Guía de apoyo para el Procedimiento Gestión de Incidentes de Seguridad de la Información.

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código: SIG - SSI - PO - 04 - PR - 03 - GI - 02	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

TABLA DE ILUSTRACIONES

RELACIÓN DE TABLAS

1 INTRODUCCION

Describe los lineamientos para poner en marcha el Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto por MINTIC, el cual está concebido para el manejo de los posibles incidentes de seguridad de la información que puedan presentarse al interior de la Superintendencia de Notariado y Registro (SNR).

2 MARCO LEGAL

El presente documento fue elaborado tomando como referencia la Norma Técnica Colombiana NTC-ISO-27001 y la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información No. 21 emitida por el Ministerio de las Tecnologías de la Información MINTIC.

Así mismo, se articulará con lo estipulado en el Decreto 338 del 08 de marzo del 2022. Por el cual se adiciona el Titulo 21 a la parte2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector Tecnologías de la Información y las Comunicaciones, mediante el cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, el Modelo y las instancias de Gobernanza de Seguridad Digital en la sección 5 modelo nacional de atención y gestión de incidentes.

3 OBJETIVO DEL PROCEDIMIENTO.

Definir de manera estructurada las directrices para realizar la gestión (detección, clasificación, análisis, tratamiento, comunicación y cierre) de los eventos e incidentes de seguridad de la información de la Superintendencia de Notariado y Registro.

3.1 OBJETIVOS SECUNDARIOS.

- Establecer pautas para la detección, clasificación, análisis, tratamiento, repuesta, comunicación y cierre de los incidentes de Seguridad de la información en la Superintendencia de notariado y registro.
- Definir roles y responsabilidades al interior de la Superintendencia de Notariado y registro para la gestión de incidentes de seguridad de la información.
- Medir el número y tipo de incidentes relacionados con la seguridad de la información.
- Detectar, clasificar, analizar, tratar, comunicar y cerrar incidentes de seguridad de la información.
- Definir pautas claras para el escalamiento de la gestión de incidentes de seguridad de la información.

- Documentar los incidentes de seguridad de la información para construir con esta información una base de datos de gestión de conocimientos en la que se registre de manera clara las lecciones aprendidas.
- Minimizar los tiempos de recuperación del servicio.
- Cuantificar gastos y pérdidas.
- Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.

4 DESCRIPCIÓN DE LA GUÍA PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

4.1 ALCANCE.

Aplica para los contratistas, funcionarios y terceros que gestionen información de la Superintendencia de Notariado y Registro.

4.2 CONSIDERACIONES.

- Este proceso hace parte de las actividades desarrolladas para la implementación del SGSI en la Superintendencia de Notariado y Registro.
- La gestión de Incidentes se encuentra constituida por un conjunto de procedimientos, guías, y controles que determinan las acciones a seguir para gestionar de manera correcta los incidentes de seguridad de la información que afectan la Superintendencia.
- La gestión de incidentes de seguridad de la información es un proceso dinámico que se apalanca en la experiencia diaria de la atención de eventos e incidentes de seguridad al interior de la Superintendencia.
- La gestión de incidentes es proceso que es parte activa tanto de la gestión de servicios tecnológicos como de la gestión de la seguridad de la información.

Área Responsable: Oficina de Tecnologías de la Información (OTI) de la superintendencia de notariado y registro.

4.3 FASES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION.

El presente documento que apoya el procesamiento de gestión de incidentes de seguridad de la información, plantea una serie de actividades para dar cumplimiento al ciclo de vida de la gestión y respuesta a los incidentes de seguridad recomendado por MINTIC:

Ilustración 1 FASES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Fuente: Guía No.21 Seguridad Privacidad de la Información - MINTIC

4.3.1 PREPARACIÓN

Es la fase con la que se dispone a anticiparse a la ocurrencia de los incidentes. Para atender los objetivos de la misma, la Superintendencia de Notariado y Registro, cuenta con herramientas tecnológicas de monitoreo que le permiten identificar y repeler diferentes tipos de incidentes que se puedan presentar. Así mismo, cuenta con un conjunto de medidas de protección base, derivadas de los controles aplicables a cada uno de los dominios de seguridad según la Norma ISO 27001:2013.

