Guía para el Equipo de Respuesta a Incidentes de Seguridad de la Información de la SNR.

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código: SIG - SSI - PO - 04 - PR - 03 - GI - 01	**Versión: 01**	**Fecha: 06 de Diciembre de 2022**

EQUIPO DIRECTIVO

WILLIAM PEREZ CASTAÑEDA
SECRETARIA GENERAL
MARIO ALEXANDER ORTIZ SALGADO
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS TORRES RODRÍGUEZ
COORDINADOR DEL GRUPO DE ARQUITECTURA ORGANIZACIONAL MEJORAMIENTO CONTINUO
LEYLA ZORAYA GUZMAN RODRIGUEZ
OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
GRUPO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
GRUPO ARQUITECTURA ORGANIZACIONAL MEJORAMIENTO CONTINUO
OFICINA ASESORA DE PLANEACIÓN

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

TABLA DE CONTENIDO

1 INTRODUCCIÓN.

Para cumplir los objetivos de los procedimientos de Gestión de Incidentes de seguridad de la información y Gestión de Vulnerabilidades técnicas es preciso contar con el **Equipo de Respuesta a Incidentes de Seguridad de la Información** con competencias y responsabilidades claramente identificadas.

El presente documento define los roles y responsabilidades del **Equipo de Respuesta a Incidentes de Seguridad de la Información** alineados con el marco normativo vigente y ajustado a la realidad operativa de la Superintendencia de Notariado y Registro.

2 MARCO NORMATIVO

- **Resolución 0500 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". Con el análisis de este marco regulatorio se establecen los siguientes aspectos a considerar:
  - La Superintendencia de Notariado y Registro es sujeto obligado de cumplimiento por el decreto 1078 de 2015 Art. 2.2.9.1.1.2.
  - Se deben adoptar medidas técnicas, administrativas y de talento humano para garantizar la seguridad digital y que se incorpore al Plan de Seguridad y privacidad de la información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.
  - Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital (Oficial de Seguridad de la Información).
- **Guía núm. 21 del MSPI Guía para la Gestión y clasificación de Incidentes de Seguridad de la información MINTIC**.
  - Capítulo 4. Objetivo "…Definir roles y responsabilidades dentro de la Organización como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio.

- Capítulo 6. Roles y responsabilidades para atender la gestión de incidentes. La Guía define los siguientes roles (en el capítulo "**6. Roles y perfiles necesarios para la atención de incidentes**"):

  - **Usuario Sensibilizado**.
  - **Agente Primer punto de contacto**.
  - **Administrador del Sistema**. Se define como la persona encargada para mantener y configurar un Activo de información.
  - **Administrador de los sistemas de seguridad**. Personas encargadas de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo.
  - **Analista Forense**. Es un experto en el tema forense, quien debe estar disponible en caso de que un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) requiera una investigación completa para solucionarlo y determinar los siguientes Ítems • Que sucedió. • Donde sucedió. • Cuando Sucedió. • Quien fue el responsable • Como sucedió.
  - **Responsables de soporte técnico**. Complementan la labor de ejecución (Nivel 3) de las actividades correctivas o preventivas al Administrador del Sistema (Nivel 2) y son internos o de terceros (sugerido por MINTIC en el capítulo 7. Recomendaciones finales y a quien debo informar).
  - **Líder del Grupo de Atención de incidentes**.

3 OBJETIVO.

Identificar formalmente los roles y responsabilidades del **Equipo de Respuesta a incidentes de seguridad de la información** y formalizar su gestión de manera alineada con el marco normativo vigente y la estructura actual de cargos de la SNR.

4 EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DE LA SNR.

4.1 OBJETIVOS DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

El Equipo de Respuesta a Incidentes de Seguridad de la Información de la SNR se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades de atención de los incidentes de seguridad de la información y de manera alineada con el marco normativo expuesto. Este Equipo incluye la gestión de **todos los incidentes** asociados a la seguridad de la información.

4.2 ROLES Y RESPONSABILIDADES

Con el fin de poder gestionar integralmente los incidentes de seguridad de la información se definen los siguientes roles del equipo de respuesta a incidentes de Seguridad de la Información en la SNR:

- **Usuario Sensibilizado**. Ciudadanos o personas de Entidades externas a la SNR, que consumen sus servicios o le prestan servicios, funcionarios, contratistas y en general cualquier persona que sostenga algún tipo de relación con la SNR y que reporta un incidente/vulnerabilidad de seguridad de la información.

