y alcance

1.1 **Propósito.** Definir las políticas y los acuerdos de nivel de servicio que norman la prestación del servicio de Seguridad Informática para los usuarios de la Universidad Autónoma de Chihuahua (UACH) y que lleva a cabo la Coordinación General de Tecnologías de Información (CGTI).

1.2 **Alcance.** Las políticas y acuerdos del presente instrumento aplican para otorgar el servicio de Seguridad Informática a maestros, empleados universitarios y usuarios externos que tengan alguna función específica que requiera conexión hacia la red universitaria, el cual proporciona el Equipo de Respuesta a Incidentes Informáticos (CERT-UACH) de la CGTI.

2.0 Acuerdos y políticas

2.1 Generales

2.1.1 Con objeto de poder garantizar la atención conforme a los acuerdos y políticas de los servicios que proporciona la CGTI, la Mesa de Servicios será el único punto de contacto mediante el cual los usuarios podrán solicitar el servicio, reportar fallas, quejas y/o sugerencias en el mismo.

2.1.2 De otra manera, cualquier solicitud y/o reporte de falla no realizada a través de la Mesa de Servicios no tiene garantía de cumplimiento en las formas y términos definidos en el presente documento.

2.1.3 A toda solicitud de servicio se le asignará un numero de identificador único, el cual se le proporcionará al usuario para su posterior seguimiento.

2.1.4 El usuario y/o los involucrados podrán en todo momento consultar el estado que guarda una solicitud accediendo a la dirección electrónica https://dau.UACH.mx/ con el usuario y contraseña de su cuenta de correo institucional de la UACH.

2.1.5 El CERT-UACH es la única área encargada de autorizar conexiones desde Internet hacia equipos y servicios dentro de la red universitaria.

2.1.6 Solo empleados de la UACH podrán solicitar el servicio de seguridad informática, teniendo que proporcionar su número de empleado al momento de levantar una solicitud a la mesa de servicios.

2.1.7 El CERT-UACH podrá hacer uso de servicios externos si así lo considera pertinente.

2.1.8 El CERT-UACH no garantiza la recuperación sobre daños en información sin respaldo.

2.1.9 El CERT-UACH podrá dar a conocer ciertos detalles acerca de incidentes informáticos como parte de acuerdos de colaboración que se tengan con otras instancias, cuidando siempre la identidad de administradores y/o usuarios afectados.

2.1.10 Bajo ninguna circunstancia se liberarán equipos de las reglas de seguridad perimetral de manera completa (todos los puertos de comunicación).

2.1.11 El servicio no tiene costo directo para el usuario.

2.1.12 La vigencia de los acuerdos y políticas contenidas en el presente documento deberán ser revisadas y en su caso renovado al menos cada doce meses.

2.2 Canales de atención.

2.2.1 El servicio podrá ser solicitado a través de los canales de atención de la Mesa de Servicios autorizados y vigentes.

2.2.2 La atención telefónica y en ventanilla solo estará disponible en los horarios de atención de la Mesa de Servicios.

2.2.3 En el caso de registrarse una solicitud por medios no presenciales o telefónicos y fuera del horario de atención de la Mesa de Servicios, la solicitud de servicio será atendida al siguiente día hábil, a partir del cual iniciaran los tiempos para el cumplimiento de los acuerdos del servicio.

2.3 Usuarios y/o solicitantes.

2.3.1 El servicio se proporciona solo a personal docente y administrativo de la UACH, quienes deberán acreditarse como usuario mediante su número de empleado y su cuenta de correo electrónico institucional de la UACH o bien con el documento que lo acredite como tal.

2.3.2 Cualquier otro usuario de la UACH que no sea personal docente o administrativo de la UACH deberá solicitar este tipo de servicio a la unidad técnica de soporte o administrativa correspondiente a la dependencia universitaria a la que pertenezca.

2.4 Propietario del servicio

El dueño o propietario de la prestación de este servicio es el Jefe del CERT-UACH.

2.5 Tipos de solicitudes

El usuario podrá realizar los siguientes tipos de solicitudes de este servicio:

2.5.1 Atención a incidentes de seguridad informática: Reporte de incidentes relacionados a:

- Virus informáticos
- Phishing
- Robo de contraseñas
- Ataques a sitios web y/o servicios universitarios
- Accesos no autorizados a equipos de cómputo

2.5.2 VPN-UACH: Solicitud de conexión desde Internet hacia la red UACH mediante un túnel de red privada virtual.

2.5.3 Seguridad perimetral: Solicitud de liberación de políticas de seguridad perimetral de equipos de cómputo y/o servicios electrónicos. Esta liberación puede ser de dos tipos:

- De salida. Cuando un equipo requiere navegar ó acceder a servicios de Internet sin utilizar los proxies de la UACH.

- De entrada. Cuando algún servicio instalado en un equipo deba ser utilizado desde Internet (fuera de la red universitaria). Debe especificarse el puerto de comunicación necesario.

