OBJETIVO

Gestionar las alertas, eventos e incidentes de seguridad de la información de la Superintendencia Nacional de Salud para tomar los correctivos necesarios, prevenir su recurrencia y cumplir con las obligaciones legales y regulatorias aplicables, a través de la descripción de las etapas de:

- Prevención.
- Reporte y análisis.
- Gestión y solución.
- Documentación y lecciones aprendidas.
- Recolección y preservación de evidencia digital.
- Evaluación de acciones legales y coordinación con autoridades.

En concordancia con la norma ISO/IEC 27001:2022 y la normativa colombiana en materia de seguridad digital y protección de datos personales.

ALCANCE

Este procedimiento aplica a:

- Toda la información generada, recibida, procesada, almacenada o transmitida por la Superintendencia Nacional de Salud, independientemente de su medio (físico, digital, nube, etc.) y de su nivel de clasificación.
- Todos los sistemas de información, servicios tecnológicos, infraestructura de TI y soluciones de analítica administrados por la Superintendencia Nacional de Salud.
- Todos los servidores públicos, empleados, contratistas, proveedores y terceros que tengan acceso a la información, sistemas o recursos tecnológicos de la entidad.
- Todas las sedes físicas, centros de datos, ambientes en la nube y canales de atención que soporten procesos misionales, estratégicos y de apoyo

RESPONSABLE DEL PROCEDIMIENTO

Responsable técnico de la gestión operativa del procedimiento: Subdirector- Subdirección de Tecnologías de la Información.

DEFINICIONES

Incidente de seguridad de la información: Evento o serie de eventos no deseados o inesperados relacionados con la seguridad de la información, que tienen una probabilidad significativa de comprometer la confidencialidad, integridad o disponibilidad de la información o de los servicios tecnológicos de la Superintendencia Nacional de Salud.

Evento de seguridad de la información: Ocurrencia identificada dentro de un servicio, sistema o red que indica una posible violación de la política de seguridad de la información, una falla de controles o una situación previamente desconocida que puede ser relevante para la seguridad.

Gestión de incidentes de seguridad de la información: Conjunto de actividades y procesos para detectar, reportar, registrar, analizar, clasificar, responder, contener, erradicar, recuperar y aprender de los incidentes de seguridad de la información.

Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISI): Grupo multidisciplinario coordinado por el Grupo de Seguridad Digital, responsable de la atención, coordinación y seguimiento de incidentes significativos de seguridad de la información.

Soporte OTI: Canal oficial para gestionar solicitudes y reportes relacionados con TI y seguridad, mediante el correo electrónico soporte.oti@supersalud.gov.co.

Violación de seguridad de los datos personales: Incidente de seguridad que ocasione la destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a datos personales transmitidos, conservados o tratados de otra forma.

Tercero/proveedor de servicios tecnológicos: Entidad externa que suministra servicios de infraestructura, aplicaciones, nube, soporte o cualquier otro servicio de TI que procese información de la Superintendencia Nacional de Salud.

Evidencia digital: Información almacenada o transmitida en forma digital, que puede ser utilizada como prueba de un hecho, actividad o evento, y que debe ser recolectada, preservada y manejada de manera que mantenga su integridad, autenticidad, trazabilidad y valor probatorio.

Cadena de custodia: Registro documentado y continuo de la posesión, transferencia, análisis y almacenamiento de la evidencia digital, desde su obtención hasta su disposición final.

ABREVIATURAS

TI: Tecnologías de la Información.

SGSI: Sistema de Gestión de Seguridad de la Información.

ERISI: Equipo de Respuesta a Incidentes de Seguridad de la Información.

OTI: Oficina/Subdirección de Tecnologías de la Información (según denominación institucional).

CSIRT: Computer Security Incident Response Team.

CSIRT-GOB CO, colCERT, CSIRT Salud: Equipos de respuesta a incidentes de seguridad digital del Gobierno de Colombia.

LINEAMIENTOS GENERALES O POLÍTICAS DE OPERACIÓN

1. Todo servidor público, contratista o tercero que identifique un evento o incidente de seguridad de la información debe reportarlo **de inmediato** a través de los canales definidos en este procedimiento, sin intentar ocultarlo o resolverlo por su cuenta sin coordinación con el Grupo de Seguridad Digital.