- **Usuario de Activo de información.** Todo funcionario y/o contratista independiente o perteneciente a una Empresa que presta servicio a la SNR que pertenece al grupo de usuarios de un Activo de Información.

- **Comité de Gestión y Desempeño**. Comité formal de dirección de la SNR que hace las veces de Comité de Seguridad de la Información.

- **Líder del Sistema de Gestión de Seguridad de la Información**. Equivalente al Oficial de Seguridad de la Información en los marcos normativos.

- **Líder del Grupo de Respuesta a Incidentes de Seguridad de la Información**. Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos. El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, , Gestión de Talento Humano, Gestión

Jurídica, Tecnología, Representante de las Directivas para el SGSI). Escala los incidentes de seguridad de acuerdo con los procedimientos definidos y consolida información asociada con el incidente.

- **Agente Primer punto de contacto Mesa de ayuda**. Recibe los reportes de incidentes de seguridad de la información, los registra y direcciona al Líder del Grupo de Atención de Incidentes.

- **Dueño del Activo de Información.** Rol a ser ejecutado por Jefes, Directores de Áreas dueños o custodios del Activo de información y su responsabilidad está enmarcada dentro de la primera línea de defensa.

- **Custodio del Activo de Información.** Rol a ser ejercido por los Coordinadores de Grupo que custodian un Activo de información. Su responsabilidad está enmarcada dentro de la primera línea de defensa.

- **Gestor Técnico de Plataforma Tecnológica.** Rol a ser ejecutado por Administradores del Sistema y personas que conforman el Equipo de soporte técnico. Son todos aquellos que configuran y mantienen un activo de información.

- **Gestores de Seguridad Informática.** Rol a ser ejecutado por Administradores de Seguridad Informática y los miembros del Equipo de seguridad. Personas encargadas de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo.

- **Administrador de Seguridad Física.** Personas encargadas del mantenimiento preventivo/correctivo y gestión de la seguridad física.

- **Proveedor de infraestructura Tecnológica/Servicios Especializados.** Personas naturales o jurídicas con contratos de servicios tecnológicos con la SNR.

- **Analista Forense**. Es un experto en el tema forense, quien debe estar disponible en caso de que un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) requiera una investigación completa para solucionarlo y determinar los siguientes Ítems • Que sucedió. • Donde sucedió. • Cuando Sucedió. • Quien fue el responsable • Como sucedió.

4.3 CONSIDERACIONES.

1. La definición de roles y responsabilidades del **Equipo de Respuesta a incidentes de seguridad de la información** se ha establecido con los marcos normativos vigentes.

2. Para el **Equipo de Respuesta a incidentes de seguridad de la información** se han establecido roles que en su gran mayoría deben ser asumidos por cargos existentes en la SNR y estas responsabilidades deben ser formalizadas por sus líderes.

3. Otros roles que requieren ejecución específica y que no son asumidos por cargos existentes son asignados a contratistas y/o contratos de prestación de servicios vigentes en la SNR.

4. La identificación de roles y responsabilidades del **Equipo de Respuesta a incidentes de seguridad de la información** se presenta en la matriz RACI (Ejecutor (**R**esponsible), Responsable (**A**ccountable), Consultado (**C**onsulted), Informado (**I**nformed)) para un mejor entendimiento de las responsabilidades y sus interacciones.

4.4 MATRIZ RACI - ROLES Y RESPONSABILIDADES

						Primera Línea de Defensa							
	Usuario sensibilizado	Comité de Gestión y desempeño	Líder del Sistema de Gestión de Seguridad de la Información	Líder del Grupo de Respuesta de Incidentes	Agente Primer punto de contacto Mesa de Ayuda	Dueño del Activo de Información	Custodio del Activo de Información	Usuario de un activo de información	Administrador de seguridad Física	Gestores Técnicos de Plataforma Tecnológica	Gestores de seguridad informática	Proveedor de Infraestructura Tecnológica - Servicio Especializado	Analista Forense
Preparación de plataforma tecnológica													
Asegurar redes, sistemas, aplicaciones, infraestructura tecnológica y física (ej.: Aplicación de parches de seguridad, Aseguramiento de plataforma, Seguridad en redes, prevención de código malicioso, sensibilización y entrenamiento de usuarios).						**I**	**A**			**R**	**R**	**R C**	
Configurar y administrar dispositivos de seguridad						**I**	**A**			**R**	**R**	**R C**	
Certificar productos y servicios				**I**		**I**	**A**			**R**	**R**	**R C**	