2.5.4 Felicitación, información, aclaración de dudas y/o procedimientos, queja y/o sugerencia: Cualquier felicitación, duda, y/o sugerencia relacionada con el servicio recibido.

2.6 Solicitudes de servicio

2.6.1 Al momento de solicitar el servicio, el usuario deberá proporcionar su número de empleado.

2.6.2 Una vez atendida y/o resuelta la solicitud de servicio, se deberá registrar el cierre de la misma conforme al proceso, y al acuerdo y políticas de la Mesa de Servicios.

2.6.3 El seguimiento y notificaciones de las solicitudes de servicio se llevaran a cabo conforme a los acuerdos y políticas de la Mesa de Servicios.

2.7 Tiempo de respuesta del servicio

2.7.1 El horario de servicio será de 8:00 a 15:00 horas de lunes a viernes.

2.7.2 El tiempo de respuesta a cada solicitud de servicio será en un máximo de 24 horas hábiles a partir de la fecha y hora de recepción y en base al horario de servicio.

2.7.3 El tiempo para escalar la solicitud de servicio a un analista de segundo nivel es de máximo 4 horas hábiles posteriores al registro de la solicitud.

2.8 Escalamientos de quejas en el servicio

En el caso de quejas en la atención del servicio o por el no cumplimiento del presente acuerdo y políticas del servicio, el usuario podrá solicitar el escalamiento de su solicitud al Gestor de la Mesa de Servicios, de no recibir una respuesta satisfactoria podrá también solicitar escalar la solicitud al Coordinador de la CGTI.

3.0 Manejo de excepciones

3.1 Desastres, Urgencias o Solicitudes con Prioridad Crítica: En caso de que se presente una situación de extrema contingencia el Jefe del CERT-UACH consultará y acordará con el Coordinador de la CGTI el proceso alternativo a seguir para dar atención a la solicitud de servicio.

3.2 Contingencia o falla de la aplicación de la Mesa de Servicios: En caso de presentarse una falla en el sistema que soporta la operación de la Mesa de servicios, se podrán utilizar los canales de atención alternos y/o llenar de manera manual el formato de solicitud de servicio; una vez restaurada la funcionalidad del sistema todas las solicitudes recibidas durante el periodo de falla deberán ser registradas junto con su respectivo cierre correspondiente.

3.3 Solicitudes de servicio no resueltas: En el caso de solicitudes no resueltas conforme a los acuerdos y políticas del servicio, el usuario además de poder solicitar el registro de una queja, podrá solicitar al Gestor de la Mesa de Servicios en coordinación con el Jefe del CERT-UACH la resolución de la solicitud brindando una solución alternativa temporal o definitiva.

4.0 Responsabilidades

4.1 Del Usuario

4.1.1 Hacer un uso adecuado de los recursos tecnológicos.

4.1.2 Mantener un respaldo de información que almacena en equipos bajo su responsabilidad.

4.1.3 Seguir las siguientes recomendaciones:

- Utilizar nombre de usuario y password en equipos de cómputo y administración y/o uso de servicios electrónicos.
- Contar con el antivirus institucional vigente y actualizado instalado en equipos de cómputo con sistemas operativos Windows.
- Contar con las últimas actualizaciones del sistema operativo.
- Mantener bitácoras de acceso al equipo de cómputo y/o servicios electrónicos.
- En el caso de administradores de servicios electrónicos, contar con capacitación adecuada para la administración de servicios y medidas de seguridad pertinentes.

4.1.4 Reportar a la Mesa de Servicios cualquier anomalía en la prestación del servicio.

4.1.5 Conocer y adherirse a los presentes Acuerdos y Políticas.

4.1.6 Tener un conocimiento básico de los servicios de Tecnologías de Información de los cuales hace uso.

4.1.7 Proporcionar una descripción clara de la situación que requiera reportar.

4.1.8 Colaborar con el personal de la Mesa de Servicios y los analistas de segundo nivel para la atención de su solicitud.

4.1.9 Disponibilidad para que el personal de la CGTI tenga acceso al equipo, instalaciones, sistemas o servicio que este siendo reportado cuando así se requiera.

4.1.10 En el caso de las solicitudes del tipo Atención a Incidentes de Seguridad Informática el usuario también deberá cumplir con los siguientes requisitos:

4.1.10.1 Solo se atenderán casos sobre servicios electrónicos y/o de información de la UACH.

4.1.10.2 Solo se atenderán casos sobre equipos de cómputo propiedad de la UACH.

4.1.10.3 El usuario afectado deberá proporcionar toda la información requerida por el CERT-UACH, así como colaborar de manera activa en la atención del incidente en caso de ser necesario.

4.1.11 En el caso de las solicitudes del tipo VPN-UACH el usuario también deberá cumplir con los siguientes requisitos:

4.1.11.1 Solo se atenderán reportes de usuarios de la UACH.

4.1.11.2 El servicio de VPN-UACH solo se otorgará para funciones administrativas ó académicas.

4.1.11.3 El solicitante será responsable del uso de la conexión por VPN hacia la red universitaria.

4.1.11.4 El equipo de cómputo donde se instale el cliente VPN deberá contar con lo siguiente:

- Contar con un firewall de host.
- Las más recientes actualizaciones del sistema operativo.
- Nunca deberá compartir el servicio de conexión de Internet con otros equipos y/o usuarios.

