1. OBJETIVO

El objetivo principal de esta guía de gestión de Incidentes de seguridad es tener un enfoque estructurado y bien planificado que permita a SuperSociedades:

a) Administrar eventos tecnológicos e incidentes de seguridad de la información
b) Definir roles, responsabilidades y tiempos de respuesta para incidentes.
c) Implementar un proceso de documentación y mejora continua basado en lecciones aprendidas.
d) Garantizar el cumplimiento normativo y la coordinación con entidades como CSIRT Gobierno, COLCERT y el Comando Conjunto Cibernético.
e) Definir y facilitar el reporte, registro, tratamiento para dar respuesta de la manera más eficiente y adecuada.
f) Definir los mecanismos que permitan monitorear los tipos, volúmenes de los incidentes o eventos de seguridad de la información, a través de los indicadores del sistema.

Estos eventos e incidentes pueden ocurrir en el procesamiento de los datos e información de la entidad o de las entidades con la que se tenga una relación de supervisión.

2. ALCANCE

Este procedimiento aplica desde la notificación de un evento o incidente de seguridad hasta su cierre, abarcando activos de información, tecnología y procesos organizacionales. Se deben considerar todos los incidentes documentados en el Catálogo de Incidentes - Taxonomía.

3. RESPONSABILIDADES

- De acuerdo con el documento *GIN-PO-001 Políticas del SGI*, Todos los funcionarios, contratistas y terceros deben reportar eventos o incidentes.
- La Mesa de Servicios es responsable del registro y clasificación inicial del incidente.
- Si los incidentes reportados se valoran como GRAVE O MUY GRAVE, deben ser informados inmediatamente después de la evaluación, al CSIRT

gobierno/COLCERT - Resolución No. 500 de MINTIC, para recibir el apoyo, acompañamiento y coordinación.

- En el caso de incidentes de seguridad en donde se vea comprometida la información de datos personales, se debe realizar el correspondiente reporte a la Super Intendencia de industria y comercio de acuerdo con el procedimiento por ellos definido y la Política de tratamiento de datos personales de la Superintendencia de Sociedades.
- La comunicación de las responsabilidades de cada funcionario de la Entidad se realiza a través de los manuales de funciones, procedimientos e instructivos previstos para tal fin, las responsabilidades frente a los incidentes de seguridad de la información se encuentran definidos en el documento GIN GU-004 GUÍA PARA EL USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN.

4. DEFINICIONES

- **ACTIVOS TECNOLÓGICOS:** Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos por su Dirección. Se pueden estructurar en las siguientes categorías: Software, Hardware, Servicios, Datos, Personal, Proveedores, instalaciones físicas, Comunicaciones, Equipamiento auxiliar.
- **CONFIDENCIALIDAD:** Garantía que la información sea accedida únicamente por usuarios y procesos autorizados.
- **CONTROL:** Medida que permite garantizar la reducción del nivel de un riesgo específico o mantenerlo dentro de límites aceptables.
- **DISPONIBILIDAD:** Garantía que los usuarios y procesos autorizados tengan acceso a los activos de información cuando los requieran.
- **EVENTO**: Suceso que puede ocurrir en un espacio y tiempo específico, generando impactos sobre los activos tecnológicos y activos del negocio. Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del proceso, del servicio o de los recursos tecnológicos que indican un incumplimiento posible de las políticas de seguridad de la información o de las políticas operacionales, una falla de las medidas de seguridad tomadas o una situación previamente desconocida que genera riesgos para la entidad.
- **EVENTOS DE SEGURIDAD DE LA INFORMACIÓN:** Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad y disponibilidad de los datos.

- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Es la materialización de eventos de acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

- **INFORMACIÓN**: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
- **IMPACTO**: Daño producido a la organización por la materialización de un riesgo sobre los activos tecnológicos, visto como diferencia en las estimaciones de los estados de seguridad obtenidas antes y después del evento.
- **INTEGRIDAD:** Condición de seguridad que garantiza que la información es actualizada, en todo su ciclo de vida, sólo por el personal y procedimientos autorizados.
- **REGISTRO DE EVENTOS:** En ingles Logs. Mecanismo mediante el cual se guarda en un archivo (generalmente de texto) toda la información correspondiente a las actividades o eventos de un determinado sistema, dispositivo o equipo.
- **RIESGO:** Probabilidad o posibilidad de que una amenaza aprovechando la vulnerabilidad o vulnerabilidades de un sistema, equipo o cualquier otro tipo de activo, se concrete, causando daños, perjuicios o pérdidas a la organización propietaria del mismo.
- **SEGURIDAD DE LA INFORMACIÓN:** Actividad que regula la protección de los recursos tecnológicos de una entidad a través de políticas, normas, procedimientos y estándares.
- **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:** Parte del sistema de gestión general de una organización, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **SISTEMA DE INFORMACIÓN:** Conjunto de datos, aplicaciones y equipos que de manera conjunta proveen a la empresa la información necesaria para la ejecución de las tareas y la toma de decisiones de los niveles estratégico, táctico y operativo.
- **TRAZABILIDAD:** Conjunto de medidas, acciones y procedimientos que permiten registrar, identificar y realizar seguimiento a los incidentes en cada producto desde su origen hasta su respuesta final.

5. CONTENIDO

5.1. ACTIVIDADES PARA LA GESTIÓN DE INCIDENTES.

La gestión de incidentes de seguridad involucra un conjunto ordenado de acciones enfocadas a prevenir, en la medida de lo posible, la ocurrencia de incidentes y en caso de que ocurran, restaurar los niveles de operación lo antes posible. El proceso de gestión de incidentes consta de diferentes fases y, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea

- Preparación
- Identificación
- Contención
- Mitigación
- Recuperación
- Post-Incidente

5.1.1. PREPARACIÓN

Esta fase dentro del ciclo de vida de la Gestión de Incidentes se realiza teniendo en cuenta dos aspectos:

a. La respuesta a los eventos tecnológicos y a los incidentes de seguridad que se presentan comúnmente en el diario trascurrir del procesamiento de datos y en la prestación de los servicios tecnológicos.

b. La prevención de los eventos tecnológicos y de los incidentes de seguridad ya que muchos de estos sucesos pueden ser detectados, evaluados y gestionados con anterioridad, mediante el monitoreo de eventos, la gestión de las vulnerabilidades en los activos de información, el parcheo de sistemas operativos, ayudando a que el hardware, software, redes, datos y procesos sean lo suficientemente seguros.

