ACTIVACIÓN Y OPERACIÓN DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DE TIC

	Elaboró:	Revisó:	Autorizó:
Puesto	Coordinación de Arquitectura de TIC	Jefatura de Gestión de Arquitectura e Infraestructura Tecnológica	Subdirección de Tecnologias de la Información y Comunicaciones
Firma			

1. Propósito

Atender de manera oportuna un incidente que requiera de la intervención del "**Equipo de Respuesta a Incidentes de Seguridad de TIC**", que se presenten en el Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra.

2. Alcance

Aplica para todas las áreas del Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra, que requieran de la atención inmediata ante un incidente que afecte la operación y la integridad de la información resguardada y almacenada en los activos de TIC, y que amerite la intervención del "Equipo de Respuesta a Incidentes de Seguridad de TIC".

3. Responsabilidades

- **Líder del ERISC**: Supervisar la difusión y la aplicación de la Guía Técnica de Respuesta a Incidente convocar al ERISC, así como verificar el establecimiento y actualización del Repositorio de Incidentes de Seguridad, recibir reportes sobre la ejecución de las acciones de resolución de incidentes y establecer los mecanismos de comunicación efectivos para convocar al ERISC, supervisar el cierre de incidentes y que se integren al Repositorio de Incidentes de Seguridad e informar al Responsable de la Seguridad de la Información en el Instituto, sobre los incidentes de seguridad de la información de TIC y su solución.

- **Líder suplente del ERISC**: Coordinar la elaboración, difusión y aplicación de la Guía Técnica de Respuesta a Incidentes, verificar el establecimiento y actualización del Repositorio de Incidentes de Seguridad, en sustitución del Líder del ERISC, convocar al Equipo, supervisar la ejecución de las acciones de resolución de incidentes y establecer los mecanismos de comunicación efectivos para convocar al ERISC, participar activamente en la aplicación de los procedimientos de atención a incidentes con el resto del Equipo, realizar el cierre de incidentes y verificar que se integren al Repositorio de Incidentes de Seguridad, e informar al Líder del ERISC sobre los incidentes de seguridad de la información de TIC y su correspondiente atención y solución.

- **Analista de Incidentes de seguridad**: Colaborar activamente en la elaboración de la Guía técnica de Respuesta a Incidentes, proponer los mecanismos de monitoreo y detección de incidentes conforme a los procesos y sistemas de su responsabilidad, participar activamente en la aplicación de los procedimientos de atención a incidentes con el resto del Equipo y en el caso de requerir tomar decisiones sobre la recuperación de la infraestructura critica que haya tenido la falla, la deberán tomar en forma conjunta las Jefaturas de Gestión de Arquitectura e Infraestructura Tecnológica, Gestión y Desarrollo de soluciones Tecnológicas, Gestión y Operación de Servicios y Gestión Estratégica , además de facilitar la información necesaria para el registro y/o actualización de los incidentes en el repositorio.

4. Políticas de operación y normas.

- Al detectar un incidente de seguridad que requiera la intervención del ERISC se notificará inmediatamente al Líder del ERISC y/o al Líder suplente del ERISC vía correo electrónico, teléfono celular o utilizar voceo solo para localización.

- Los integrantes del ERISC son los que activan el procedimiento de atención a incidentes de seguridad de la información de TIC.

- La información relativa a los incidentes de seguridad de la información de TIC, es decir: Guía técnica de respuesta a incidentes, Registro de datos del incidente y su solución, así como los Reportes de incidentes al Responsable de la Seguridad de la Información, será almacenada en el Repositorio de Incidentes de Seguridad. Dicho repositorio contará con controles de acceso para los miembros del equipo conforme al rol desempeñado y al tema específico de su atención.

- Mantener informada a la Mesa de Servicios en el ciclo del incidente de seguridad de la información de TIC, de manera formal por medio del correo dgos@inr.gob.mx, como único canal de comunicación hacia las áreas usuarias afectadas.