2. Los incidentes de seguridad de la información se gestionan de manera centralizada por el **Grupo de Seguridad Digital**, con el apoyo de los grupos técnicos (Infraestructura y Servicios Tecnológicos, Sistemas de Información, Estrategia, Gobierno y Arquitectura de TI, Subdirección de Analítica y otros que corresponda).

3. El reporte inicial de incidentes se realizará mediante correo electrónico a:

   - soporte.oti@supersalud.gov.co
     con copia obligatoria a:
   - seguridaddigital@supersalud.gov.co

4. Los incidentes se registrarán y gestionarán en la herramienta institucional de mesa de servicios **CA Service Desk Manager**, donde se abrirá un caso/ticket asignado al grupo **“Grupo Seguridad de la Información”** con:

   - Prioridad: **1**
   - Urgencia: **5 – Inmediatamente**
   - Impacto: **1 – Toda la organización**

5. La clasificación de severidad de los incidentes se realizará considerando, entre otros:
    - Alcance del incidente (usuarios, procesos, sedes afectadas).
    - Sensibilidad y volumen de la información comprometida.
    - Afectación a la prestación de servicios misionales y derechos de los ciudadanos.
    - Obligaciones de reporte y posibles sanciones legales o regulatorias.
6. Para la **recolección y preservación de evidencia digital** se aplicarán los principios establecidos en la norma ISO/IEC 27037 (legalidad, integridad, autenticidad, trazabilidad, competencia del personal, proporcionalidad), sin reproducir su contenido textual, mediante las actividades definidas en este procedimiento.
7. Siempre que un incidente pueda constituir una violación de datos personales, un posible delito informático o un hecho relevante para autoridades de control, el Grupo de Seguridad Digital coordinará con la **Subdirección de Defensa Jurídica** y la **Subdirección Recursos Jurídicos** la evaluación de acciones legales y de reporte a autoridades.
8. Este procedimiento se integra al SGSI y debe revisarse al menos **una vez al año**, o antes, cuando se presenten incidentes de alto impacto, cambios significativos en la normatividad o modificaciones relevantes en la arquitectura de TI.

DIAGRAMA DE FLUJO

Ver Flujograma Procedimiento de Gestión de Incidentes de Seguridad de la Información.

DESARROLLO -DESCRIPCIÓN

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
1	**Identificar fuentes de alerta y grupos de interés especial** Identificar y mantener actualizados los contactos y fuentes de alertas de seguridad (CSIRT Salud, colCERT/CSIRT-GOB CO, fabricantes, proveedores tecnológicos, comunidades de seguridad, MinTIC, etc.), que puedan emitir avisos sobre vulnerabilidades y amenazas relevantes para la Superintendencia Nacional de Salud.	Grupo de Seguridad Digital	Permanente: Revisión mínima mensual.	No aplica
2	**Analizar comunicados y alertas de seguridad recibidas** Analizar los comunicados, boletines y alertas de seguridad recibidos para identificar su relevancia frente a los sistemas, infraestructuras y servicios de la entidad, determinando si se requieren medidas preventivas.	Grupo de Seguridad Digital	Cada vez que se reciba un comunicado	Correo y registro de Sharepoint con alertas recibidas, con conclusiones y