Esta fase debe ser apoyada por los responsables de la administración de la infraestructura tecnológica, a través de la implementación de las políticas establecidas en el GIN-PO-001_DocumentoPoliticasSGI y el GIN-PO-003 Políticas de Seguridad y Privacidad de la Información del SGSI y las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones, entre los que se encuentran:

- Gestión de Parches de Seguridad: A través de la gestión oportuna de las vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, Otro Software Instalado).
- Aseguramiento de plataforma: Asegurar correctamente la plataforma tecnológica antes de salir a producción y configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios internos como externos. Revisión de configuraciones por default (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el registro de eventos.
- Seguridad en redes: Realizar una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.
- Prevención de código malicioso: Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas actualizadas al día.
- Sensibilización y entrenamiento de usuarios: Los usuarios en SUPERSOCIEDADES incluidos los administradores de TI deben ser sensibilizados sobre seguridad digital de acuerdo con las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad. Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos, así mismo se realizarán ejercicios o entrenamientos sobre fraudes o amenazas existentes a través de situaciones simuladas lo que permite conocer las amenazas actuales que pueden afectar a los sistemas de información y los mecanismos existentes que pueden servir para combatir las amenazas.
- La gestión de cambios: La actualización de activos de información (hardware, software, redes, datos, procesos, instalaciones y personas), deben estar sujetos a la autorización previa, a las pruebas antes de su despliegue y a la actualización de la documentación relacionada.
- Monitoreo de eventos de seguridad sobre la plataforma tecnológica por medio de un servicio de monitoreo y alertamiento en tiempo real.

Las actividades descritas anteriormente buscan prevenir la ocurrencia de incidentes de seguridad sobre la infraestructura soportada por TI, y adicionalmente es necesario realizar una evaluación periódica (semanal, mensual, semestral, anual) a través de indicadores.

5.1.2. Recursos de Comunicación

Los elementos necesarios para la comunicación del equipo de atención de incidentes dentro de la entidad son:

- Información de Contacto: En el Anexo No.1 de esta guía se establece la lista de contactos de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.
- Información de Escalamiento: El escalamiento de los incidentes se encuentra establecido en el Catálogo de incidentes gestionada por la Mesa de servicio
- Información de los administradores de la plataforma tecnológica (Servicios, Servidores)
- Contacto con el área de recursos humanos o quien realice sus funciones (por si se realizan acciones disciplinarias).
- Los equipos externos (contacto con áreas interesadas o grupos de interés) que pueden ser contactados en la atención de incidentes y que pueden apoyar la resolución de los incidentes de seguridad o ciberseguridad se encuentran documentados en el Anexo No.1 de este documento.

La Comunicación hacia la ciudadanía se encuentra establecida de acuerdo con el documento GCO-PG-002 Plan Estratégico de Comunicaciones, en donde se encuentra establecida la política de comunicación externa.

5.1.3. Notificación de eventos e Incidentes de Seguridad

A continuación, se describen las actividades de notificación de los eventos e incidentes de seguridad:

Un usuario, un tercero o un contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo al primer punto de contacto definido por la entidad Centro de Servicios Tecnológicos, o al correo Servicios.tecnologicos@supersociedades.gov.co o a través de la línea telefónica 601-2201000 opción 1 Ext.911.

El primer punto de contacto recibe el evento y realiza una catalogación de acuerdo con la 5.1.5. Clasificación de Eventos y lo escalan al administrador de la plataforma de seguridad, para identificar si el evento se trata de un falso positivo o un incidente de seguridad.

El primer punto de contacto será el encargado de realizar la asignación de las tareas requeridas para la atención y tratamiento del evento y realiza el seguimiento hasta su cierre definitivo.

El administrador de la plataforma de seguridad identificará el tipo de incidente o evento (de acuerdo con la tabla clasificación de incidentes o eventos numeral 5.1.5. Clasificación de incidentes y/o eventos. Validará si el evento reportado corresponde a un incidente de seguridad o está relacionado con requerimientos propios de la infraestructura de TI.

En caso de que el evento sea clasificado como incidente de seguridad, se notificará de manera inmediata a la Coordinación del Grupo de Seguridad e Informática Forense (GSIF) y al Oficial de Seguridad de la Información, con el propósito de coordinar la atención y definir los recursos humanos y técnicos que conformarán el equipo responsable de su gestión.

De acuerdo con la naturaleza, alcance y criticidad del incidente, se realizará el escalamiento correspondiente a los administradores de las plataformas o sistemas involucrados, quienes integrarán el Equipo de Respuesta a Incidentes y ejecutarán las acciones necesarias para su contención, análisis, erradicación y recuperación.

El/la Coordinador(a) del grupo GSIF será responsable de informar al director de la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), a fin de que se comunique oportunamente a la Alta Dirección de la entidad, se activen los canales de comunicación institucionales y se adopten las decisiones estratégicas pertinentes, en articulación con las demás áreas de la entidad y, cuando aplique, con las partes interesadas externas.

Toda la información inicial debe ser documentada en el Formato: GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información, en colaboración con todos los intervinientes en la resolución del incidente.

Si el incidente de seguridad es identificado por otra línea diferente a un usuario de la entidad, a través de los elementos de detección o administradores de TI, este es notificado al centro de servicios tecnológicos para que siga el flujo establecido anteriormente.

El director de la Dirección de Tecnología de la información y las comunicaciones tendrá la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad.

5.1.4. Registro y documentación de Incidentes

Los elementos necesarios para el registro de los incidentes que se reportan (ya sea por parte interna de la Dirección de Tecnología de la Información y las Comunicaciones o por parte de los usuarios) son:

a) Los eventos o incidentes son escalados a través del Centro de Servicios tecnológicos y teniendo en cuenta la clasificación que se relaciona a continuación son atendidos por los profesionales de segundo y tercer nivel quienes deben realizar el análisis preliminar, la investigación y la respuesta y cierre de los eventos tecnológicos e incidentes de seguridad. Así mismo, se debe mantener el registro o ticket abierto con el fin de llevar un registro histórico que servirá de base para la medición de los indicadores de gestión de las actividades de incidentes y eventos y tomar acciones y lecciones aprendidas de todo lo ocurrido.

b) Para el registro de la información del incidente presentado, el tratamiento y el conocimiento resultante de la investigación y de las acciones realizadas, se debe utilizar el Formato GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información, en el cual, debe quedar documentando por parte de todos los implicados, el tratamiento y resolución del incidente.

5.1.5 Clasificación de incidentes y/o eventos

Para realizar la evaluación de un evento tecnológico y/o un evento o incidente de seguridad se debe tener en cuenta los niveles de clasificación, para lo cual se adopta la TAXONOMÍA CLASIFICACIÓN CIBERINCIDENTES suministrado por el Colcert.