4.1.11.5 El uso del servicio de VPN-UACH es personal, por lo que la cuenta de conexión no podrá pasarse a otro usuario.

4.1.11.6 El solicitante deberá indicar la vigencia de la cuenta de VPN que solicita.

4.1.12 En el caso de las solicitudes del tipo seguridad perimetral el usuario también deberá cumplir con los siguientes requisitos:

4.1.12.1 La liberación de equipos de salida debe ser solicitada por un jefe de departamento ó director de unidad académica ó área mediante una solicitud en la Mesa de Servicios. Esta persona será el responsable del uso del equipo liberado, y el uso del servicio de Internet deberá apegarse a fines estrictamente laborales y/o académicos.

4.1.12.2 La liberación de entrada de un equipo debe responder a una necesidad administrativa y/o académica de un grupo de usuarios internos y/o externos.

4.1.12.3 La liberación de equipos de entrada debe ser solicitada a la Mesa de Servicios y además el director de la unidad académica o área deberá realizar una solicitud mediante un oficio dirigido al Jefe del CERT-UACH indicando lo siguiente:

Datos del equipo

- Tipo de Equipo (server, PC, Laptop, etc.)
- Dirección IP
- Dirección MAC
- Ubicación física
- Sistema Operativo
- Cuenta con AVI (cuál)
- Cuenta con Firewall activo y configurado (cuál)
- Cuenta con un registro de eventos

Datos del servicio

- Descripción del Servicio
- Puertos de comunicación solicitados
- Justificación de la liberación
- Quienes pueden acceder al servicio
- Descripción de las medidas de seguridad implementadas.

Datos del administrador del equipo y del servicio

- Nombre
- Puesto
- Correo electrónico
- Teléfono oficina
- Teléfono celular
- Con cual capacitación cuenta para la administración del servicio

Con la información entregada en este oficio, el CERT-UACH hará un análisis para aceptar ó rechazar dicha solicitud.

4.1.12.4 El administrador del equipo y/o servicio se compromete a:

- Mantener las actualizaciones de software requeridas.
- Mantener el acceso restringido al equipo, configuraciones, administración del servicio, etc.
- Verificar de manera periódica los eventos del equipo y del servicio.
- Mantener un programa de respaldo de información periódico relacionado con el equipo y servicio a liberar.
- Mantener y verificar periódicamente un registro de:
  + Quién accede
  + De donde accede
  + Cuando accede
  + Cuando se desconecta

4.1.12.5 Todos los equipos liberados de las políticas de seguridad perimetral están sujetos a auditorías de seguridad que pueden consistir en:

- Análisis de vulnerabilidades
- Revisión de bitácoras de eventos
- Revisión de actualizaciones, AVI y Firewall
- Revisión de accesos
- Revisión de respaldos de información

4.1.13 Responder la encuesta de satisfacción cuando se le solicite.

4.2 Analistas de primer nivel

4.2.1 Recibir, registrar y dar seguimiento hasta su consecución de la solicitud de servicio.

4.2.2 Informar los acuerdos y políticas del servicio y el estado de las solicitudes de registradas.

4.2.3 Aplicar encuestas de satisfacción cuando se requiera.

4.3 Del CERT-UACH

4.3.1 Proporcionar el servicio de Seguridad Informática dentro de los términos descritos en esta política de servicio.
4.3.2 Atender dentro de los tiempos descritos las solicitudes de los usuarios.

5.0 Restricciones (exclusiones) para el usuario

5.1 Cuando existan fallas de conexión de red local o red WAN.
5.2 Cuando existan fallas de energía eléctrica.
5.3 Cuando se lleven a cabo tareas de mantenimiento preventivo y/o correctivo, actualizaciones de hardware y/o software.
5.4 Fallas del proveedor del servicio de Internet (Transtelco, Telmex, Cablemas, etc.).
5.5 Equipos con recursos insuficientes de memoria, disco duro y/o procesador.
5.6 Equipos que no cuenten con el antivirus institucional.
5.7 Equipos que no cuenten con las últimas actualizaciones del sistema operativo.
5.8 Equipos y/o servicios ajenos a la UACH.
5.9 Falta de información o colaboración del usuario.
5.10 Solicitudes de personal no considerado usuario del servicio.
5.11 Solicitudes rechazadas con anterioridad.

6.0 Referencias

6.1 Procedimiento de Atención a Incidentes de Seguridad Informática.

7.0 Formatos

7.1 Registro de VPN-UACH
7.2 Formato de Atención de Fallas
7.3 Registro de Liberación de Equipos
7.4 Registro de Incidentes Informáticos

8.0 Vigencia

Del: 01 de Octubre del 2013
Al: 30 de Septiembre del 2014