 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2
		Fecha: 03/Feb./2026

PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	
OBJETIVO:	Establecer las actividades para la gestión eficaz de eventos, incidentes y debilidades de seguridad de la información en la Superintendencia de Notariado y Registro (SNR), protegiendo los activos de información y minimizando los posibles impactos operativos.
ALCANCE:	Limite Inicial: Reporte de situación (incidente, evento o debilidad).
	¿Qué hace? Gestionar adecuadamente los incidentes, eventos o debilidades reportados por los usuarios de la SNR.
	Limite Final: Documentación y cierre del caso de incidente, evento o debilidad debidamente gestionados.
PRODUCTOS:	<ul style="list-style-type: none"> • Formato de Gestión de Incidentes de Seguridad • Formato de Costeo de Incidentes de Seguridad • Planes de mejora de incidentes
RESPONSABLE:	Estratégico: Jefe Oficina Tecnologías de la Información Operativo: Gestor de Incidentes

1. GLOSARIO

Activo de Información: Cualquier dato, documento, sistema, infraestructura, proceso o recurso tecnológico que soporte la operación institucional y requiere protección por su valor para la entidad.

Alta Dirección: Nivel directivo responsable de tomar decisiones estratégicas frente a incidentes significativos y asignar recursos necesarios para su tratamiento.

Análisis de Causa Raíz (ACR): Método utilizado para identificar las causas fundamentales que originaron un incidente o evento de seguridad, con el fin de evitar su recurrencia.

Contención: Acciones inmediatas dirigidas a detener la propagación, impacto o evolución de un incidente. Incluye aislar equipos, bloquear accesos, suspender servicios o detener comportamientos anómalos.

Corrección: Acciones dirigidas a restaurar la operación normal afectada por un incidente o evento, sin necesariamente eliminar la causa raíz.

CSIRT / COLCERT: Grupo nacional de respuesta a incidentes cibernéticos encargado de coordinar, asesorar y recibir notificaciones de incidentes significativos conforme a normatividad vigente en Colombia.


Debilidad de Seguridad: Falla, brecha, ausencia de control o condición que aumenta la posibilidad de que ocurra un incidente de seguridad de la información.

Erradicación: Conjunto de acciones orientadas a eliminar completamente la causa del incidente (malware, cuentas comprometidas, configuraciones inseguras o vulnerabilidades explotadas).

Evento de Seguridad de la Información: Suceso o situación no deseada o inesperada que puede estar relacionada con la seguridad de la información, pero que no afecta directamente la confidencialidad, integridad o disponibilidad. Requiere análisis y revisión, pero no necesariamente constituye un incidente.

Gestor de Incidentes: Responsable de coordinar, clasificar, escalar y hacer seguimiento a las acciones para el tratamiento de incidentes y eventos, asegurando el cumplimiento del procedimiento.

Impacto: Consecuencia que genera un incidente sobre los procesos, servicios institucionales, usuarios o activos de información.

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2 Fecha: 03/Feb./2026

Incidente de Seguridad de la Información: Evento o serie de eventos no deseados que afectan o comprometen la confidencialidad, integridad, disponibilidad, trazabilidad o autenticidad de los activos de información.

Lecciones Aprendidas: Conocimientos obtenidos durante la gestión del incidente, que deben documentarse y utilizarse para mejorar controles, procesos o tecnologías.

Mesa de Ayuda Integral (MAI): Primer nivel de atención encargado de recibir reportes, registrar casos y realizar el escalamiento inicial al Gestor de Incidentes o área correspondiente.

Mesa Técnica de Gestión de Incidentes: Equipo interdisciplinario convocado para analizar incidentes significativos o extensos, definir acciones técnicas y estratégicas y coordinar el tratamiento integral del incidente.

Mitigación: Reducción del impacto o probabilidad de un incidente mediante la aplicación de controles inmediatos o complementarios.

Oficial de Seguridad de la Información (OSI): Responsable del cumplimiento del SGSI, verificación del proceso de gestión de incidentes, asesoría técnica y aseguramiento del cumplimiento normativo.

Plan de Mejoramiento: Documento que define acciones específicas, responsables y plazos orientados a corregir causas identificadas y prevenir la recurrencia de un incidente, no conformidad o situación que afecte la operación o la seguridad de la información.

Recuperación: Acciones destinadas a restablecer completamente la operación normal, restaurar servicios afectados y asegurar la continuidad funcional tras un incidente.