CATALOGO DE INCIDENTES TAXONOMÍA[1]			
Clasificación	**Definición**	**Tipo de incidente**	**Descripción**
Contenido abusivo	Ataques destinados a dañar la imagen	**Spam**	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje compartido.

[1] Taxonomía para Reporte de Incidentes al CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno

CATALOGO DE INCIDENTES TAXONOMÍA[1]			
Clasificación	**Definición**	**Tipo de incidente**	**Descripción**
	de la organización o utilizar sus recursos electrónicos para usos ilícitos (como publicidad, extorsión o ciberdelincuencia en general)	**Delito de odio**	Contenido difamatorio o discriminatorio. Ej: Ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos o grupos.
		Materiales de abuso/explotación sexual infantil, contenido sexual o Violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	Incidentes relacionados con actividades maliciosas, aplicaciones y archivos dañinos para obtener acceso no autorizado al sistema para sustraer, exfiltrar, eliminar, modificar su información privada que pretenden acceder a sus datos.	**Sistema infectado**	Sistema infectado con malware. Ej: Sistema, computador, dispositivos móviles infectado con un rootkit
		Servidor C&C (Comando y Control)	Conexión con servidor de Comando y Control (C&C) mediante malware o sistemas infectados.
		Distribución de malware	Recurso usado para distribución de malware. Ej: Recurso de una organización empleado para distribuir malware.
		Configuración de malware	Recurso que aloje archivos de configuración de malware Ej: Ataque de webinjects para troyano.
Obtención de información	Incidentes relacionados con la identificación y recopilación de información de personas,	**Escaneo de redes (scanning)**	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: Peticiones DNS, ICMP, SMTP y escaneo de puertos.

CATALOGO DE INCIDENTES TAXONOMÍA[1]			
Clasificación	**Definición**	**Tipo de incidente**	**Descripción**
	infraestructura tecnológica y activos de información de una organización a través de técnicas no autorizadas con fines delictivos.	**Análisis de paquetes (sniffing)**	Observación y grabación del tráfico de redes.
		Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: Mentiras, trucos, sobornos, amenazas.
Intento de intrusión	Incidentes relacionados con la utilización de técnicas que intentan atacar una infraestructura tecnológica o un activo de información aprovechándose de una vulnerabilidad para obtener el control y privilegios administrativos o de ejecución.	**Explotación de vulnerabilidades conocidas**	Compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: Desbordamiento de buffer, puertas traseras y cross site scripting (XSS).
		Acceso con vulneración de credenciales	Múltiples intentos y vulneración de credenciales. Ej: Intentos de ruptura de contraseñas, ataque por fuerza bruta.
		Ataque desconocido	Ataque empleando exploit desconocido
Intrusión	Ataques que aprovechar las vulnerabilidades de diseño, funcionamiento o configuración de las diferentes tecnologías, para entrar de forma fraudulenta a los sistemas de una	**Compromiso de cuenta con privilegios**	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
		Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
		Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades del software. Ej: Inyección SQL y defacement.
		Robo	Intrusión física. Ej: acceso no autorizado a Centro de

CATALOGO DE INCIDENTES TAXONOMÍA[1]			
Clasificación	**Definición**	**Tipo de incidente**	**Descripción**
	organización		Procesamiento de Datos.
Disponibilidad	Interrupción de la capacidad de procesamiento y respuesta de los sistemas y redes para dejarlos inoperativos Acción premeditada para dañar un sistema, interrumpir un proceso, cambiar o borrar información.	**DoS (Denegación de Servicio)**	Ataque de denegación de servicio. Ej: Envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
		DDoS (Denegación Distribuida de Servicio)	Ataque de Denegación Distribuida de Servicio. Ej: Inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
		Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
		Sabotaje	Sabotaje físico. Ej: Cortes de cableados de equipos, desconexión de equipos o incendios provocados
		Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de Información	Incidentes relacionados con el acceso, filtraciones (confidencialidad), la modificación o el borrado (integridad) de información.	**Acceso no autorizado a información**	Acceso no autorizado a información. Ej: Robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
		Modificación no autorizada de información	Modificación no autorizada de información. Ej: Modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
		Pérdida de datos	Pérdida de información Ej: Pérdida por fallo de disco duro o robo físico.
Fraude	Incidentes relacionados Con la pérdida de bienes causada con intención fraudulenta o deshonesta en	**Uso no autorizado de recursos**	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
		Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor.

CATALOGO DE INCIDENTES TAXONOMÍA[1]			
Clasificación	**Definición**	**Tipo de incidente**	**Descripción**
	procura de un beneficio económico para sí mismo, para otra persona o empresa		Ej: Warez
		Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
		Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	Incidentes relacionados con la identificación del grado de debilidad inherente en un sistema de hardware o software que permitan a un atacante realizar actividades no autorizadas a la misma organización o en contra de otra.	**Criptografía débil**	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: Servidores web susceptibles de ataques POODLE/FREAK.
		Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
		Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
		Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
		Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Incidentes no clasificados en la taxonomía existente o amenazas persistentes avanzadas	**Incidente no clasificado**	Incidentes que no se ajustan a la clasificación existente, actuando como indicador para la actualización de la clasificación.
		APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

EVENTOS: Los eventos se encuentran registrados en la herramienta dispuesta para tal fin por parte de la DTIC

CATALOGO DE EVENTOS				
ID	**Categoría**	**Subcategoría**	**Descripción**	**Tipificación**
CAT 1	Investigación	Eventos potencialmente maliciosos o actividad sospechosa que requieren una investigación		Tarea
CAT 2	Intento de actividad no satisfactoria	Mal uso y/o abuso de los servicios informáticos, Violación de las normas y uso de internet	Intentos deliberados para obtener acceso no autorizado o evadir un control	Evento
CAT 3	Incumplimiento de actividad / política	Manipulación indebida de la planta eléctrica, UPS, dispositivos eléctricos o electrónicos	No ejecución de una actividad que potencialmente aumenta la exposición de riesgo	Evento
CAT 4	Reconocimiento	Sniffers (software utilizado para capturar información que viaja por la red) - Escaneo de vulnerabilidades	Actividad que busca obtener información de los sistemas, aplicaciones, redes o usuarios	Evento
CAT 5	Disponibilidad	Eventos de indisponibilidad de servicios tecnológicos que impiden la prestación de los servicios	Eventos masivos de No disponibilidad de los servicios tecnológicos	Evento
CAT 6	Actividad Explicada	Eventos sospechosos que posterior a una investigación se determinan que no son maliciosos (falso positivo)		N/A

