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

1. Descripción general.

El Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, en la Administración Pública Federal, establece que las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI) alineado a la política general de seguridad de la información.

El MGSI debe conformarse, entre otros elementos, por un protocolo de respuesta ante incidentes de seguridad de la información, que contemple la conformación de un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC), acciones de preparación, detección y análisis, contención, erradicación y recuperación, así como actividades posteriores al incidente, de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

En observancia a lo anterior, la Dirección General de Tecnologías de la Información (DGTI) realizará procedimientos de monitoreo de incidentes de los distintos servicios TIC que administra la DGTI y de los que son usuarios las Unidades Administrativas y Órganos Administrativos Desconcentrados de la Secretaría de Salud.

2. Propósito.

Administrar de manera oportuna el ciclo de vida de los incidentes de seguridad que requieran de la intervención del "**Equipo de Respuesta a Incidentes de Seguridad de TIC (ERISC)**", que se presenten en la Secretaría de Salud.

3. Alcance.

Aplica para todos los servicios de tecnologías de la información y comunicación de la Secretaría de Salud que requieran de la atención inmediata ante un incidente de seguridad que impacte en la disponibilidad, integridad y confidencialidad de la información resguardada y almacenada en los activos de información.

4. Responsabilidades para la Integración del ERISC.

Líder del ERISC (Dirección de Red y Telecomunicaciones): Supervisar la aplicación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, convocar al ERISC, así como verificar el establecimiento y actualización del sistema de tickets, 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 sistema de tickets e informar al Responsable de la Seguridad de la Información de la Secretaría de Salud, sobre los incidentes de seguridad de la información de TIC y su solución.

Líder suplente del ERISC (Director de Sistemas e Infraestructura): Coordinar la aplicación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, verificar el establecimiento y actualización del sistema de tickets, 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 sistema de tickets, e informar al Líder del ERISC sobre los incidentes de seguridad de la información de TIC y su correspondiente atención y solución.

Responsable del manejo de Incidentes (Dirección de Seguridad a la Información): Colaborar activamente en la aplicación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, 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, avisar al área responsable sobre la recuperación de la infraestructura critica que haya tenido la falla, distribuir al área correspondiente la información necesaria para la atención de los incidentes en el sistema de tickets.

5. Matriz de roles y responsabilidades (RACI).

Se identifican y asignan los diferentes roles y responsabilidades que existen dentro del ERISC:

ACTIVIDAD	ROL			
	Responsable de la Seguridad de la Información	Líder del ERISC	Líder suplente del ERISC	Responsable del manejo de Incidentes
Convocar al ERISC	I	R	R	I
Aplicación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos	I	R	R	R
Reporte de incidentes de seguridad de la información de TIC.	I	R	A	C
Propuesta de mecanismos de monitoreo y detección de incidentes	A	A	C	R
Participación en la aplicación de los procedimientos de atención a incidentes.	C	R	R	R
Ejecución de las acciones de resolución de incidentes.	A	R	R	R
Cierre de incidentes.	A	R	R	R
Distribuir al área correspondiente la información necesaria para la atención de los incidentes	I	A	A	R

(R) Responsable **(A) Aprueba** **(C) Consultado** **(I) Informado**

6. Políticas de operación.

Correo electrónico. Establecer las condiciones para el uso adecuado del correo Institucional de la Secretaría de Salud.

Desarrollo de software. Garantizar la seguridad en los nuevos desarrollos de software que se realicen en la Secretaría de Salud, así como en los existentes, en cualquiera de las UA u OAD.

Implementación del Centro de Datos. Definir los requisitos mínimos necesarios de seguridad, para la implementación del Centro de Datos para la Secretaría de Salud, a través de un prestador de servicio.

Portales y páginas alojadas en la infraestructura de la Secretaría. Proporcionar información para la definición de las reglas y normas de seguridad, para la protección en los sitios web del dominio salud.gob.mx.

Protección de datos personales. Cumplir con las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Red Local e Internet. Establecer la condiciones y responsabilidades para el uso de la red local e internet.

Respaldo y borrado seguro de información. Validar que, al retirar los servidores del Centro de Datos y Equipo de Cómputo Personal, éstos no lleven registro de algún dato que pueda ser recuperado a fin de garantizar la seguridad de la información.