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
				acciones recomendadas.
3	**Implementar medidas preventivas en coordinación con grupos técnicos** Establecer y ejecutar las acciones preventivas necesarias (aplicación de parches, cambios de configuración, restricciones de acceso, refuerzo de monitoreo, etc.) en los sistemas y servicios afectados.	Grupo de Seguridad Digital, Grupo de Infraestructura y Servicios Tecnológicos, Grupo de Sistemas de Información	Cada vez que se identifiquen vulnerabilidades o riesgos relevantes	Tickets en CA Service Desk Manager u otros registros de cambios/preventivos.
4	**Reportar el evento o incidente de seguridad de la información** Reportar el evento o incidente de seguridad mediante correo a **soporte.oti@supersalud.gov.co** con copia a **seguridaddigital@supersalud.gov.co**, indicando como mínimo: • Descripción del hecho. • Fecha y hora aproximada de ocurrencia. • Sistemas, información y/o procesos aparentemente afectados.	Todos los servidores públicos, contratistas y terceros	Inmediato, al detectar el evento	Registro del incidente en ticket en CA Service Desk Manager.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
5	**Registrar el evento en CA Service Desk Manager** Recibir el correo de reporte y registrar el caso en **CA Service Desk Manager**, asegurando que: • Se cree un ticket clasificado como incidente de seguridad de la información. • Se asigne al grupo **"Grupo Seguridad de la Información"**. • Se configure **Prioridad 1**, **Urgencia 5 – Inmediatamente**, **Impacto 1 – Toda la organización**. • Se adjunten al ticket los correos y evidencias preliminares.	Operario de la mesa de servicio (agente de primer punto de contacto).	Inmediato, al recibir el correo	Ticket en CA Service Desk Manager.
6	**Notificar al Grupo de Seguridad Digital sobre el nuevo ticket** Notificar al Grupo de Seguridad Digital (por avisos automáticos de la herramienta y/o correo interno) sobre la creación del ticket de incidente de seguridad de la información.	Operario de la mesa de servicio	Inmediato, una vez registrado el ticket	Notificación automática de la herramienta / correo interno.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
7	**© Validar si el evento corresponde a un incidente de seguridad de la información** • Revisar la información registrada en el ticket y las evidencias preliminares para determinar si el evento reportado cumple la definición de incidente de seguridad de la información. ○ ¿El evento corresponde a un incidente de seguridad de la información? ▪ **Sí:** Continúe en la actividad 8. ▪ **No:** Continúe en la actividad 9.	Grupo de Seguridad Digital	Dentro de las primeras 2 horas hábiles siguientes al registro del ticket (o antes, si se observa afectación crítica)	Actualización del ticket en CA Service Desk Manager con la decisión de validación.
8	**Clasificar el incidente y valorar su severidad** Analizar el incidente validado considerando: • Impacto potencial o real sobre servicios misionales y derechos de los ciudadanos.	Grupo de Seguridad Digital	Máximo 4 horas hábiles después de la validación	Ticket en CA Service Desk Manager con la clasificación de severidad.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
	• Sensibilidad y volumen de la información comprometida (incluyendo datos personales). • Número de usuarios/procesos afectados. • Posibles obligaciones de reporte a entes externos. Definir la severidad (crítico, alto, medio, bajo) y registrar la clasificación.			
9	**Cerrar o redirigir eventos que no constituyen incidentes de seguridad de la información** Cuando el evento no corresponda a un incidente de seguridad de la información, actualizar el ticket indicando la justificación y, de ser necesario, reclasificarlo como solicitud de servicio, incidente de TI general u otra categoría correspondiente, siguiendo los procedimientos de TI.	Grupo de Seguridad Digital.	Inmediato, tras la validación.	Ticket en CA Service Desk Manager con justificación de reclasificación/cierre.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
10	**© Decidir si se requiere activar el ERISI** Con base en la severidad, alcance y sensibilidad de la información involucrada: ¿El incidente es crítico o alto, o implica posibles obligaciones legales significativas (p. ej. violación de datos personales masiva, afectación grave de servicios de salud)? • **Sí:** Activar ERISI y continúe en la actividad 11. • **No:** Gestionar con equipo de Seguridad Digital y grupos técnicos sin activar ERISI formal; continúe en la actividad 12.	Grupo de Seguridad Digital	Inmediato, para incidentes clasificados como crítico o alto	Anotación en el ticket y/o acta o correo de convocatoria del ERISI.
11	**Convocar y coordinar el ERISI (cuando aplique)** Convocar a los miembros definidos del ERISI (Seguridad Digital, Infraestructura y Servicios Tecnológicos, Sistemas de Información, Estrategia, Gobierno y Arquitectura de TI, Subdirección de Analítica, Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional, Subdirección de Defensa Jurídica/Subdirección	Grupo de Seguridad Digital	Inmediato, incidente crítico o alto	Acta o resumen de convocatoria (correo, minutas de reunión), referenciada en el ticket.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
	Recursos Jurídicos, Oficina de Control Interno y demás que aplique) para coordinar acciones de respuesta y seguimiento.			
12	**Definir la estrategia de contención y mitigación** Analizar el incidente y definir medidas de contención (aislamiento de equipos, bloqueo de cuentas, deshabilitación de servicios, filtros temporales, entre otros) y mitigación para restringir el impacto y evitar su propagación.	Grupo de Seguridad Digital, Grupo de Infraestructura y Servicios Tecnológicos, Grupo de Sistemas de Información (y otros grupos según el caso)	Inmediato, según severidad del incidente	Ticket en CA Service Desk Manager con la estrategia de contención y mitigación.
13	**Implementar la solución técnica del incidente** Ejecutar las acciones técnicas necesarias para erradicar la causa del incidente (aplicar parches, restaurar respaldos, reconfigurar controles, limpiar malware, ajustar reglas de firewall, etc.), coordinando con el Grupo de Seguridad Digital.	Grupo de Infraestructura y Servicios Tecnológicos, Grupo de Sistemas de Información, otros grupos técnicos	Según plan definido en la actividad 12	Detalle de actividades técnicas en el ticket, evidencias técnicas (logs, capturas, reportes de herramientas).