5.1.6. Impacto o Severidad

Con el fin de permitir una atención adecuada a los incidentes se debe determinar el nivel de impacto de este, y de esta manera atenderlos adecuadamente según la necesidad. Para medir el impacto potencial y la prioridad se deben tener en cuenta las siguientes actividades:

- Evaluar a que activos está afectando
- Determinar el valor o importancia dentro de la entidad y del proceso que Soporta el o los sistemas afectados.
- Analizar información resultante del incidente

Con la información anterior se debe medir el impacto de acuerdo con las siguientes categorías:

MUY GRAVE	GRAVE	MENOS GRAVE	MENOR
* De alta importancia para la Entidad, se requiere una decisión estratégica inmediata * No existe estructura de control o se violaron los controles * Interrupción de todas las intendencias regionales a nivel Nacional y la sede central superior a 4 horas. * Sanciones económicas por incumplimiento repetitivo de las normas establecidas por los entes reguladores * Imagen negativa sostenida por mal servicio	* Estructura de control débil, los controles no mitigan la probabilidad o la consecuencia adecuadamente. * Interrupción de algunas intendencias regionales o la sede central superior a 4 horas *Observaciones por incumplimiento de las normas establecidas por los entes reguladores que generen un plan de acción a corto plazo. *Afectación de la imagen por el servicio ineficaz o inoportuno. *Inoportunidad de la información ocasionando retrasos en las labores de las áreas, respuesta a los entes reguladores y a los aprendices mayor a	*Existen algunos controles, pero no son los suficientes. *Interrupción de las operaciones en las intendencias regionales a nivel nacional o sede central entre 2 a 4 horas. *Reproceso de actividades y aumento de la carga operativa entre 24 a 36 horas. *Acceso fraudulento a los sistemas de información a nivel local. * Pérdidas económicas	*La estructura de control actual es susceptible de mejoras. *Interrupción de las operaciones en las intendencias regionales o la sede central menor a 2 horas. *Intentos de acceso no autorizado a los sistemas de información. * La estructura de control es adecuada *No hay interrupción de las operaciones *No genera sanciones económicas y/o administrativas *No afecta la oportunidad de la información

MUY GRAVE	GRAVE	MENOS GRAVE	MENOR
* Pérdida de información reservada de la entidad * Fraude importante y exitoso, sistemas de información Core totalmente comprometidos y/o vulnerados * Pérdidas económicas * Pérdida de vidas humanas	36 horas. * Pérdidas económicas		*Debilidad o amenaza de seguridad de la información * No se presentan pérdidas económicas * Daños pequeños de la infraestructura de la entidad.

5.1.7. Priorización de los Incidentes.

Con el fin de permitir una atención adecuada a los incidentes se debe determinar el nivel de prioridad y de esta manera atenderlos adecuadamente según la necesidad. El nivel de prioridad está ligado con el impacto del evento tecnológico y/o del incidente de seguridad.

NIVEL PRIORIDAD	DEFINICIÓN
BAJA	Sistemas no críticos que apoyan a funcionarios y a una sola dependencia.
MEDIA	Sistemas que apoyan más de una dependencias o proceso de la entidad
ALTA	Sistemas y activos de información críticos que sostienen servicios misionales

5.1.8 Tiempos de Escalamiento y Respuesta

Para el caso de la atención de incidentes de seguridad se han establecido unos tiempos máximos de atención, con el fin de atenderlos adecuadamente de acuerdo con su criticidad e impacto. Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo

en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Impacto	**Tiempo máximo de atención**
Muy Grave	≤ 18 horas
Grave	≤ 24 horas
Menos Grave	24 - 48 horas
Menor	3 - 10 días

Rol	**Disponibilidad**	**Tiempo Escalamiento Horario No Hábil**	**Tiempo Escalamiento Horario Hábil**
Coordinador Grupo de Seguridad e Informática Forense -Oficial de seguridad	L-V de 8 am a 5 pm	8 horas	3 horas
Coordinadores DTIC	L-V de 8 am a 5 pm	6 horas	2 horas
Administradores de plataformas (sistemas de información, bases de datos, plataformas de seguridad, servidores, directorio activo)	Según criticidad del caso de uso	4 horas	1 hora
Gestor de Incidentes de Seguridad (SOC)	L-V de 8 am a 5 pm	6 horas	2 horas
Centro de Servicios Tecnológicos	L-V de 8 am a 5 pm	No aplica	30 minutos

5.2. IDENTIFICACION

En esta fase se tiene en cuenta las diferentes fuentes de reporte o detección de eventos tecnológicos materializados y de incidentes o eventos de seguridad.

a. Reporte de usuarios.
   La principal fuente de detección de eventos e incidentes son los funcionarios que hacen uso de los diferentes servicios de la Dirección de Tecnología de la

Información y las Comunicaciones, de los sistemas y aplicaciones para realizar sus labores de actualización y generación de información para la toma de decisiones en los diferentes niveles administrativos.

b. Gestión Administrativa de Infraestructura
La revisión continua del funcionamiento de los activos de información permite prevenir problemas, eventos no deseados e incidentes de seguridad.

c. El monitoreo de infraestructura y los servicios.
Contar con herramientas de monitoreo e indicadores que nos indiquen que posiblemente se ha presentado o se va a presentar un incidente.

Generalmente algunos de estos elementos son:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Reportes de funcionarios de monitoreo
- Informes de Software antivirus
- Funcionamientos de sistemas fuera de lo normal
- Servicios del SOC
- Servicios del NOC
- Análisis de Auditorias de los sistemas y de la infraestructura tecnológica, basados en:
  - Logs de servidores
  - Logs de aplicaciones
  - Logs de herramientas de seguridad

d. Cualquier otra herramienta que permita la identificación de un incidente de seguridad.

Teniendo en cuenta lo establecido en la resolución 500 del 2021 del Ministerio TIC, la cual establece las etapas para la gestión de los incidentes de seguridad digital y el reporte de estos por parte de los sujetos obligados al Equipo de Respuesta a Incidentes de Seguridad Cibernética del sector Gobierno - CSIRT Gobierno y al Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT. Los incidentes catalogados como Muy Grave y Grave de acuerdo con el impacto definido en el numeral anterior, serán notificados por el Oficial de Seguridad de la Información para el respectivo apoyo y coordinación en la gestión, a través del formato de reporte definido por ellos y disponible en la siguiente página web Reportar un Incidente (colcert.gov.co).

