1. OBJETIVOS

- Minimizar el impacto del negocio ante la materialización de un incidente de seguridad de la información.
- Definir los roles y responsabilidades asociados a la gestión de incidentes de seguridad
- Establecer una metodología para la gestión de incidentes de seguridad usando como base las mejores prácticas de la industria
- Definir la categorización de los incidentes de seguridad y su correspondiente escalamiento dentro de la entidad.

2. ALCANCE

El alcance en la gestión de incidentes de seguridad de la información está compuesto por cuatro etapas, iniciando con la preparación ante un incidente de seguridad, seguido de las etapas de detección y registro, contención y erradicación del incidente de seguridad de la información, y finalizando con las lecciones aprendidas donde se incluirán planes de mejora y acciones correctivas.

Aplicable a la Oficina de informática para la gestión de incidentes que sean categorizados como incidentes de seguridad

3. NORMATIVIDAD

Ver Normograma.

4. DEFINICIONES

- **Activo de información**: Es cualquier elemento que tenga valor para la organización y en consecuencia, debe ser protegido.
- **Amenaza:** Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.
- **Autenticidad**: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.
- **Cadena de Custodia**: Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
- **Contención**: Evitar que el incidente siga ocasionando daños.
- **Erradicación**: Eliminar la causa del incidente y todo rastro de los daños.
- **Evento de seguridad:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2009]
- **Gestión de Incidentes**: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder

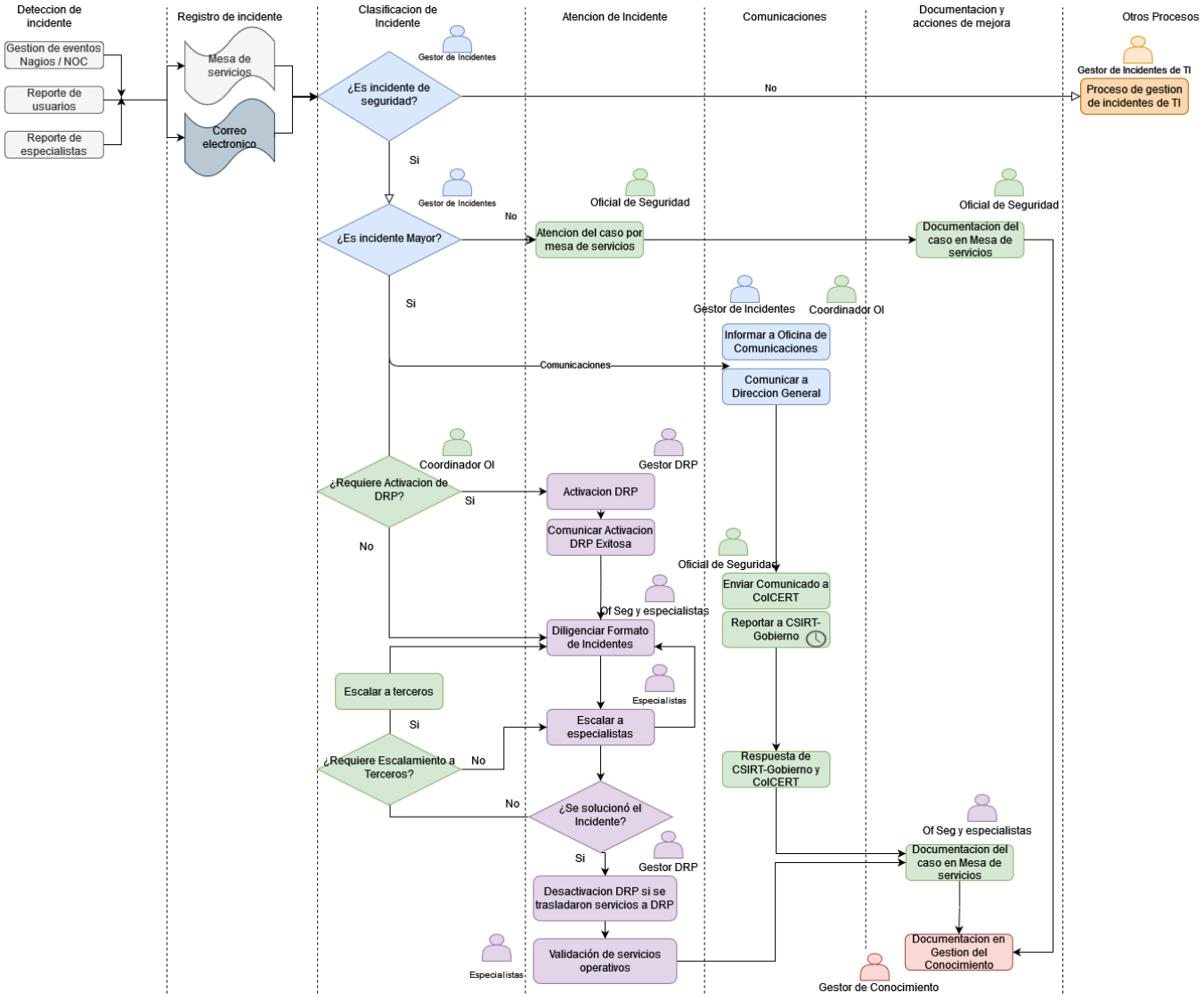
de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.