Registro del Incidente: Documento o formato oficial donde se consignan las acciones tomadas, responsables, tiempos, impacto, análisis y cierre del incidente o evento.

SGSI: Sistema de Gestión de Seguridad de la Información.

SOC (Security Operations Center): Equipo o servicio especializado encargado del monitoreo, detección y análisis de eventos o incidentes de seguridad en tiempo real.

Vulnerabilidad: Debilidad explotable en un sistema, proceso o servicio que puede resultar en un incidente si no es corregida.


2. CONDICIONES GENERALES:

2.1. Normatividad:

Ley Estatutaria 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales.”

Decreto 767 de 2022. “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.”

Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.”

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2
		Fecha: 03/Feb./2026

2.2. Políticas de operación

- 1. Reporte Inmediato:** Toda situación que pueda constituir un incidente, evento o debilidad de seguridad debe ser reportada de inmediato por cualquier funcionario, contratista o tercero a través de la Mesa de Ayuda Integral (MAI) o, en su defecto, presencialmente en la Oficina de TI. El reporte debe registrarse siempre en la herramienta MAI, sin excepciones.
- 2. Clasificación Obligatoria:** Toda situación reportada debe ser clasificada por el **Gestor de Incidentes** según:
 - Tipo: **Incidente, Evento, Debilidad.**
 - Nivel de criticidad conforme a las tablas institucionales.
 - No puede existir gestión sin clasificación previa.


2.1. La clasificación de los **incidentes** de debe realizar de acuerdo con la siguiente tabla.

NIVEL	DESCRIPCIÓN
Extenso	Situación de seguridad que implica un paro total o suspensión de las operaciones de la entidad por un tiempo prolongado
Significativo	Situación de seguridad que compromete la operación normal de algunos procesos de la entidad, pero que pueden ser controlados en forma paralela al desarrollo de las demás actividades del negocio
Moderado	Situación que compromete la integridad, confidencialidad o disponibilidad de las operaciones de la entidad de forma muy leve, y que por lo tanto no requieren una acción inmediata
Menor	Situación que compromete la integridad, confidencialidad y/o disponibilidad a un grupo localizado de usuarios o que causan un impacto muy limitado de las operaciones de la entidad, y que por lo tanto no requieren una acción inmediata
Soporte	Eventos que no comprometen las operaciones de la entidad, que afectan a solo un usuario y que por lo tanto pueden tramitarse como un REQUERIMIENTO o SOLICITUD DE CASO DE SOPORTE.

2.2. La clasificación de **eventos** se debe realizar de acuerdo con la siguiente tabla.

NIVEL	DESCRIPCIÓN
Evento de criticidad Media	Posibles anomalías o situaciones detectadas por los sistemas de información y/o personas que puedan ser relevantes para la seguridad de la información. Con el fin de evitar que el evento vuelva a ocurrir se deberá implementar controles y verificar si se encuentra en planes de

Código de Formato: SIG - FR - 002 Versión: 1 Fecha Aprobación: 09/Jun./2025

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2 Fecha: 03/Feb./2026

NIVEL	DESCRIPCIÓN
	concientización o si se requiere una comunicación específica para la situación.
Evento de criticidad Alta	Implica el daño de un activo y el posible incumplimiento de una política de seguridad pero que no presenta resultados negativos en cuanto a la afectación de los pilares de seguridad de la información. Con el fin de evitar que el evento vuelva a ocurrir se deberá realizar una solicitud de acción de mejora.

2.3. Las debilidades no se gestionan como incidente y no se clasifican. Deben ser asignadas al Gestor de Riesgos de Seguridad Digital, quien evalúa la debilidad, actualiza matriz de riesgos, define plan de tratamiento y realiza cierre en MAI.


3. Contención Inmediata de Incidentes: La contención inicial de los incidentes debe ejecutarse antes de convocar a comités o informar a instancias superiores. Esto incluye medidas como: aislamiento, bloqueo, deshabilitación de cuentas, desconexión de equipos, entre otros.