Los incidentes catalogados como Menos Grave y Menor pueden ser comunicados al Colcert, si así lo define el Oficial de Seguridad de la Información, en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos a nivel Gobierno.

Según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, se deben realizar los respectivos planes de mejoramiento, para lo cual el Oficial de Seguridad de la Información supervisará y hará seguimiento a su cumplimiento.

Una vez identificado y reportado el evento o incidente, se procede a realizar las actividades de análisis las cuales involucran los siguientes aspectos:

5.2.1. Análisis

Se aclara que los incidentes de seguridad son sucesos que contravienen las políticas de seguridad de la información y/o que generan acciones en contra de los principios de disponibilidad, integridad y confidencialidad de la información.

Los eventos tecnológicos son sucesos que impiden el correcto procesamiento de la información o la no prestación de los servicios tecnológicos. Algunos de estos eventos pueden tomarse como incidentes de seguridad debido al impacto que generan sobre el cumplimiento de los objetivos de los procesos de SuperSociedades.

Teniendo en cuenta el conocimiento que tienen los administradores de los recursos y los usuarios frente al uso de los activos de información y el estado normal de operación de la Superintendencia, cualquier suceso o caso que pueda ser considerado anormal, debe requerir un análisis detallado o en profundidad. Generalmente, solo una pequeña parte de todos los eventos que se procesan por los sistemas son motivo de análisis en detalle y considerados incidentes de seguridad.

Esta fase está muy relacionada con la fase de preparación, ya que existe un constante salto entre ambas. Cuando un evento requiere de un mayor análisis se podría decir que se pasa de la fase de preparación a la fase de identificación, sin embargo, si se descarta el evento, se volvería de nuevo a la fase de preparación hasta que un nuevo evento requiera de mayor atención.

A partir del momento en que se inicia la fase de identificación se recomienda aplicar políticas de confidencialidad y considerar el principio de “necesidad de conocer”, compartiendo la información solamente con aquellas personas implicadas que

realmente necesiten conocerla. Las comunicaciones cifradas y el almacenamiento seguro de la información se deben tener en cuenta también a partir de este momento.

Resulta imposible disponer de playbooks o guías para gestionar todos los incidentes que pueden llegar a materializarse, sin embargo, existen unos vectores de ataque comunes que ayudan a identificar un incidente de seguridad, determinar su alcance y los sistemas afectados. Algunos vectores habituales que merecen especial atención son:

Correo electrónico: Los ataques de suplantación de identidad a través de correo electrónico (spear, phishing) han resultado ser una técnica con un elevado porcentaje de éxito y son ampliamente utilizados. Este tipo de ataques puede contener enlaces o ficheros adjuntos maliciosos.

Vulnerabilidades conocidas: Las vulnerabilidades en gestores de contenidos, componentes, módulos, componentes, aplicaciones web y software en general, incluido el propio sistema operativo, pueden suponer, además del acceso no autorizado a los sistemas, el robo de información sensible, credenciales u otra información que puede ser utilizada en combinación con alguna otra técnica para lograr un ataque exitoso.

Dispositivos de almacenamiento externo: Los dispositivos de almacenamiento masivo que se conectan a través de USB son un vector de ataque que debe tenerse en cuenta durante la identificación de un incidente.

Uso inapropiado de los activos: La instalación de programas no autorizados, el acceso a páginas web de dudosa legalidad o los posibles descuidos al utilizar documentación clasificada o reservada son un origen común de numerosos incidentes.

Pérdida o robo de activos: La pérdida o robo de documentación o de dispositivos que no cuentan con las medidas de seguridad apropiadas como el borrado remoto o el cifrado de información.

Vectores externos: Algunos ataques, como sabotajes o los ataques de fuerza bruta, son causa de problemas relacionados con la disponibilidad de los servicios.

Recursos para el Análisis de Incidentes

- Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Tener un diagrama de red para tener la ubicación rápida de los recursos existentes

- Línea Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Se debe tener un análisis del comportamiento de red estándar en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

Una vez que se han considerado los vectores del ataque, se pueden emplear diferentes fuentes de información que ayuden a identificar el origen de un posible incidente y su alcance. Por ejemplo:

A nivel de red:

- Registros de conexiones realizadas a través de sistemas proxy.
- Registros de conexiones autorizadas por los cortafuegos.
- Registros de intentos de conexión que han sido bloqueadas en los cortafuegos.
- Trazas de red que muestren conexiones a destinos, puertos o a través de protocolos no esperados, así como picos de tráfico anómalos o en horarios no habituales.
- Conexiones que tengan como origen o destino nodos de la red TOR o activos que aparezcan en listas de reputación como potencialmente maliciosos.
- Sistemas de correlación de eventos de seguridad (SIEM).
- Sistemas en red de detección/prevención de intrusos (NIDS/NIPS).
- Sistemas en red de prevención de fugas de información (NDLP).

A nivel de equipo:

- Registros de sistemas locales de detección/prevención de intrusos (IDS/IPS)
- Cuentas de usuario inusuales en el sistema, especialmente aquellas con privilegios administrativos.
- Ficheros ocultos o con tamaños, nombres o ubicaciones sospechosas, pudiendo indicar los mismos algún tipo de fuga de información o almacenamiento por parte de algún malware.
- Ficheros con permisos inusuales, con SUID o SGID en rutas no habituales, ficheros huérfanos y que pudieran determinar algún tipo de intrusión o rootkit.
- Entradas sospechosas en el registro, principalmente en el caso de infecciones por malware en sistemas Windows, donde ésta es una de las técnicas habituales utilizadas por el malware para asegurar la persistencia en el sistema comprometido.
- Registros de auditoría y accesos no autorizados.

- Sistemas locales de prevención de fugas de información (DLP).
- Procesos y servicios inusuales, no sólo servicios a la escucha, sino también conexiones establecidas a puertos o host extraños, poco habituales o incluidos en algún tipo de lista negra de servidores de Comando y Control (C&C) utilizados por botnets.
- Una carga excesiva de disco o memoria puede estar producida por un incidente de seguridad como malware, denegaciones de servicio o intrusiones.
- Sesiones abiertas en la máquina desde otros equipos, anomalías en las tablas ARP, carpetas compartidas inusuales o con permisos excesivos, o un elevado número de conexiones con algún flag TCP activado de manera anómala y que pudiera evidenciar un ataque.

