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.

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

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 CGTI- CERT: F04 (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 CGTI-CERT: F04 (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 CGTI-CERT: F05 (Bitácora De Seguimiento de Auditorias de Seguridad) y se entrega mediante oficio al RES y al JDC correspondiente, para que corrijan la situación.

4.3. RES CJDC Reparación de vulnerabilidades.

4.3.1. El RES tiene un plazo máximo de 30 días naturales (a partir de la entrega del CGTI-CERT: F05) 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.

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.

COPIA NO CONTROLADA

4.4.3. En caso de que una vulnerabilidad no haya sido atendida después de 60 días después de la entrega del formato del CGTI-CERT: F06-01, 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 Innovación	MPI CGTI 01
Procedimiento de Acciones Correctivas	CGTI-IDI: P08

6.0 Formatos.

Plan anual de Auditorías de Seguridad	CGTI-CERT: F04	1 año
Bitácora de Seguimiento de Auditorías de Seguridad	CGTI-CERT: F05	1 año

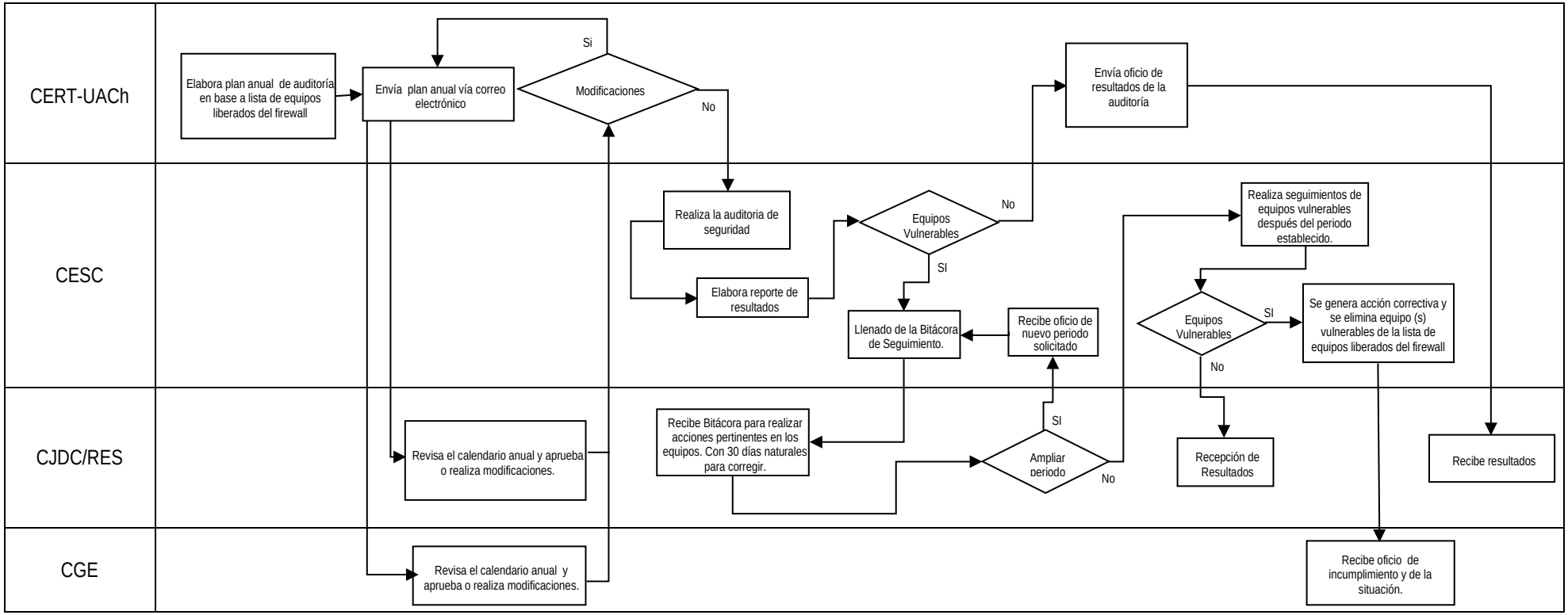
7.0 Historial de Revisiones.

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

COPIA NO CONTROLADA

DIAGRAMA DE INTERACCIÓN PARA AUDITORÍAS DE SEGURIDAD

Proceso definido	CGTI-CERT: P02-01 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.

COPIA NO CONTROLADA