- **Hash**: Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
- **IDS**: Software de detección de intrusos
- **Impacto**: Consecuencias que produce un incidente de seguridad sobre la organización.
- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2009]
- **Libros de estrategias:** Procedimientos documentados que tienen como objetivo trazar la ruta de acción ante un tipo de incidente específico.
- **Log's:** Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
- **Recuperación:** Volver el entorno afectado a su estado natural.
- **SSI**: Subsistema de Seguridad de la Información.
- **Validación:** Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- **Vulnerabilidad:** Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

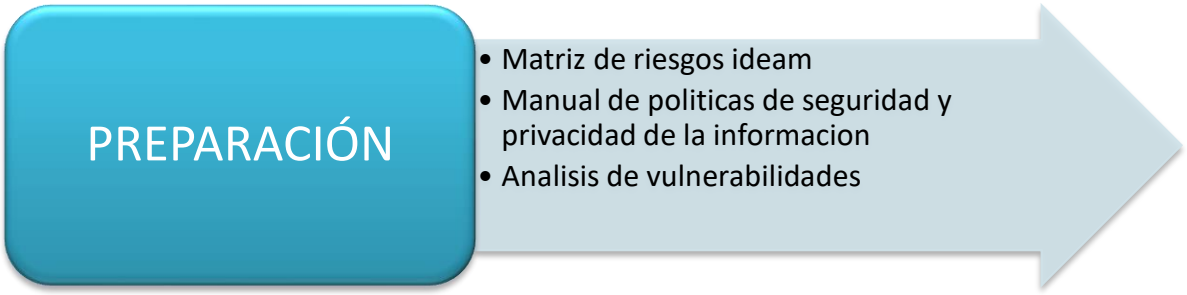
5. GESTION DE INCIDENTES

5.1. FASES DEL PROCESO DE GESTION DE INCIDENTES

5.1.1. DIAGRAMA DE FLUJO DEL PROCESO DE GESTION DE INCIDENTES DE SEGURIDAD



5.2. PREPARACION PARA INCIDENTES DE SEGURIDAD



5.2.1. Matriz de Riesgos IDEAM

La matriz de riesgos consiste en la identificación de amenazas y vulnerabilidades para el análisis de riesgos de seguridad digital, controles para la mitigación de los riesgos de seguridad digital, el reporte de riesgos de seguridad digital y otros aspectos adicionales para llevar a cabo una gestión del riesgo de seguridad digital adecuada.

Esta se encuentra publicada y actualizada por la oficina asesora de planeación y el GAESI para la oficina de informática

5.2.2. Manual de políticas y privacidad de la Información IDEAM

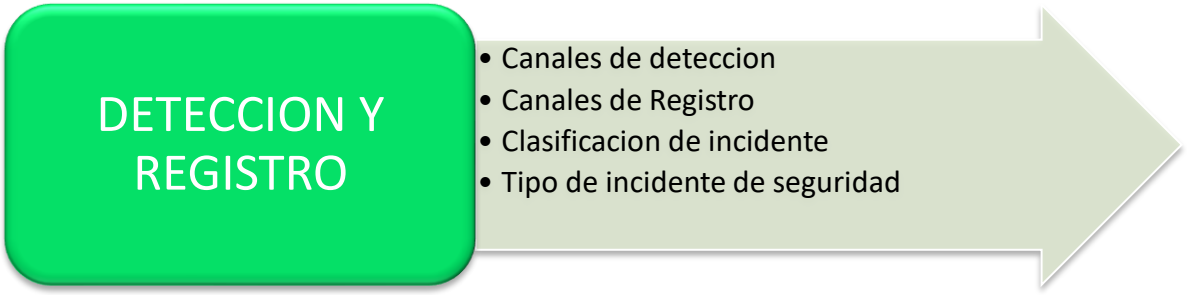
El manual de políticas de seguridad de la entidad se encuentra publicado en el Sistema de gestión Integrado allí se establecen las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas y aplicadas a nivel nacional en el marco de la operación por procesos del IDEAM y por los servidores públicos, contratistas, proveedores de servicios o a el personal que tenga alguna relación con el IDEAM