De la misma manera se ha establecido como línea base de defensa la formulación de la atención de incidentes a través de este documento, con lo cual se busca mejorar la arquitectura de seguridad de la entidad

.

4.3.1.1 CRITERIOS DE CLASIFICACIÓN DE UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

La Gestión de Seguridad de la Información mediante la relación del impacto del incidente asociado con la importancia del recurso, preserva la metodología para la medición de Riesgo que se contemplada en la metodología de Riesgos de la Entidad, así como a la guía para la identificación de riesgos, oportunidades, evaluación del diseño y efectividad de controles - para riesgos de gestión de procesos o seguridad de la información.

Teniendo en cuenta que los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad o disponibilidad".

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Los criterios para clasificar los incidentes estarán determinados por:

4.3.1.2 IMPACTO DEL INCIDENTE.

El impacto del incidente Identifica las implicaciones tanto técnicas como operacionales del proceso en caso de presentarse un incidente de seguridad. Así mismo, permite identificar que tan crítico es el activo de información que puede afectar el incidente y la afectación en la operación de la Superintendencia de Notariado y Registro.

Para identificar el nivel de impacto del incidente se han definido las siguientes escalas:

INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTROFICO (5)
Sin afectación de la integridad	Afectación leve de la integridad	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros
Sin afectación de la disponibilidad	Afectación leve de la disponibilidad.	Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.
Sin afectación de la confidencialidad	Afectación leve de la confidencialidad	Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación muy grave confidencialidad de la información

Tabla 1 IMPACTO DEL INCIDENTE

4.3.1.3 CRITICIDAD DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La criticidad para la valoración de los incidentes de seguridad de la información está definida según la matriz de probabilidad e impacto, basado en la guía para la Administración del Riesgo y Oportunidades tal como se ilustra a continuación:

CRITICIDAD DEL INCIDENTE				
Probabilidad de Ocurrencia	**IMPACTO DEL INCIDENTE**			
	MENOR (2)	**MODERADO (3)**	**MAYOR (4)**	**CATASTROFICO (5)**
Casi seguro (Totos los meses)	Medio	Medio	Alto Crítico	Alto Crítico
Probable (cada 6 meses)	Bajo	Medio	Alto Crítico	Alto Crítico
Posible (cada año)	Bajo	Bajo	Medio	Alto Crítico
Rara vez (cada 3 años o más)	Bajo	Bajo	Medio	Medio

Tabla 2 CRITICIDAD DEL INCIDENTE

La criticidad del incidente puede ser:

- ***Alto Crítico:*** El incidente de seguridad afecta activos de información considerados *de impacto catastrófico y mayor* que influyen directamente a los objetivos misionales de la Superintendencia. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre de la Entidad o involucren aspectos legales.

- ***Medio:*** El incidente de seguridad afecta a activos de información considerados de *impacto moderado* que influyen directamente a los objetivos de un proceso determinado.

- ***Bajo:*** El incidente de seguridad afecta a activos de información considerados de *impacto menor e insignificante*, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

4.3.1.4 TIEMPO DE ATENCIÓN DE UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

La atención del incidente de seguridad de la información está determinado por una escala de tiempo, el cual se encuentra establecido según el nivel de criticidad del mismo. Y corresponde al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Toda vez que la solución de los incidentes puede variar dependiendo del caso.

Criticidad del incidente	Tiempo para atención
Alto Critico	2 horas
Medio	1día
Bajo	1 semana

Tabla 3 TIEMPO DE ATENCION DE UN INCIDENTE DE SEGURIDAD

4.3.1.5 CLASIFICACION Y/O TIPO DE INCIDENTES DE SEGURIDAD

Algunos de los incidentes de seguridad que se pueden presentar.

a) Daño o pérdida de información física
b) Daño o pérdida de información digital
c) Pérdida o alteración de registros de base de datos no autorizados
d) Pérdida de dispositivos de almacenamiento de información
e) Mal funcionamiento de dispositivos que interactúan con los sistemas de información
f) Evidencias de correos o comunicaciones sospechosas
g) Denegación del servicio
h) Uso indebido de imagen institucional
i) Presencia de código malicioso malware, Ransomware.