4. Mesa Técnica de Gestión de Incidentes: La Mesa Técnica de Gestión de Incidentes será convocada cuando se trate de un incidente **con nivel de criticidad Extenso o Significativo** (de manera presencial o virtual), y su función es analizar impactos y recomendar acciones de contención, corrección, contingencia o comunicación ante incidentes de alta criticidad, así como para apoyar el análisis de causa raíz y planes de mejora. La Mesa Técnica estará integrada por los siguientes roles:

- Jefe de la Oficina de Tecnologías de la Información (preside la mesa y define la decisión final cuando no haya unanimidad).
- Coordinadores de la Oficina de Tecnología de la Información
- Gestor de Cambios
- Gestor de Incidentes
- Oficial de Seguridad de la Información
- Invitados (funcionarios, Contratistas y/o Proveedores)

5. Reporte a Instancias Nacionales: Se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad (o sus equivalente en su procedimiento interno). El reporte a COLCERT/CSIRT gobierno se realiza al correo contacto@colcert.gov.co

6. Evidencia y Preservación: Durante la contención y corrección de los incidentes, deben preservarse evidencias relevantes sin comprometer la operación. El responsable de gestionar el incidente debe mantener una bitácora de acciones que posteriormente será documentada en el Formato de Gestión de Incidentes.


 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2 Fecha: 03/Feb./2026

7. **Documentación Obligatoria:** Toda gestión de incidentes debe quedar registrados en:
- **Formato de Gestión de Incidentes**
 - **Formato de Costeo de Incidentes** (Cuando aplique)
8. **Gestión de Problemas de Seguridad de la Información:** Cuando un incidente sea recurrente o no tenga causa conocida, se reclasificará como **problema**. La gestión de problemas seguirá el mismo flujo general de incidentes, pero con las siguientes particularidades:
- Participación de coordinaciones, líderes técnicos de los componentes involucrados y, cuando aplique, proveedores.
 - Conformación de mesas técnicas de emergencia para analizar la causa raíz.
 - Elaboración de un plan de acción específico para eliminar o mitigar la causa subyacente.
 - Documentación del análisis y las decisiones adoptadas, diferenciándolas del registro de incidentes.
9. **Apoyo de Terceros:** Cuando la atención de un incidente exceda la capacidad técnica del colaborador asignado, la Oficina de Tecnología de la Información podrá solicitar apoyo a proveedores, terceros o entidades gubernamentales. El Oficial de Seguridad de la Información (o el Grupo de Seguridad de la Información) deberá mantener actualizado el listado Contactos con Autoridades y Grupos de Interés del SGSI, con la información de autoridades y proveedores con acuerdos vigentes. El Gestor de Incidentes utilizará este listado para realizar los escalamientos o solicitudes de apoyo externo necesarios.


3. DESCRIPCIÓN DE ACTIVIDADES DEL PROCEDIMIENTO:

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
INICIO 1. REPORTAR SITUACIÓN CONSIDERADA COMO EVENTO, INCIDENTE O DEBILIDAD.	1.1. Reportar de manera inmediata cualquier señal, anomalía o hecho que pueda constituir un evento, incidente o debilidad de seguridad de la información.	Cualquier usuario – Área reportante o Sistema automático	Ticket de Mesa de Ayuda
2. ASIGNAR AL GESTOR DE INCIDENTES PARA CLASIFICACIÓN ESPECÍFICA.	2.1. Recibir y enviar reporte al Gestor de Incidentes, quien inicia la evaluación preliminar y clasifica el tipo de situación de acuerdo con lo establecido en el Procedimiento de Mesa de Ayuda. 2.2. Clasificar inicialmente la situación entre evento, incidente o debilidad según su naturaleza, alcance y afectación potencial. Ver Política de Operación No. 2.	Gestor de Incidentes / Mesa de Servicio / SOC	Ticket de Mesa de Ayuda


Código de Formato: SIG - FR - 002 Versión: 1 Fecha Aprobación: 09/Jun./2025

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
		Versión: 2
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Fecha: 03/Feb./2026


ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
	<p>¿Qué tipo de situación está siendo reportada?</p> <p>Es un incidente: Ir a la actividad No. 3. Es un evento: Ir a la actividad No. 14.</p> <p>Punto de Control: El Jefe de la Oficina de Tecnologías de la Información debe asegurar que siempre haya personal disponible para recibir reportes inmediatos de señales, anomalías o hechos relacionados con eventos, incidentes o debilidades de seguridad de la información.</p>		
3. REALIZAR CLASIFICACIÓN DEL NIVEL DE CRITICIDAD DEL INCIDENTE	<p>3.1. Determinar la criticidad del incidente (menor, moderado, significativo o extenso) según impacto, alcance y urgencia.</p> <p>Ver Política de Operación No. 2.1.</p>	Gestor de Incidentes	Ticket de Mesa de Ayuda
4. ASIGNAR EL INCIDENTE AL ESPECIALISTA RESPONSABLE DE LA ATENCIÓN Y RESPUESTA	<p>4.1. Asignar el incidente formalmente al especialista técnico o equipo responsable de su análisis y atención según la naturaleza o activos afectados por el incidente.</p> <p>4.2. Informar al Oficial de Seguridad de la Información para su conocimiento.</p>	Gestor de Incidentes	Ticket de Mesa de Ayuda
5. EJECUTAR ACCIONES INICIALES DE CONTENCIÓN, MITIGACIÓN Y CORRECCIÓN DEL INCIDENTE	<p>5.1. Implementar medidas para contención, erradicación y recuperación ante el incidente, de la siguiente forma:</p> <ul style="list-style-type: none"> - Identificación y Aislamiento: Se detecta el incidente y se toman medidas inmediatas para detener su propagación y limitar su alcance. Esto implica por ejemplo aislar la amenaza, desconectar sistemas comprometidos o segmentar la red para evitar que el incidente se propague. - Nota: Si para la contención, se requiere realizar algún cambio en la infraestructura o configuración, se podrá acudir a los cambios de emergencia conforme a lo establece el Procedimiento de Control de Cambios de TI. - Contención de la actividad maliciosa: Si el incidente está relacionado con una actividad maliciosa, se busca contener y detener lo antes posible. Esto puede implicar bloquear direcciones IP, deshabilitar cuentas comprometidas o eliminar malware. - Preservación de la evidencia: Durante la contención, también se debe tener cuidado de preservar la evidencia relacionada con el incidente. Esto es fundamental para investigaciones futuras y posibles acciones legales. <p>5.2. Implementar medidas de corrección del incidente, de la siguiente forma:</p> <ul style="list-style-type: none"> - Restauración de la funcionalidad: Una vez que el incidente está bajo control y aislado, se procede a trabajar en la restauración de la funcionalidad normal del sistema o servicio afectado. Esto puede implicar la restauración desde copias de seguridad limpias. 	Especialista Técnico / Analista SOC / Gestor de Incidentes	Ticket de Mesa de Ayuda Control de Cambios (Si aplica)

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
		Versión: 2
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Fecha: 03/Feb./2026

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
	<p>- Implementación de medidas de seguridad adicionales: Se identifican las vulnerabilidades que permitieron el incidente y se toman medidas para parchear o corregir esas vulnerabilidades. Además, se implementan mejoras en la seguridad para prevenir futuros incidentes similares.</p>		
6. DEFINIR MANEJO DEL INCIDENTE SEGÚN SU NIVEL DE CRITICIDAD	<p>6.1. Validar el nivel de criticidad para decidir si se continúa por un flujo estándar (menor/moderado) o se requieren acciones más profundas como activación del equipo de respuesta ampliado (Extenso/Significativo).</p> <p>¿Qué nivel de criticidad se tiene?</p> <p>Si es un incidente Extenso/Significativo: Ir a la actividad No. 7. Si es un incidente Menor/Moderado: Ir a la actividad No. 11.</p>	Gestor de Incidentes	Ticket de Mesa de Ayuda
7. REPORTAR A COLECTIC/CSIRT Y CONVOCAR LA MESA TÉCNICA DE GESTIÓN DE INCIDENTES (SOLO SI APLICA)	<p>7.1. Notificar al COLCERT/CSIRT de acuerdo con lo establecido por norma.</p> <p>7.2. Reunir a la Mesa Técnica de Gestión de Incidentes para revisión, coordinación estratégica y toma de decisiones complementarias dado el caso.</p> <p>7.3. Registrar la sesión (acta o grabación), documentar las decisiones y remitirlas a los participantes de la Mesa Técnica.</p> <p>Nota: Los especialistas asignados de TI responsables de la atención del incidente deberán asistir, presentar avances y ejecutar las acciones acordadas en la Mesa Técnica.</p> <p>Ver Política de Operación No. 4.</p>	Gestor de Incidentes	Ticket de Mesa de Ayuda
8. REVISAR EL INCIDENTE Y PLANTEAR ACCIONES COMPLEMENTARIAS	<p>8.1. Analizar el incidente con mayor detalle y se definen acciones adicionales en caso de ser necesarias (erradicación profunda, reforzamiento de controles, recuperación, etc.).</p>	Mesa Técnica de Gestión de Incidentes de Seguridad	Acta de Sesión o Informe Preliminar del Incidente
9. INFORMAR A LA ALTA DIRECCIÓN DE IMPACTOS, ACCIONES EJECUTADAS Y REQUERIMIENTOS ADICIONALES	<p>9.1. De la mesa técnica realizada, se deberá informar a la alta dirección sobre los impactos del incidente, acciones ejecutadas, posibles acciones adicionales o recursos requeridos para la mitigación definitiva del incidente, según cada caso.</p>	Gestor de Incidentes Oficial de Seguridad de la Información	Acta de Sesión o Informe Preliminar del Incidente
10. EJECUTAR ACCIONES ADICIONALES DE ERRADICACIÓN, CONTENCIÓN O MITIGACIÓN SEGÚN LO DEFINIDO POR LA MESA TÉCNICA	<p>10.1. Aplicar medidas avanzadas de contención, limpieza, erradicación o restauración definidas en la mesa técnica para asegurar la eliminación o recuperación total del incidente.</p>	Especialistas Oficina de TI	Evidencia de las acciones ejecutadas Ticket de Mesa de Ayuda