En el caso de equipos de usuario o terminales móviles, pueden indicar algún tipo de infección en el sistema, entre otros:

- Comportamiento anómalo de alguna aplicación, ventanas emergentes del navegador, conexiones muy lentas, reinicios o aplicaciones que se cierran sin motivo.
- Tareas programadas o actividad sospechosa en los registros de auditoría y logs que indique un funcionamiento anormal del sistema o intentos de intrusión en algún servicio, por ejemplo, mediante fuerza bruta.
- Registros de consolas antivirus o de alguna herramienta habitualmente instalada en el sistema para la identificación de rootkits, de control de integridad de ficheros, firma de los binarios, etc.
- Registros de consolas antispam.
- Anomalías o condiciones reportadas por otros usuarios.

A nivel de aplicación:

- Registros de auditoría y accesos no autorizados.
- Registros o logs de aplicaciones que puedan recoger información de interés, como fechas, transacciones o actividad de los usuarios.

Existen otro tipo de fuentes externas que proporcionan información que debe ser considerada:

- Anomalías o condiciones reportadas por otros usuarios externos a la organización.
- Información sobre nuevos exploits o vulnerabilidades reportadas por fabricantes, proveedores de servicios u otros equipos de respuesta como Colcert.
- Información disponible públicamente a través de redes sociales, en muchos casos relativas a campañas de actividades hacktivistas.

- Conviene comprobar siempre aquellos sistemas con configuraciones similares a los afectados, ya que un atacante podría utilizar una misma técnica de intrusión en diferentes equipos.

Conocer cuál es el estado normal de operación ayudará a detectar anomalías que pueden requerir de un análisis en detalle.

También es importante no caer en una falsa sensación de seguridad causada por la existencia de tecnologías de protección, ya que éstas no son infalibles.

Cada vez que se presente un incidente se deberá revisar si existe una guía de contención de este o en su defecto se deberá crear o actualizar de acuerdo con el tratamiento que se le dé a este; estas guías deberán ser revisadas al menos una vez al año; Esta actividad será desarrollada por el servicio SOC, o por la persona encargada de la atención de los incidentes del grupo GSIF.

En este punto se consideran los elementos básicos para la contención de un posible incidente, Backup de Información, imágenes de servidores, y cualquier información base que pueda recuperar el funcionamiento normal del proceso o servicio.

5.3. CONTENCIÓN

Es importante para la SuperSociedades implementar una estrategia que permita tomar decisiones oportunamente, para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Una vez identificados los elementos que hacen parte del incidente de forma inicial, así como posibles servicios afectados, se procede a establecer acciones que permitan aislar, detener y/o contener los elementos que pueden generar el incidente, a través del aislamiento de equipos de la red, bloqueo de comunicaciones y puertos, congelamiento de procesos, entre otros, estas dependerán del incidente a contener.

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:

- Criterios Forenses
- Daño potencial y hurto de activos
- Necesidades para la preservación de evidencia
- Disponibilidad del servicio
- Tiempo y recursos para implementar la estrategia

• Efectividad de la estrategia para contener el incidente (parcial o total)
• Duración de la solución

La Entidad ha identificado las más comunes y se han creado guías o playbooks para la contención de:

- Ciberataque
- Malware (Adware, virus, gusanos, troyanos)
- Phishing
- Ransomware
- Defacement
- Modificación de Portales
- Correo Spam

Con las acciones antes mencionadas se busca evitar la afectación de otros elementos que hacen parte de la red, infraestructura e incluso evitar el impacto a procesos y actividades de la Superintendencia.

Al desarrollarse las labores de contención es necesaria la participación de responsables de infraestructura tecnológica, soporte e incluso puede llegar a requerirse la intervención de terceros externos a la operación, si las causas del incidente sólo pueden contenerse con acciones al exterior de la Superintendencia, como por ejemplo un ataque de denegación de servicio distribuido, o ataques tipo Zombie, para tal fin se requerirá del personal definido Anexo No.1 de este documento

Las actividades de contención se documentan en el formato GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información.

5.3.1. Investigación

Para una correcta y eficiente gestión de incidentes la SuperSociedades, a través del Grupo de Seguridad e Informática Forense, cuenta con todos los requerimientos y da el soporte en los incidentes de seguridad que llegaren a materializarse a través de los siguientes elementos:

- Portátiles Forenses:
- Analizadores de protocolos.
- Software de adquisición.
- Software para recolección de evidencia.

- Kit de respuesta a incidentes.
- Software de análisis forense.
- Medios de almacenamiento

Durante la investigación se apoyará al personal especializado en la recolección de la evidencia digital, su almacenamiento en el repositorio de evidencias y del suministro de la documentación requerida para ser presentada a los entes legales o autoridades reguladoras, en caso de ser necesario se realizará la recolección de evidencia digital, muestras de datos, tráfico, información volátil de equipos y otros elementos que permitan realizar un análisis exhaustivo que determine las causas que pudieron desencadenar los eventos que se transformaron en incidentes de seguridad, lo anterior siguiendo los lineamientos del procedimiento GTI-PR-012_Extraccion Evidencia Digital, y el uso de herramientas o procedimientos específicos de recolección de datos y evidencia que aporten los insumos para la investigación y así establecer planes de remediación.

Si dentro del análisis se determina un presunto fraude o el incidente que involucra a personal de la Entidad, se notificará al responsable del grupo de Control interno Disciplinario.

Teniendo en cuenta que a lo largo de la investigación es probable determinar otros actores o elementos parte del incidente que inicialmente podrían no haber sido identificados, desde esta misma fase pueden ejecutarse actividades similares a las realizadas en contención con el fin de evitar mayor impacto o propagación de la situación generada por el incidente.

5.4. MITIGACIÓN

Las actividades en torno a la mitigación y remediación del incidente involucran la erradicación de componentes generadores del incidente, establecimiento de configuraciones protegidas, instalación de parches y actualizaciones, en caso de ser requerido, y todas las acciones que busquen cerrar la posible brecha o debilidad que pudo dar pie a la generación del incidente.

Se tiene en cuenta que de acuerdo con los procedimientos de la Superintendencia es necesario surtir procesos como los controles de cambios y solicitud de autorizaciones correspondientes. De acuerdo con el impacto y categorización del incidente o incidentes se determinará si es una situación de emergencia, lo que requeriría un manejo especial y prioritario.

Las acciones de remediación al momento de su implementación o ejecución deben aportar a la restitución de los servicios, evitando generar traumatismos, obstaculización de procesos y por supuesto, evitar generar espacios o condiciones para que se generen nuevos incidentes. Es por lo anterior que las acciones de remediación deben ser planificadas y justificadas para su ejecución, siendo posible en cada caso, contar con el apoyo de fabricantes y agentes externos involucrados con tecnologías que hacen parte del incidente.

Las actividades de remediación que se definan deben quedar documentadas en el GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información.