4.3.2 DETECCIÓN Y ANÁLISIS

La detección de un incidente hace referencia a la identificación y validación del mismo. Se debe verificar si se trata de un incidente de seguridad o de un incidente de gestión tecnológica. Si se trata de un incidente de seguridad, se debe tipificar de acuerdo a lo descrito en el numeral 6.1.5 de éste documento. El líder de

seguridad de mesa de ayuda debe identificar si se trata de un incidente crítico, lo cual debe identificar según lo descrito en la guía del procedimiento.

Si se trata de un incidente de seguridad de connotación crítica, debe convocar al equipo de gestión de incidentes, quienes deben solucionar en los tiempos establecidos para incidentes de dicha connotación y proceder a realizar la documentación correspondiente según la información recolectada y la solución al mismo.

El Oficial de seguridad y Jefe de la Oficina de Tecnologías de la Información informaran al Comité Institucional de Gestión y Desempeño acerca del incidente, quienes decidirán si se informa a Entes externos como CCIRT o policía.

4.3.3 CONTENCION, ERADICACIÓN Y RECUPERACION.

La contención busca la detección de los incidentes con el fin de que no se propaguen en la Entidad y puedan generar más daños a la información o a la arquitectura de TI.

Las acciones que se adopten como estrategia para la contención varían según el tipo de incidente y deben ser implementadas en coordinación con la Jefatura de la Oficina de Tecnologías de la información. De igual manera deben ser suficientemente documentadas.

La erradicación, busca remover la causa del incidente y la eliminación de cualquier rastro dejado por el incidente.

Recuperación. Algunas de las operaciones entorno a la recuperación pueden ser las siguientes: Restitución del servicio caído, Restauración de Backups, Reparar el sitio web, Reinstalación del equipo y recuperación de datos.

4.3.4 POST- INCIDENTE

Registrar en la herramienta de Gestión de incidentes las lecciones aprendidas, las medidas tecnológicas, disciplinarias y/o penales que se hayan tomado en desarrollo de la solución al incidente. Con el fin que en caso de presentarse el mismo tipo de incidente se responsa de una manera eficaz.

4.4 ROLES PERFILES Y RESPONSABILIDADES

A continuación, se describen los perfiles y responsabilidades de quienes pueden intervenir ante un incidente de seguridad.

1. Usuarios

2. Oficial de Seguridad

3. Comité Institucional de Gestión y Desempeño
   Este grupo multidisciplinario compuesto por:
   a) Secretario General.
   b) Superintendente Delegado para el Registro.
   c) Superintendente Delegado para el Notariado.
   d) Superintendente Delegado de Tierras
   e) Jefe Oficina Jurídica.
   f) Jefe Oficina Asesora de Planeación.
   g) Jefe Gestión Documental.
   h) Jefe Oficina de Recursos Humanos

4. Equipo de respuesta a Incidentes de seguridad. El cual está conformado por los profesionales que ocupan los siguientes cargos:

   a) Jefe Oficina de Tecnologías de la Información.
   b) Coordinador de Sistemas de Información.
   c) Coordinador de Innovación y Desarrollo
   d) Coordinador de Servicios Tecnológicos.
   e) Oficial de Seguridad.
   f) CSO - Chief Security Officer – Física y Tecnológica.
   g) Líder de Bases de Datos
   h) Líder de Redes e infraestructura.
   i) Líder de comunicaciones.
   j) Líder del portal Institucional e Intranet.

   Este equipo es considerado un componente fundamental de los programas de respuesta a incidentes y actúa como una herramienta de experiencia en el establecimiento de recomendaciones para el aseguramiento de los sistemas de información y la plataforma que los soporta.

- **Información de Contacto:** Se cuenta con la lista de los funcionarios que hacen parte de equipo de atención a incidentes de seguridad de la información, la cual contiene el nombre, correo electrónico y número telefónico. En caso de ausencia temporal o definitiva son reemplazados por otro funcionario quien desempeñará las funciones correspondientes.

- **Información de Escalamiento:** El Jefe de la Oficina de Tecnologías de la Información y el Oficial de seguridad de la Información, escalaran al Comité Institucional de Gestión y Desempeño, el incidente de seguridad dependiendo de su impacto y criticidad. Dicho comité autorizará cuales incidentes pueden ser comunicados a los medios y cuáles no. Así mismo, autorizará comunicar a los grupos de interés como CCP - Policía Nacional, Fiscalía, CCIRT entre otras.

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**	