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 les equipos de cómputo y servicios públicos que son propiedad de la UACH.

2.0 Responsables.

DAU	Departamento de atención a usuarios
JCERT	Jefe del CERT-UACH
RES	Responsable de equipo o servicio
IS	Ingeniero en seguridad del CERT-UACH
USU	Usuario afectado

3.0 Procedimiento.

3.1. DAU Recepción de solicitud

3.1.1. 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.

3.1.2. El DAU asigna la solicitud al CERT-UACH.

3.1.3. El CERT-UACH recibe la solicitud por parte del DAU.

3.2. IS Atención del incidente

3.2.1. El IS se contacta con el USU o con el RES para obtener detalles del incidente.

3.2.2. El IS Inicia el llenado del formato **CGTI- CERT: F03** (Formato de registro de incidentes informáticos).

3.2.3. 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.

3.2.4. 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

3.2.5. El IS podrá aplicar las técnicas o mecanismos que considere pertinentes para contener el ataque y resolver la afectación.

3.3. IS Resolución del Incidente.

3.3.1. Una vez resuelta la situación, se finaliza el llenado del formato CGTI- CERT: F03 (Formato de registro de incidentes informáticos).

3.3.2. 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.

4.0 Referencias.

4.1 Documentos de Referencia

Manual de Políticas de Innovación	MPI CGTI: 01-01
Acuerdos y Políticas de servicio de atención de incidentes de Seguridad Informática	CGTI- CERT: D02

5.0 Formatos.

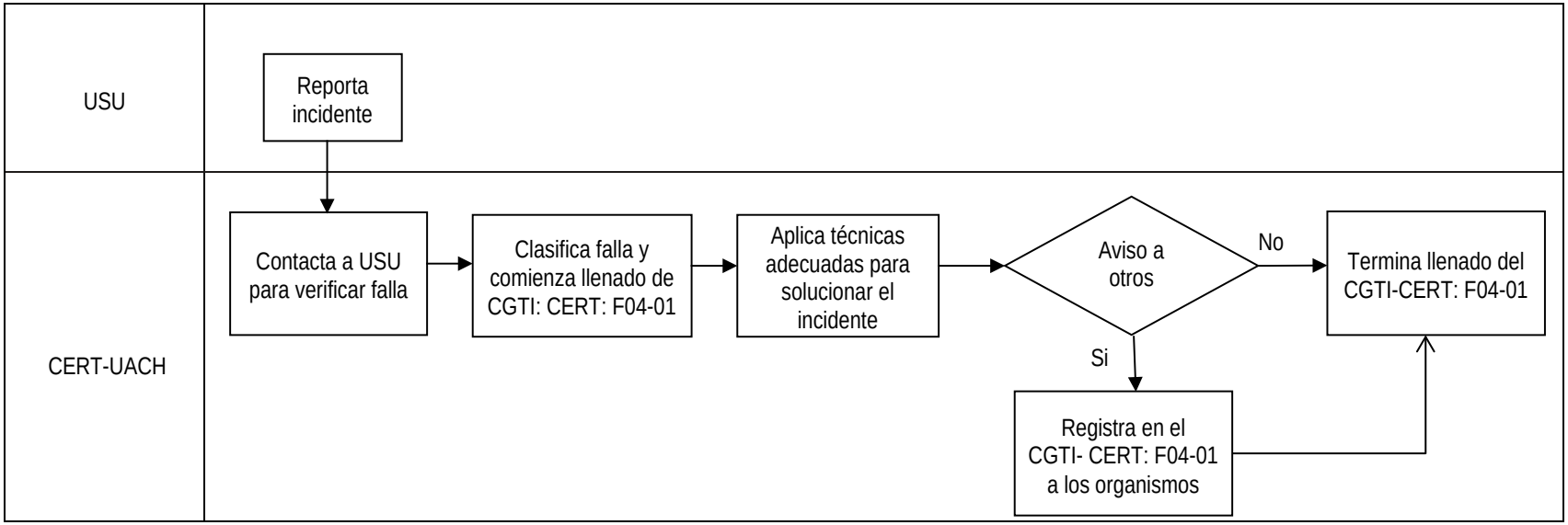
Formato de Registro de incidentes informáticos	CGTI- CERT: F03	1 año

6.0 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

DIAGRAMA DE INTERACCION PARA PROCEDIMIENTO DE ATENCIÓN A INCIDENTES DE SEGURIDAD INFORMÁTICA

Proceso definido	CGTI- CERT: P01-01 Referencia



Los recursos de maquinaria, equipo y herramientas se establecen y se asignan de acuerdo a su respectivo inventario vigente.
Los recursos de personal se establecen y se asignan de acuerdo a la plantilla autorizada que muestra el manual de organización.
Los recursos financieros se establecen y se asignan de acuerdo al presupuesto anual.

Proceso de interacción

El proceso que se muestra en esta interacción se define en su respectivo procedimiento o diagrama de flujo de referencia

→ Indica la comunicación formal que existe entre cada proceso.