						Primera Línea de Defensa							
	Usuario sensibilizado	Comité de Gestión y desempeño	Líder del Sistema de Gestión de Seguridad de la Información	Líder del Grupo de Respuesta de Incidentes	Agente Primer punto de contacto Mesa de Ayuda	Dueño del Activo de Información	Custodio del Activo de Información	Usuario de un activo de información	Administrador de seguridad Física	Gestores Técnicos de Plataforma Tecnológica	Gestores de seguridad informática	Proveedor de Infraestructura Tecnológica - Servicio Especializado	Analista Forense
Conocer totalmente los comportamientos de la infraestructura administrada red, sistemas y equipos				**I**		**I**	**A**			**R**	**R**	**R**	
Mantener base centralizada de información que permita hacer análisis del incidente, (Logs de servidores, redes, aplicaciones).				**I**		**I**	**A**			**R**	**R**	**R**	**I**
Correlacionar eventos para descubrir patrones de comportamiento anormal y poder identificar las causas del incidentes						**I**	**A**			**R**	**R**	**R**	
Administrar unicidad en fuente de tiempo (sincronizar relojes)							**R**			**R**	**A**	**R**	
Mantener una base de conocimiento con información de nuevas vulnerabilidades			**I**	**I**		**I**	**R**			**R**	**A**	**R**	

						Primera Línea de Defensa							
	Usuario sensibilizado	Comité de Gestión y desempeño	Líder del Sistema de Gestión de Seguridad de la Información	Líder del Grupo de Respuesta de Incidentes	Agente Primer punto de contacto Mesa de Ayuda	Dueño del Activo de Información	Custodio del Activo de Información	Usuario de un activo de información	Administrador de seguridad Física	Gestores Técnicos de Plataforma Tecnológica	Gestores de seguridad informática	Proveedor de Infraestructura Tecnológica - Servicio Especializado	Analista Forense
Mantener una base de conocimiento con información de servicios habilitados			**I**	**I**	**I**	**I**	**A**			**R**	**R**	**R**	
Mantener actualizada la lista de contactos de gestión de incidentes			**I**	**A**	**I**	**R**	**R**			**R**	**R**	**R C**	**R C**
Identificar y gestionar elementos para alerta sobre futura ocurrencia del incidente (Análisis de logs de servidores, logs de aplicaciones, logs de herramientas de seguridad, cualquier otra herramienta que permita la identificación de un incidente de seguridad.			**I**	**I**		**I C**	**A**			**R**	**R**	**C**	**C**
Investigar y/o implementar productos y proyectos de seguridad de la información													

						Primera Línea de Defensa							
	Usuario sensibilizado	Comité de Gestión y desempeño	Líder del Sistema de Gestión de Seguridad de la Información	Líder del Grupo de Respuesta de Incidentes	Agente Primer punto de contacto Mesa de Ayuda	Dueño del Activo de Información	Custodio del Activo de Información	Usuario de un activo de información	Administrador de seguridad Física	Gestores Técnicos de Plataforma Tecnológica	Gestores de seguridad informática	Proveedor de Infraestructura Tecnológica - Servicio Especializado	Analista Forense
Gestionar listado de fuentes generadoras de incidentes			**I**	**I**		**C I**	**R**			**R**	**A**	**C**	**C**
Procedimientos de gestión de incidentes de seguridad de la información y Capacitación													
Crear procedimientos necesarios para atención de incidentes de seguridad de la información			**A**	**R**		**C I**	**R**			**R**	**R**	**C**	**C**
Clasificar y priorizar los incidentes de seguridad		**C**	**A**	**R**		**R**	**R**						
Identificar indicadores de incidentes		**C I**	**A**	**R**		**R**	**R**						
Diseñar e implementar programas de capacitación incidentes de seguridad de la información		**C**	**A**	**R**		**I**	**I**			**I**	**I**	**I**	**I**