5.5. RECUPERACIÓN

Desarrolladas las actividades de remediación que han logrado contener de forma permanente las causas generadoras del incidente y que impedirían que éstos se generen nuevamente con las mismas condiciones iniciales (vulnerabilidades, configuraciones débiles, protocolos de comunicación inseguros, etc); El administrador de TI o quien haga sus veces deben restaurar sistemas y/o servicios, aplicaciones y comunicaciones y restablecer la funcionalidad de los sistemas afectados a su estado funcional previo al incidente y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

La reactivación o recuperación de servicios se realiza de forma progresiva analizando comportamiento de cada elemento inicializado detectando comportamientos irregulares o que representen algún peligro o reincidencia generando impacto negativo. Se mantiene monitoreo luego de la recuperación para detectar algún evento como los comentados anteriormente. En caso de reincidir el incidente, se debe volver a la fase de contención e investigación.

Una vez que se recupera el sistema, este debe mantenerse en monitoreo continuo.

Debe existir un plan de contingencia del servicio suficientemente probado en los diferentes escenarios, como apoyo en la restauración de los servicios, sistemas y aplicativos.

Las actividades de recuperación se documentan en el formato GTI-FM-025 Registro y Tratamiento de Incidentes de Seguridad de la Información

5.6. POST-INCIDENTE

Las actividades Post-Incidente básicamente se componen en:

a. Finalizar la documentación del formato GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información, después de que el servicio haya sido reestablecido completamente.
b. El Oficial de Seguridad de la información deberá revisar la completitud del formato GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información, para en caso de que le sea solicitado un informe ejecutivo del incidente presentado. Dicho informe debe contener información detallada del evento tecnológico y/o incidente de seguridad de la información que indique lo que paso, como se resolvió, elementos implicados, las lecciones aprendidas y el tiempo que demoro la solución y el tiempo sin servicio, esto teniendo en cuenta la información registrada en el formato mencionado anteriormente.
c. Se deben actualizar los indicadores de gestión de incidentes.
d. Establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias.
e. Registro en la base de conocimiento.
f. Una vez que se ha alcanzado una solución definitiva del incidente, ésta será comunicada a todos los actores implicados en el incidente, para su cierre.

5.6.1. Lecciones Aprendidas:

Las lecciones aprendidas pueden poner de manifiesto la falta de un paso o una inexactitud en un procedimiento y son un punto de partida para el cambio, y es precisamente debido a la naturaleza cambiante de la tecnología de la información y los cambios en el personal, que el equipo de respuesta a incidentes debe revisar toda la documentación y las guías o procedimientos para el manejo de incidentes en determinados a intervalos de tiempo.

El Oficial de Seguridad de la Información, junto con el equipo de respuesta a incidentes, después de un incidente grave o Muy grave, y periódicamente después de los incidentes menores, se reunirán con el fin de identificar lecciones aprendidas sobre los incidentes presentados y así evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, la mejora de las medidas de seguridad y el proceso de gestión de incidentes.

Mantener un adecuado registro de lecciones aprendidas permite conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Actualizar las guías o playbooks existentes o documentar las nuevas.

- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Validar la materialización de los riesgos.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas para prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.
- Alimentación de bases de conocimiento con las acciones realizadas, cambios ejecutados y todo el análisis requerido para aplicar en caso de presentarse eventos o incidentes similares.
- Se toman decisiones frente a la generación de reportes o informes con el fin de socializar a involucrados e interesados toda la información (no sensible) respecto al tratamiento realizado, investigación y lecciones aprendidas del incidente, buscando evitar que esto se presente nuevamente o que en caso de ocurrir se cuente con preparación para ello.
- De ser necesario generar espacios para capacitar a personal para enfrentar estas actividades y contar con preparación para futuros eventos.

6. Anexos y registros.

GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información

7. CONTROL DE CAMBIOS.

Versión	Fecha	Descripción del Cambio
001	16-06-2017	Creación del documento
002	28-12-2020	Se incluye reconocimiento al CSIRT Gobierno y al comando Conjunto Cibernético de la Policía Nacional
003	23-12-2021	Se actualizaron los nombres de los grupos y de la Dirección TIC, acorde con la nueva estructura funcional. Se incluyó dentro de la introducción, la referencia a la Guía 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información, emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones
004	08/08/2023	Se ajustan las etapas de atención del incidente y se incluyen las referencias a los formatos: *GTI-FM-024 Bitácora de eventos e incidentes de seguridad* y *GTI-FM-025 Registro y tratamiento de incidentes de seguridad de la información.*

005	01/04/2025	Se actualiza la matriz de contacto con autoridades, se ajusta matriz de eventos y se actualizó documento de acuerdo con los nuevos parámetros establecidos en la guía de elaboración de documentos del SGI *"GIN-GU-003"* del Sistema de Gestión Integrado proceso gestión Integral.
006	06/05/2026	Se actualiza la dirección de correo electrónico de la mesa de ayuda, se ajustan actividades teniendo en cuenta la automatización del proceso en el Centro de Servicios tecnológicos.

Elaboró	Revisó	Aprobó
Nombre: Andrés Hernando Ortiz Tibaquirá Cargo: funcionario Grupo Seguridad e informática Forense. Fecha: 22/02/2026	Nombre: Rocío Pedrozo Cargo: Coordinadora Grupo Seguridad e informática Forense Fecha: 22/02/2026	Nombre: Ricardo Ríos Cargo: director tecnología de la información y las comunicaciones Fecha:06/05/2026

ANEXO No.1. MATRIZ DE CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
DIRECTOR DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	Cuando ocurra un incidente catalogado como MUY GRAVE Y GRAVE	Centro Cibernético Policial (CCP)	Acceso abusivo a sistemas informáticos Violación de Datos personales Uso de Software malicioso Suplantación de Sitios Web Transferencia no consentida de activos Hurto por medios informáticos Phishing Ingeniería Social	http://www.ccp.gov.co adenunciar.policia.gov.co Centro Cibernético Policial caivirtual@policia.gov.co +571 5159727 @caivirtual - Twiter, Facebokk, Instagram	Autoridad
		COLCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	Respuesta a Emergencias Cibernéticas de Colombia	www.colcert.gov.co colCERT contacto@colcert.gov.co Línea Directa: 57 601 3442222 phishing-report@colcert.gov.co + 571 2959897 @colCERT Comando Conjunto Cibernético soc-ccoc@ccoc.mil.co	Autoridad

