

Código: PRO 7.5 CERT 02	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 AUDITORÍA DE SEGURIDAD EN CÓMPUTO

1.0 Propósito Y Alcance.

1.1 Propósito

Identificar vulnerabilidades en sistemas de cómputo con servicios informáticos públicos e internos que pongan en riesgo la información y la infraestructura tecnológica.

1.2 Alcance

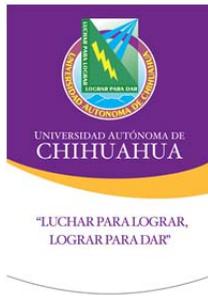
Este procedimiento aplica a todos los equipos con servicios públicos dentro de la red de datos de la UACH.

2.0 Definiciones Y Terminología.

Vulnerabilidad	Debilidad de un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia de un sistema o de sus datos o aplicaciones.
Base de Datos	Estructura de software que colecciona información relacionada. Se diseñó con la finalidad de solucionar y agilizar la administración de los datos que se almacenan en la memoria de la computadora.
Servidor	Es una computadora o un conjunto de aplicaciones (software) que provee una clase específica de servicio a un software "cliente" ubicado en otra computadora. Una sola computadora puede alojar varios paquetes de software de servidor corriendo en ella, y así proveer de varios servicios a clientes de la red.
CGTI	Coordinación de Tecnologías de Información
TI	Tecnologías de Información
CERT-UACH	Equipo de Respuesta a Incidentes de Seguridad en Cómputo.

3.0 Responsables.

JDC	Jefe de Departamento o Coordinador
JCERT	Jefe del CERT-UACH
GS	Gestor de Seguridad del CERT-UACH
RES	Responsable de Equipo o Servicio



Código: PRO 7.5 CERT 02	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 AUDITORÍA DE SEGURIDAD EN CÓMPUTO

4.0 Procedimiento.

4.1. CERT-UACH **Elabora plan anual de auditoría de seguridad.**

- 4.1.1. Durante el primer mes del año el JCER elabora el calendario anual donde se especifican las fechas en las que se llevará a cabo la auditoría de seguridad, mediante el formato **FOR 7.5 CERT 02** (Plan Anual De Auditorías De Seguridad).
- 4.1.2. Este calendario es enviado por oficio o correo electrónico a todos los JDC de la CGTI.
- 4.1.3. Los JDC tienen hasta un máximo de 5 días hábiles para solicitar un cambio de fecha para la auditoría, debiendo indicar la fecha deseada y no pasando de 30 días de la fecha propuesta. Esta solicitud debe ser enviada por oficio o por correo electrónico al JCERT. En caso de no recibir solicitudes, se considera como aceptada la fecha propuesta en el formato **FOR 7.5 CERT 02** (Plan Anual De Auditorías De Seguridad).

4.2. GS **Realización de la Auditoría de Seguridad en Cómputo**

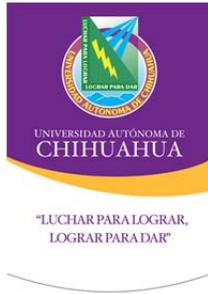
- 4.2.1. El GS realiza la auditoría de seguridad mediante el uso de cualquier herramienta informática especializada.
- 4.2.2. Los resultados generales de la auditoría serán entregados a CJDC correspondiente.
- 4.2.3. En caso de encontrarse vulnerabilidades críticas en los equipos auditados, se llena el **FOR 7.5 CERT 03** (Bitácora De Seguimiento De Auditorías De Seguridad) y se entrega mediante oficio al RES y al JDC correspondiente, para que corrijan la situación.

4.3. RES **Reparación de Vulnerabilidades.** CJDC

- 4.3.1. El RES tiene un plazo máximo de 30 días naturales (a partir de la entrega del FOR 7.5 CERT 03) para llevar a cabo la reparación de las vulnerabilidades encontradas.
- 4.3.2. Si la solución que implemente el RES para reparar las vulnerabilidades encontradas en la auditoría toman más de 30 días, el JDC correspondiente deberá mandar un oficio al JCERT indicando la razón por la cual la solución llevará más de 30 días en su implementación, así como la fecha final de solución..

4.4. JCERT **Verificación.**

- 4.4.1. Después de finalizar el período para la resolución de las vulnerabilidades críticas, se llevará a cabo otro análisis de vulnerabilidades como seguimiento a los equipos afectados.



Código: PRO 7.5 CERT 02	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 AUDITORÍA DE SEGURIDAD EN CÓMPUTO

4.4.2. Si después del período definido de resolución de las vulnerabilidades encontradas, el RES no ha implementado alguna medida para la corrección pertinente, se dará aviso al CG acerca de la situación, y el RES deberá realizar una acción correctiva.

4.4.3. En caso de que una vulnerabilidad no haya sido atendida después de 60 días después de la entrega del formato del FOR 7.5 CERT 03, se eliminará el acceso desde Internet del equipo hasta que sea corregida la vulnerabilidad del equipo.

5.0 Referencias.

5.1 Documentos de Referencia

Manual de Políticas de Calidad
Procedimiento de Acciones Correctivas

MPC 4.2 CGTI
PRO 8.5 CNO 02

6.0 Formatos.

Plan anual de Auditorías de Seguridad	FOR 7.5 CERT 02	1 año
Bitácora de Seguimiento de Auditorías de Seguridad	FOR 7.5 CERT 03	1 año

7.0 Historial de Revisiones.

No. De Revisión	Descripción de la Revisión	Fecha de Revisión
1	Liberación de procedimiento de auditoria de seguridad en cómputo.	08/11/2013