5.2.3. Análisis de vulnerabilidades

La oficina de informática debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información y componentes de infraestructura tecnológica.

El análisis de vulnerabilidades para la entidad se debe de realizar al menos una vez al año

5.3. DETECCION Y REGISTRO DE INCIDENTES DE SEGURIDAD



5.3.1. Canales de detección de incidentes

Fuentes de detección del incidente:

- Gestión de eventos (Nagios / NOC)
- Reporte usuario
- Reporte de especialista

5.3.2. Canales de registro habilitados

- Caso en mesa de servicio
- Correo electrónico
- Registro – Mesa de servicio – Formato

5.3.3. Clasificación de incidentes

- **Incidente de TI**
  - Incidente Menor
  - Incidente Mayor
- **Incidente de seguridad**
  Los incidentes de seguridad se clasifican según su severidad
  - Incidente Menor
    - La entidad aún puede prestar servicio a todos los usuarios
  - Incidente Mayor
    - Interrupción o degradación de servicios críticos a un subconjunto de usuarios
    - Interrupción de los servicios esenciales de la entidad durante un tiempo prolongado, ningún usuario puede hacer uso de las funciones críticas del negocio.
    - Información propia de la entidad ha sido expuesta, robada o comprometida.
    - La integridad de la información del negocio ha sido cambiada.

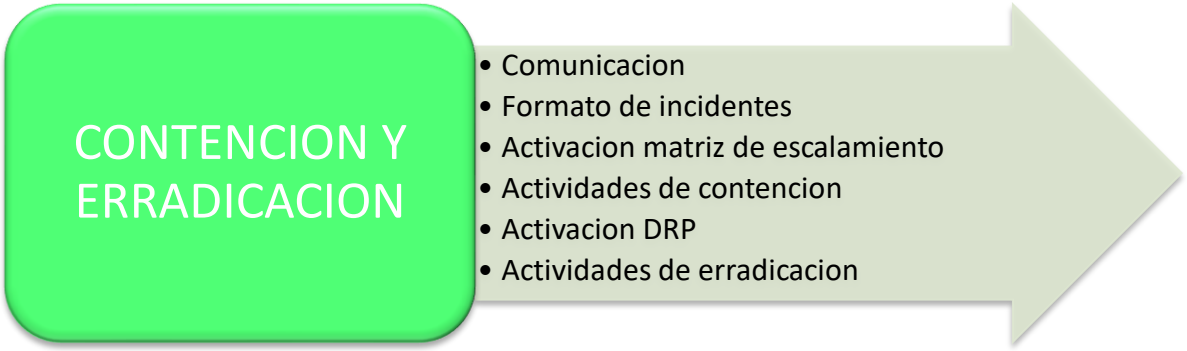
5.3.4. Tipos de incidentes de seguridad

Categoría	Tipos de Incidentes	Ejemplo
1	Manejo inadecuado de los datos	* Compartir información con terceros no autorizados * Almacenamiento de información sensible en medios sin cifrar * Almacenar información en repositorios no autorizados (DropBox, Mega, etc..)
2	Uso inadecuado de credenciales	* Almacenamiento de contraseñas en texto claro * Transmisión de contraseñas en canales inseguros (http, telnet, ftp, smtp) * Fuga de credenciales