Seguridad de voz por IP. Establecer los lineamientos de seguridad para el uso de equipos de telefonía IP, a fin de proporcionar a las UA/OAD las herramientas tecnológicas en materia de telefonía IP que permitan la interconexión para los servicios de voz y datos, bajo el protocolo IP.

Seguridad física y ambiental. Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la Secretaría de Salud.

Servicio de Seguridad perimetral. Establecer servicios que evalúan y actúan sobre la continuidad y calidad de entrega de los servicios de la tecnología tales como el monitoreo, seguridad y atención y respuesta a incidentes.

Servicios de Centro de Datos. Establecer las condiciones adecuadas para el uso y aprovechamiento de los recursos del Centro de Datos.

Uso de cuentas VPN's. Definir el uso adecuado de las VPN (Red Privada Virtual).

Uso de Equipo de Cómputo. Definir el uso adecuado de los equipos de cómputo.

7. Descripción del procedimiento.

El procedimiento de monitoreo de incidentes de los distintos servicios TIC que administra y de los que son usuarios las Unidades Administrativas y Órganos Administrativos Desconcentrados de la Secretaría de Salud, será el siguiente:

No.	ACTIVIDAD	RESPONSABLE
1.	Identificar un incidente de seguridad de TIC que debe atender el ERISC.	Responsable del manejo de Incidentes
2.	Informar al Líder del ERISC y/o Líder suplente del ERISC del incidente.	Responsable del manejo de Incidentes
3.	Asignar al personal correspondiente para la atención de incidentes de seguridad.	Líder del ERISC/Líder suplente del ERISC
4.	Realizar un análisis exhaustivo del incidente en colaboración con los coordinadores de las diferentes Áreas Técnicas de la DGTI.	Líder del ERISC/ Líder suplente del ERISC/ Responsable del manejo de Incidentes

5.	Ejecutar acciones de contención, corrección y de ser necesario, se apoyará con los responsables de los Dominios Tecnológicos y representantes técnicos de las empresas proveedoras de los servicios de TIC para su solución.	Responsable del manejo de Incidentes Líder suplente del ERISC Líder del ERISC
	¿Se solucionó el incidente? **Si:** Pasar a la actividad 7. **No:** Realiza una investigación técnica para la contención del incidente e informar a la Mesa de Servicios el tiempo estimado de solución. Pasar a la actividad 6.	
6.	Realiza el monitoreo del avance de la solución del incidente con el personal designado para la atención de incidentes de seguridad involucrados.	Líder suplente del ERISC.
	¿Se solucionó el incidente? **Si:** Pasa a la actividad 7. **No:** Pasar a la actividad 5.	
7.	Integración de la información de las acciones realizadas de la solución del incidente en el sistema de tickets.	Responsable del manejo de Incidentes
8.	Termina Procedimiento.	

8. Documentos de referencia.

- ✓ Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, en la Administración Pública Federal.
  Difusión: https://dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021#gsc.tab=0

- ✓ Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.
  Difusión: https://www.gob.mx/gncertmx/documentos/94081

- ✓ Políticas de Seguridad de la Información, Secretaría de Salud.
  Difusión: https://dgti.salud.gob.mx/doctos/dgti/POLITICAS_DE_SEGURIDAD_DE_LA_INFORMACION.PDF

9. Términos y definiciones.

i. Activo de información: La información, los datos y los recursos que la contienen, procesan y transmiten, que por su importancia y el valor que representa para la Secretaría de Salud, deben ser protegidos.

ii. DGTI: Dirección General de Tecnologías de la Información.

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

iv. 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.

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

vi. MSGI: Marco de Gestión de Seguridad de la Información.

vii. Seguridad de la Información: La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

viii. Sistema de tickets: Sistema desarrollado para el registro y atención de incidentes de seguridad y seguimiento a requerimientos, relacionados con servicios TI de la Secretaría de Salud.

ix. TIC: Tecnologías de la Información y Comunicación.

10. Bitácora de actualizaciones o control de cambios.

DESCRIPCIÓN DEL CAMBIO	ALCANCE	APROBÓ	FECHA DE APLICACIÓN
Primera versión de este documento	Observancia para todas las áreas técnicas de la DGTI	DGTI-SSA	Diciembre 2023