

Código: PRO 7.5 CERT 01	Página 1 de 3
Fecha de emisión:08/11/2013	Fecha de Revisión:08/11/2013 Número de Revisión:1
Elaboró: Jefe del CERT-UACH	
Aprobado por: Coordinador General	

PROCEDIMIENTO DE ATENCIÓN A INCIDENTES DE SEGURIDAD INFORMÁTICA

1.0 Propósito Y Alcance.

1.1 Propósito

Proporcionar a la comunidad universitaria una respuesta oportuna y efectiva a situaciones en donde se ha comprometido la seguridad de la plataforma de TI.

1.2 Alcance

Este procedimiento aplica a todos los equipos de cómputo y servicios públicos que son propiedad de la UACH.

2.0 Definiciones Y Terminología.

Plataforma de Tecnologías de Información (TI)

Es el conjunto de hardware y software que componen las instalaciones y servicios tecnológicos de la UACH.

Plataforma de Tecnología Crítica

Es el conjunto de hardware, software e información institucional que resultan esenciales para la prestación de servicios de TI a la comunidad universitaria y a usuarios externos.

Incidente de Seguridad

Evento que comprometa la seguridad de cualquier elemento que conforme la plataforma tecnológica de la UACH.

Información Institucional

Conjunto de datos obtenidos, gestionados y resguardados por la UACH, los cuales representan un gran interés para la operación de las diversas dependencias universitarias.

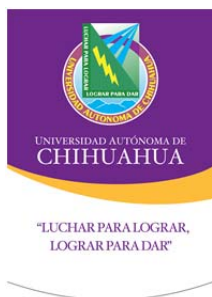
CERT-UACH

Equipo de Respuesta a Incidentes de Seguridad en Cómputo.

3.0 Responsables.

DAU
JCERT
RES
IS
USU

Departamento de Atención a Usuarios
Jefe del CERT-UACH
Responsable de Equipo o Servicio
Ingeniero en Seguridad del CERT-UACH
Usuario Afectado



Código: PRO 7.5 CERT 01	Página 2 de 3
Fecha de emisión: 08/11/2013	Fecha de Revisión: 08/11/2013 Número de Revisión: 1
Elaboró: Jefe del CERT-UACH	
Aprobado por: Coordinador General	

PROCEDIMIENTO DE ATENCIÓN A INCIDENTES DE SEGURIDAD INFORMÁTICA

4.0 Procedimiento.

4.1. DAU Recepción de solicitud

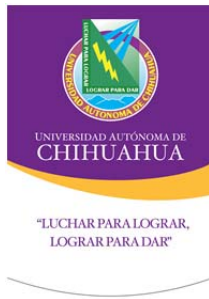
- 4.1.1. El USU o el RES detectan una anomalía en un equipo o servicio universitario y levanta una solicitud de servicio al DAU o el CERT-UACH.
- 4.1.2. El DAU asigna la solicitud al CERT-UACH.
- 4.1.3. El CERT-UACH recibe la solicitud por parte del DAU.

4.2. IS Atención del Incidente

- 4.2.1. El IS se contacta con el USU o con el RES para obtener detalles del incidente.
- 4.2.2. El IS inicia el llenado del formato **FOR 7.5 CERT 01** (Formato de Registro De Incidentes Informáticos).
- 4.2.3. De acuerdo a la afectación originada del incidente, clasificar el nivel de gravedad:
 - Nivel 1:** La plataforma tecnológica crítica (hardware, software e información institucional) no se encuentra en riesgo inminente. Ningún servicio institucional se encuentra afectado.
 - Nivel 2:** La integridad de la plataforma tecnológica crítica no se encuentra en riesgo inminente, pero parte de los servicios institucionales se encuentran afectados o inoperantes para varios usuarios.
 - Nivel 3:** La integridad de la plataforma tecnológica crítica (parte de ella o toda ella) se encuentra afectada o inoperante para todos o gran parte de los usuarios. Este nivel abarca el daño, robo, pérdida y/o modificación no autorizada de Bases de Datos e información institucional.
- 4.2.4. De acuerdo a la situación, el IS podrá atender dicha solicitud por los siguientes métodos:
 - Llamada telefónica
 - Correo electrónico
 - Chat o mensajería instantánea
 - Acceso remoto
 - Atención en sitio
- 4.2.5. El IS podrá aplicar las técnicas o mecanismos que considere pertinentes para contener el ataque y resolver la afectación.

4.3. IS Resolución del Incidente.

- 4.3.1. Una vez resuelta la situación, se finaliza el llenado del formato **FOR 7.5 CERT 01** (Formato de Registro De Incidentes Informáticos).
- 4.3.2. En caso de considerarlo pertinente, El IS podrá dar aviso a otros organismos de seguridad acerca del tipo de ataque informático contenido con la intención de apoyar en la prevención de este ataque a otras organizaciones, evitando dar información que pudiera ser utilizada para atentar contra la integridad de la plataforma tecnológica de la Universidad Autónoma de Chihuahua.



Código: PRO 7.5 CERT 01	Página 3 de 3
Fecha de emisión:08/11/2013	Fecha de Revisión:08/11/2013 Número de Revisión:1
Elaboró: Jefe del CERT-UACH	
Aprobado por: Coordinador General	

PROCEDIMIENTO DE ATENCIÓN A INCIDENTES DE SEGURIDAD INFORMÁTICA

5.0 Referencias.

5.1 Documentos de Referencia

**Manual de Políticas de Calidad
Acuerdos y Políticas de servicio de atención de incidentes de
Seguridad Informática**

**MPC 4.2 CGTI
DOC 7.5 CERT 02**

6.0 Formatos.

Formato de Registro de incidentes informáticos **FOR 7.5 CERT 01** 1 año

7.0 Historial de Revisiones.

No. De Revisión	Descripción de la Revisión	Fecha de Revisión
1	Liberación de procedimiento de atención a incidentes de seguridad informática.	08/11/2013