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
11. IDENTIFICAR LA CAUSA RAÍZ DEL INCIDENTE, ESTRUCTURAR PLAN DE MEJORAMIENTO	<p>11.1. Realizar análisis de causa raíz (ACR), identificando factores técnicos, humanos o de proceso, en el formato "Análisis Causa Raíz" identificado con el Código: SIG - FR - 025 del Proceso Sistema Integrado de Gestión</p> <p>11.2. Estructurar el plan de mejoramiento en que se incluya un análisis que permita identificar causas, y orientar las actividades a prevenir reincidencias del incidente, definiendo el responsable de su ejecución y los términos para su desarrollo. En el Formato "Formulación, Reformulación del Plan de Mejoramiento", identificado con el código SIG-FR-027 del Proceso Sistema Integrado de Gestión.</p> <p>11.3. Completar el registro "Formato Gestión de incidentes" documentando causa raíz, acciones tomadas, tiempos, responsables y lecciones aprendidas.</p> <p>Punto de Control: El Oficial de Seguridad podrá solicitar en cualquier momento, la generación de un reporte de los incidentes de seguridad ocurridos y el estado actual de los mismos. Así mismo, podrá revisar la concordancia de la información reportada por los diferentes colaboradores en el formato de Autoridades y Grupos de Interés del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la adecuada gestión de estos y generar el informe correspondiente.</p>	<p>Gestor de Incidentes</p> <p>Especialistas Oficina de TI</p>	<p>Formato "Gestión de Incidentes de Seguridad de la Información"</p> <p>Formato "Análisis Causa Raíz"</p> <p>Formato "Formulación Reformulación Plan de Mejoramiento"</p>
12. REALIZAR MONITOREO Y EJECUCIÓN DE PLANES DE MEJORA.	<p>12.1. Supervisar la implementación de los planes de mejora definidos y se hace seguimiento a su cumplimiento.</p> <p>¿Se soluciono el incidente?</p> <p>Validar las medidas implementadas corrigieron completamente el incidente y eliminaron riesgos asociados.</p> <p>Si: Ir a la actividad No. 13</p> <p>No: Reasignar el incidente al especialista. Ir a la actividad No. 4.</p>	<p>Gestor de Incidentes</p> <p>Oficial de Seguridad de la Información</p>	<p>Correo electrónico</p>
13. REALIZAR CUANTIFICACIÓN DEL INCIDENTE Y CIERRE	<p>13.1. Se cierra formalmente el incidente, registrando su impacto cuantitativo y cualitativo, tiempos de atención y cumplimiento del proceso mediante un informe.</p> <p>Nota: El informe de costos de incidentes consolidado debe ser presentado a la alta dirección, por parte del jefe de tecnología de la información y el Oficial de Seguridad de la información en la revisión anual que se realice por parte de la dirección al Sistema de Gestión de Seguridad de la Información</p>	<p>Gestor de Incidentes</p>	<p>Registro de análisis de Impacto</p>
14. CLASIFICAR EL EVENTO DE SEGURIDAD Y ASIGNARLO AL ENCARGADO DE SU REVISIÓN	<p>14.1. Clasificar el tipo de evento y asignar a un responsable para su revisión y seguimiento.</p> <p>Ver Política de Operación No. 2.2.</p>	<p>Gestor de Incidentes</p>	<p>Ticket de Mesa de Ayuda</p>