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro

14	**© Verificar la efectividad de la solución**
	
	Validar que el incidente haya sido efectivamente contenido y solucionado (no se presentan nuevos eventos, el servicio se restableció de forma segura, no hay indicios de persistencia de la amenaza).
	
	• ¿La solución es efectiva y el incidente está controlado?
	  ○ **Sí:** Continúe en la actividad 15.
	  ○ **No:** Retorne a la actividad 12 para redefinir acciones de contención/solución.
		Grupo de Seguridad Digital	Tras la implementación de la solución	Evidencias de verificación anexas al ticket (pruebas, validaciones, reportes).

15	**Notificar la solución del incidente a los afectados y partes interesadas** Comunicar a los usuarios o áreas afectadas la solución implementada, el restablecimiento de los servicios y, cuando aplique y sea autorizado, orientaciones para prevenir incidentes similares. En incidentes de alto impacto o con repercusión externa, coordinar	Grupo de Seguridad Digital; Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional (cuando aplique)	Una vez verificada la solución	Comunicados enviados, correos, avisos internos, asociados al ticket.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
	mensajes oficiales con la Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional.			
16	**Documentar el incidente en la herramienta y/o formato institucional** Completar en CA Service Desk Manager y en los formatos del SGSI la información del incidente, incluyendo: • Descripción detallada del incidente. • Causa raíz (cuando sea posible identificarla). • Sistemas y datos afectados. • Acciones de contención, erradicación y recuperación ejecutadas. • Tiempo de indisponibilidad o afectación de servicios.	Grupo de Seguridad Digital	Dentro de los 5 días hábiles posteriores al cierre técnico	Ticket finalizado y/o formulario interno de registro de incidentes de seguridad de la información.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
17	**Identificar controles y requisitos del SGSI e ISO 27001 afectados** Analizar el incidente y determinar qué controles del SGSI y qué requisitos de la ISO/IEC 27001:2022 se vieron comprometidos o resultan relevantes, para alimentar la gestión de riesgos y la mejora continua.	Grupo de Seguridad Digital	Conjuntamente con la actividad 16	Nota en el ticket y/o ficha de análisis de incidentes del SGSI.
18	**Registrar lecciones aprendidas y acciones de mejora** Identificar lecciones aprendidas (falencias, buenas prácticas observadas, aspectos a reforzar) y proponer acciones de mejora (ajuste de controles, actualización de procedimientos, nuevas capacitaciones, mejoras tecnológicas).	Grupo de Seguridad Digital	Posterior al cierre del incidente	Acta de lecciones aprendidas, plan de acción, tareas registradas en el SGSI o en el sistema de gestión institucional.
19	**Cerrar formalmente el incidente en el SGSI y en la herramienta de registro** Actualizar el ticket en **CA Service Desk Manager** y los registros del SGSI indicando: • Fecha de cierre.	Grupo de Seguridad Digital	Una vez concluidas las acciones técnicas y, cuando aplique, las principales decisiones	Ticket cerrado en CA Service Desk Manager y registros del SGSI.

N.	Actividad	Responsable	Tiempo frecuencia si aplica	Registro
	• Estado final del incidente. • Principales lecciones aprendidas. • Acciones de mejora generadas.		legales y administrativas	

ANEXOS

No aplica.

Control de cambios					
Versión	**Fecha**	**Descripción de los cambios**			
1	02/03/2026	Versión inicial del documento			
Elaboró		**Revisó**		**Aprobó**	
Nombre	Jose Luis Alejandro Carrillo Valderrama	Nombre	Omar Fredy García Ortega	Nombre	Jose Alexander de Los Reyes Aldana
Cargo	Profesional especializado	Cargo	Subdirector Técnico	Cargo	Director de Innovación y Desarrollo
Fecha	27/02/2026	Fecha	27/02/2026	Fecha	27/02/2026