						Primera Línea de Defensa							
	Usuario sensibilizado	Comité de Gestión y desempeño	Líder del Sistema de Gestión de Seguridad de la Información	Líder del Grupo de Respuesta de Incidentes	Agente Primer punto de contacto Mesa de Ayuda	Dueño del Activo de Información	Custodio del Activo de Información	Usuario de un activo de información	Administrador de seguridad Física	Gestores Técnicos de Plataforma Tecnológica	Gestores de seguridad informática	Proveedor de Infraestructura Tecnológica - Servicio Especializado	Analista Forense
Diseñar política de publicación y publicar incidente													
Diseñar política de publicación de Incidentes de Seguridad		**C**	**A**	**R**		**C**							
Publicar incidentes de Seguridad		**C**	**A**	**R**		**C**							
Detectar Incidentes de seguridad													
Reportar incidentes de seguridad de la información	**R**	**R I**	**R I**	**R**	**R**	**A**	**R**	**R**		**R**	**R**	**R**	**R**
Atender incidentes de seguridad													
Escalar incidentes de seguridad de la información			**I**	**A**		**R**	**R**			**R**	**R**	**R**	
Recolectar y analizar evidencia digital			**I**	**R**	**R**	**A**	**R**			**R**	**R**	**R**	**R**
Analizar incidentes de seguridad de la información													

						Primera Línea de Defensa							
	Usuario sensibilizado	Comité de Gestión y desempeño	Líder del Sistema de Gestión de Seguridad de la Información	Líder del Grupo de Respuesta de Incidentes	Agente Primer punto de contacto Mesa de Ayuda	Dueño del Activo de Información	Custodio del Activo de Información	Usuario de un activo de información	Administrador de seguridad Física	Gestores Técnicos de Plataforma Tecnológica	Gestores de seguridad informática	Proveedor de Infraestructura Tecnológica - Servicio Especializado	Analista Forense
Determinar la severidad, clasificar y priorizar los incidentes y tiempos de respuesta			**C**	**A**		**I**	**R**			**R**	**R**	**R**	
Declarar y notificar el incidente de acuerdo con la severidad e impacto. Comunicar anuncios de seguridad		**C I**	**A**	**R**		**C**	**R**						
Mitigar y Remediar incidentes de seguridad de la información (contención y erradicación)													
Ejecutar el plan de acción para contener el incidente de seguridad de la información			**I**	**I**	**I**	**A**	**R**	**R**		**R**	**R**	**R**	
Documentar el incidente de seguridad de la información			**I**	**I**		**A**	**R**			**R**	**R**	**R**	**R**
Consolidar información de incidentes de seguridad de la información			**I**	**A**		**R**	**R**			**R**	**R**	**R**	**R**

						Primera Línea de Defensa							
	Usuario sensibilizado	Comité de Gestión y desempeño	Líder del Sistema de Gestión de Seguridad de la Información	Líder del Grupo de Respuesta de Incidentes	Agente Primer punto de contacto Mesa de Ayuda	Dueño del Activo de Información	Custodio del Activo de Información	Usuario de un activo de información	Administrador de seguridad Física	Gestores Técnicos de Plataforma Tecnológica	Gestores de seguridad informática	Proveedor de Infraestructura Tecnológica - Servicio Especializado	Analista Forense
Contener (hacer análisis de riesgo para evitar vuelva a ocurrir)			I	I		A	R			R	R	R	
Implementar las acciones de mitigación del riesgo		I	I	I		A	R	R		R	R	R	
Actualizar la base de conocimiento con información de experiencias con incidentes anteriores.			I	A	R	I	R			R	R	R	
Gestionar las vulnerabilidades													
Identificar las vulnerabilidades	R	I	I	I		A	R	R	R	R			
Solucionar las vulnerabilidades			I	I		A	R	R	R	R	R	R	
Actualizar la base de conocimiento con la solución de las vulnerabilidades		I	I	A		R	R	R	R	R	R	R	R

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**

ELABORACIÓN Y APROBACIÓN					
ELABORÓ	**REVISIÓN METODOLOGICA**	**APROBÓ**		**Vo.Bo Oficina Asesora de Planeación**	
Jorge Armando Silva Pineda Jaime Enrique Camacho Pardo Jorge Alberto Echeverri	Jeiffe Jubelly Muñoz Robayo	Leyla Zoraya Guzmán Rodríguez	Oficina de Tecnología de la Información	Juan Carlos Torres Rodríguez	Coordinador del Grupo de Arquitectura Organizacional Mejoramiento Continuo o quien haga sus veces
Oficina de Tecnología de la Información – Sistema de Gestión de Seguridad y Privacidad de la información	Oficina Asesora de Planeación.				
Fecha: 03 de Noviembre de 2022	Fecha: 29 de Noviembre de 2022	Fecha: 30 de Noviembre de 2022		Fecha Aprobación: **06 de Diciembre de 2022**	