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 2

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
15. PLANTEAR Y EJECUTAR LAS ACCIONES DE MITIGACIÓN DEL EVENTO DE SEGURIDAD	15.1. Definir e implementar acciones correctivas o preventivas asociadas al evento reportado.	Especialistas Oficina de TI	Ticket de Mesa de Ayuda
16. EVALUAR SI LAS ACCIONES APLICADAS PERMITIERON CONTROLAR TOTALMENTE EL EVENTO.	16.1. Realizar seguimiento y evaluar si las acciones aplicadas permitieron controlar totalmente el evento. ¿Las medidas fueron eficaces para mitigar y controlar el evento? Si: Ir a la actividad No. 16. No: Reasignar el evento al especialista. Ir a la actividad No. 14.	Gestor de Incidentes Oficial de Seguridad de la Información	Ticket de Mesa de Ayuda
17. ESTABLECER MEDIDAS PREVENTIVAS Y DOCUMENTAR LAS MEDIDAS EFECTUADAS PARA EL CIERRE DEL EVENTO DE SEGURIDAD	17.1. Establecer acciones preventivas para evitar que el evento evolucione hacia un incidente de seguridad. 17.2. Registrar el tratamiento del evento, acciones realizadas, responsables y estado final.	Gestor de Incidentes	Ticket de Mesa de Ayuda
18. ORGANIZAR Y ARCHIVAR LA DOCUMENTACIÓN FIN	18.1. Organizar y archivar la documentación de acuerdo con los lineamientos del proceso de Gestión Documental y Gestión de Tecnologías de la Información con el fin de garantizar la disponibilidad, la integridad y confidencialidad de la información (Políticas de Seguridad de la Información y de Gestión Documental)	Funcionario y/o contratista de la Oficina de Tecnologías de la Información	Carpeta digital u archivo físico de la Oficina.


4. DOCUMENTOS ASOCIADOS:

4.1. Documentos internos:

- Manual de Políticas del SGSI – Superintendencia de Notariado y Registro - Sección 6.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- Manual de Gestión de Incidentes de Seguridad
- Formato de Gestión de Incidentes
- Formato de Costeo de Incidentes
- Procedimiento de cambios de TI
- Procedimiento de mesa de ayuda

4.2. Documentos externos:

- ISO27001:2022 Control 8.21 – Gestión de Incidentes de Seguridad
- Modelo de Seguridad y Privacidad de la Información - MinTic

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PR-009
		Versión: 2
	PROCEDIMIENTO: GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Fecha: 03/Feb./2026

VERSIÓN DE CAMBIOS			
Código:	Versión:	Fecha:	Motivo de la actualización:
GTI-PR-009	1	19/Dic./2025	Elaboración y emisión de la primera versión del Procedimiento, como mecanismo para la prevención, detección, respuesta y recuperación ante eventos que afecten la confidencialidad, integridad o disponibilidad de la información, en el marco del SGSI.
GTI-PR-009	2	03/Feb./2026	Se ajusta la actividad N. 11 con la adopción de los formatos del sistema integrado de gestión "Análisis Causa Raíz" para realizar el registro del análisis de causa del incidente de seguridad presentado y el formato "Formulación, Reformulación del Plan de Mejoramiento" para registrar las actividades correctivas y preventivas para el incidente presentado, además, de anexar el formato gestión de incidentes de seguridad de la información.

ELABORACIÓN Y APROBACIÓN			
ELABORÓ	APROBÓ	REVISIÓN METODOLOGICA	Vo. Bo. Oficina Asesora de Planeación
Jorge Armando Serrano Caicedo	Jorge Arcenio Cañaverl Rojas	Paula Natalia Castellanos Sierra	Nubia Patricia López Méndez
Profesional Oficina de Tecnologías de la Información	Jefe de la Oficina de Tecnologías de la Información	Grupo Arquitectura Organizacional y Mejoramiento Continuo Oficina Asesora de Planeación	Jefe de la Oficina Asesora de Planeación.
Fecha: 29/01/2026	Fecha: 29/01/2026	Fecha: 30/01/2026	Fecha de Aprobación: 03/02/2026