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
				+571266-0247 +573103008916	
		CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	Atención a incidentes de seguridad digital	https://cc-csirt.policia.gov.co CSIRT Gobierno csirtgob@mintic.gov.co csirt-ponal@policia.gov.co dijin.cecip-jef@policia.gov.co - apoyo cadena de custodia 018000910742 opc. 4 @Ministerio_TIC	Autoridad Grupo de Interés
		Comando Conjunto Cibernético	Atención a incidentes de seguridad digital	soc-ccoc@ccoc.mil.co + 571 2660247 +573103008916 Apoyo a incidente informático servicio 24x7 - ccoci Cel 3183506143	Autoridad
		Seguridad Digital DNI Dirección Nacional de Inteligencia	Atención a incidentes de seguridad digital	www.dni.gov.co seguridad.digital@dni.gov.co + 571 4320000 ext 0783 - 0782 - 0785	Autoridad
Líder del Grupo GSIF	Cuando se requiera apoyo	Colcert	Para enviar una muestra de Malware	Correo electrónico: malware@colcert.gov.co	Autoridad

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
	para la identificación del malware				
Líder del Grupo GSIF	Coordinador Grupo de Seguridad e Informática Forense / Oficial de seguridad de la Información	Equipo de Respuesta a Incidentes Superintendencia de Sociedades	Compuesto por los administradores de la infraestructura son los que realizan la coordinación para la atención y respuesta del incidente presentado	GSIF@SUPERSOCIEDADES.GOV.CO	
	Coordinadores Grupos DTIC		Convocados dependiendo del incidente presentado	GIDAA@SUPERSOCIEDADES.GOV.CO GAD@SUPERSOCIEDADES.GOV.CO GPT@SUPERSOCIEDADES.GOV.CO GSAT@SUPERSOCIEDADES.GOV.CO GSIF@SUPERSOCIEDADES.GOV.Co	
	Administradores de plataformas		Convocados para que se realice la gestión	GSAT@SUPERSOCIEDADES.GOV.CO	

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
	(sistemas de información, bases de datos, plataformas de seguridad, servidores, directorio activo)		dependiendo el sistema o la plataforma afectada	GSIF@SUPERSOCIEDADES.GOV.CO GIDAA@SUPERSOCIEDADES.GOV.CO	
	Gestor de Incidentes de Seguridad (SOC)		Si se cuenta con el SOC contratado externamente se contacta al Supervisor del Contrato para gestionar el apoyo necesario	GPT@SUPERSOCIEDADES.GOV.CO	
	Mesa de Ayuda (Especialistas)		Si se cuenta con Mesa de Ayuda contratada externamente se contacta al Supervisor del Contrato Para gestionar el apoyo necesario	GPT@SUPERSOCIEDADES.GOV.CO SERVICIOS.TECNOLOGICOS@SUPERSOCIEDADES.GOV.CO	
	Mesa de Ayuda (Agentes)		Contactados para centralizar los incidentes y registrar la información que se genere a raíz del incidente o	Centro de Servicios Tecnológicos, o al correo Servicios.tecnologicos@supersocieddades.gov.co o a	

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
			evento presentado	través de la línea telefónica 601-2201000 opción 1 Ext.911.	
Oficial de Protección de Datos Personales	Cuando ocurra un incidente de seguridad que comprometa bases de datos con información personal	SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO - Registro Nacional de Bases de Datos	Reportar ante el Registro Nacional de Bases de Datos dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.	https://www.sic.gov.co/registro-nacional-de-bases-de-datos	Autoridad
Grupo Administrativo	Cuando ocurra un evento que afecte la infraestructura física, funcionarios.	Bomberos	Emergencia por Incendio	119	Autoridad
		Policía Nacional	Robo	112	Autoridad
		Gaula	Antisecuestro y Antiextorsión	165	Autoridad
		Defensa Civil	Siniestros ambientales	144	Autoridad
		Cruz Roja	Incidentes Laborales	132	Autoridad
		Centro Toxicológico	Incidentes laborales	136	Autoridad
		Dijin	Robo	157	Autoridad
Oficial de Seguridad de la	N/A	Segu Info	Página web argentina, con información relevante sobre seguridad de la	blog.segu-info.com.ar www.segu-info.com.ar	Grupo de Interés

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
información Grupo de Seguridad e Informática Forense			información a nivel mundial, donde se relacionan, cursos, actualizaciones de infraestructura, avances en el campo y noticias en general		
		Incibe	Página Web Española, que emite periódicamente noticias sobre vulnerabilidades identificadas en los sistemas de información e infraestructura, además de mejores prácticas para la administración del SGSI	https://www.incibe.es/	Grupo de Interés
		Hispasec "Una al día"	Hispasec es primer servicio diario de información técnica en español sobre seguridad informática, creado por un grupo de especialistas con el propósito de divulgar y	https://www.hispasec.com/es/	Grupo de Interés

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
			concienciar a los usuarios de la importancia de este sector.		
		X @COLCERT @MINDEFENSA @CAIVIRTUAL @CSIRTFINANCIERO @CSIRTPONAL @OEA_CYBER @INCIBE_CERT	Grupos de notificaciones permanentes sobre incidentes de seguridad, incidentes cibernéticos y eventos de seguridad	X	Grupo de Interés
		Elladodelmal	Página web de Chema Alonso, experto en seguridad informática. Contiene información relevante de ataques, nuevas tendencias, actualizaciones de infraestructura e información a nivel general	https://www.elladodelmal.com/	Grupo de Interés
		Enlace Digital	Grupo Privado de Seguridad Digital con los Oficiales de Seguridad y responsables de	Mensajeria Whatsapp Signal	Grupo de Interés

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
			Seguridad digital de las entidades del Estado, se alertan problemas de seguridad, información técnica de seguridad.		
		CSIRT - Financiero - ASOBANCARIA	Es el equipo de apoyo para la respuesta a incidentes cibernéticos sectorial, comunidad de intercambio y centro de excelencia en investigación y colaboración gremial para anticipar y mitigar riesgos derivados de amenazas cibernéticas, así como, apoyar la respuesta de los incidentes bajo una visión global.	CSIRT - Financiero - ASOBANCARIA	Grupo de Interés
NA	NA	Microsoft Security	Inteligencia de Amenazas, Alertas y prácticas	**https://www.microsoft.com/security**	Grupo de Interés
		Virus Total	Inteligencia de amenazas,	**https://www.virustotal.com**	Grupo de Interés

QUIEN REPORTA	CUANDO REPORTAR	ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	TIPO DE CONTACTO
			Análisis malware		
		Have I Been Pwned	Inteligencia de Amenazas, Filtraciones credenciales	**https://haveibeenpwned.com**	Grupo de Interés