- El Responsable de la Seguridad de la Información del Instituto, contará con información periódica de los incidentes ocurridos en el periodo, misma que será proporcionada por el líder del ERISC.

- El cierre de los incidentes solo podrá ser realizado por el Líder Suplente del Equipo de Respuesta a Incidentes de Seguridad de la Información de TIC.

5. Descripción del procedimiento:

N°	RESPONSABLE	ACTIVIDAD
1.	**Analista de incidentes de seguridad**	Identificar un incidente de seguridad de la información de TIC que debe atender el ERISC.
2.		Informar al Líder del ERISC y/o Líder suplente del ERISC, vía correo electrónico, teléfono celular o voceo.
3.	**Líder del ERISC/Líder suplente del ERISC**	Activar el procedimiento de atención de acuerdo a las **guías técnicas de respuesta a incidentes**. Asignar a los **Analistas de incidentes de seguridad** correspondientes para la atención del incidente.

4.	**Analista de incidentes de seguridad**	Realiza una revisión exhaustiva del incidente.
5.	**Analista de incidentes de seguridad**	Ejecuta acciones de corrección de acuerdo a las **guías técnicas de respuesta a incidentes** y de ser necesario se apoya con los responsables de los Dominios Tecnológicos para su solución. ¿Se solucionó el incidente? Si: Pasar a la actividad 7. No: Realiza una investigación técnica para la contención del incidente, de acuerdo a las guías técnicas de respuesta a incidentes, e informar a la Mesa de Servicios el tiempo estimado de solución. Pasar a la actividad 6.
6.	**Líder suplente del ERISC.**	Monitorear el avance de la solución del incidente con los Analistas de incidentes de seguridad involucrados. ¿Se solucionó el incidente? Si: Pasa a la actividad 7. No: Pasar a la actividad 5.
7.	**Analista de incidentes de seguridad**	Elaborar reporte de las acciones realizadas de la solución del incidente e integra la información en el Repositorio de Incidentes de Seguridad.

6. Documentos de referencia:

DOCUMENTO	CODIGO
NMX-CC-9001-IMNC-2008 ISO 9001:2008 Sistemas de Gestión de la Calidad	N/A
Manual de Gestión de la Calidad	MGC-DG-01
Control de Documentos y Registros	PR-SGC-01
MAAGTICSI	Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información

REGISTRO	TIEMPO DE CONSERVACIÓN	RESPONSABLE DE CONSERVACIÓN	CODIGO
Metodología de Auditoría Informática y Seguridad de la Información	Sin fecha límite	Coordinador de Auditoría Informática y Seguridad de la Información	MT-STIC-02
Ambiente de Pruebas	2 años	Coordinador de Auditoría Informática y Seguridad de la Información	F12-MT-STIC-08

7. Glosario

TIC: Tecnologías de la Información y Comunicaciones.

STIC: Subdirección de Tecnologías de la Información y Comunicaciones.

DGAIT: Departamento de Gestión de Arquitectura e Infraestructura Tecnológica.

Incidente: Cualquier evento que no forma parte de la operación estándar de un servicio y que puede causar una interrupción o una reducción de la calidad del mismo.

Activos de TIC: Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, sus componentes, medios de transmisión y comunicación, las bases de datos o archivos electrónicos y la información contenida en éstos.

Analista Especializado: Es el personal experto en la atención o solución de uno o más servicios proporcionados por la STIC (colaboradores de la mesa de servicio, ingenieros de servicios de infraestructura para voz, datos y edificio inteligente, e ingeniero de arquitectura para cambios y configuraciones, arquitecto-diseñador o desarrollador-integrador o proveedor).

ERISC: Equipo de Respuesta a Incidentes de Seguridad de TIC.

Incidentes de Seguridad: Cualquier Evento provocado por un agente interno o externo que modifica o daña la Infraestructura y la información.

8. Control de cambios

Revisión	Descripción del cambio	Fecha
00	Inicio en el Sistema de Gestión de la Calidad	Julio 2013
01	Actualización de la imagen institucional, actualización del nombre del instituto	JUN 15