3	Violación a Políticas de Seguridad de la Información	* Acceso a sitios web prohibidos * Descargas ilegales de material con copyright * Envío de correos abusivos o malintencionados * Instalación de software no autorizado * Deshabilitar funcionalidades de seguridad de los equipos
4	Acceso no autorizado a los activos de información	* Acceso a equipos o información no autorizada *Accesos mediante robo de credenciales * Acceso no autorizado a zonas restringidas
5	Intrusión	* Explotación de vulnerabilidades * Uso de exploits contra infraestructura o aplicaciones *Cambio de configuraciones establecidas por la organización en los sistemas o infraestructura * Acceso no autorizado a zonas restringidas.
6	Intentos de actividad No satisfactoria	*Ataques de fuerza bruta *Intentos de intrusión *Reconocimiento de puertos y escaneos
7	Ingeniería Social	* Correo fraudulento (phishing) * Llamada fraudulenta (vishing) * Cualquier otro mecanismo de suplantación digital o física
8	Negación de servicio	* Sobrecarga de los sistemas debido al incremento de tráfico de red (DoS, DDoS)
9	Vulnerabilidades	* Vulnerabilidades que afecten los sistemas o la infraestructura de la organización
10	Malware	* Cualquier tipo de código malicioso (Virus, Gusanos, Troyanos, Spyware, Ransomware, Rootkits, Criptominner)

Cuadro 1. Tipos de Incidentes de seguridad

5.4. CONTENCION Y ERRADICACION DEL INCIDENTES DE SEGURIDAD



5.4.1. Comunicaciones

5.4.1.1. Comunicación a la dirección y Oficina de Comunicaciones

El gestor de incidentes comunicara a la oficina de comunicaciones (comunicaciones@ideam.gov.co) y dirección general formalmente la afectación de los servicios
Este comunicado se realiza vía correo electrónico con el fin de indicar a los usuarios finales los servicios que presentan afectación

5.4.1.2. Escalamiento a ColCERT

Se realiza el escalamiento a ColCERT de acuerdo al formato publicado:
Se deben cumplir con los parámetros especificados en el link:
http://www.colcert.gov.co/?q=contenido/reportar-un-incidente
Y enviar el correo a contacto@colcert.gov.co

5.4.1.3. Escalamiento a CSIRT Gobierno

Identificado el incidente cibernético, por el oficial de seguridad o encargado de seguridad digital de la entidad, diligenciar el formato de reporte de incidentes en su totalidad y enviarlo al CSIRT Gobierno para su gestión y acompañamiento.

Mesa de servicio CSIRT Gobierno
Contactando a la mesa de servicio, llamando a la línea gratuita 018000910742, Opción 2, seguridad digital.

Correo electrónico:
Enviando un mensaje de correo electrónico informando el incidente al buzón csirtgob@mintic.gov.co, adjuntando el Formato de Reporte de Incidentes debidamente diligenciado.

5.4.1.4. Activación matriz de escalamiento interno

Los escalamientos internos se dan a los especialistas según el diagrama de flujo indicado anteriormente y el rol de cada especialista, al momento de emitir el presente instructivo la matriz de escalamientos se nombre como
IAITIC-2020-33- Matriz-Escal.xlsx

5.4.2. Diligenciamiento formato de incidentes

Ante los incidentes mayores se debe de diligenciar el formato para reporte de incidentes con su tipo y clasificación, allí se diligencian las actividades realizadas en orden cronológico, con el responsable de cada actividad e inconvenientes u observaciones presentadas

El formato se encuentra en el SGI como E-GI-F004 formato para reporte de incidentes IDEAM

5.4.3. Matriz de escalamiento

El gestor de incidentes comunicara a la oficina de comunicaciones (comunicaciones@ideam.gov.co) y dirección general formalmente la afectación de los servicios
Este comunicado se realiza vía correo electrónico con el fin de indicar a los usuarios finales los servicios que presentan afectación

5.4.4. Activación de centro de datos alterno DRP

Ver. E-SGI-SI-M004 MANUAL PLAN RECUPERACIÓN DESASTRESv3.pdf publicado en sgi.ideam.gov.co

5.4.5. Contención y erradicación del Incidente

Esta actividad busca impedir que el incidente se propague y pueda generar más daños a través de toda la infraestructura o a otros activos de información.

La siguiente tabla muestra algunas estrategias que se pueden tomar ante la presencia de algunos Incidentes de seguridad de TI.

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del Root	Volcados de memoria, registros para evidencia digital. Desconexión de la red mientras se recobra el manejo del equipo
Reconocimiento	Scanning de puertos	Incorporación de reglas de filtrado en el firewall

La estrategia de contención varía según el tipo de incidente. Los criterios deben ser documentados Claramente para facilitar la rápida y eficaz toma de decisiones algunos de los criterios que deben ser definidos 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 manipulación de la evidencia es otro aspecto de suma importancia a tener en cuenta en la resolución de un incidente de seguridad. En tales casos, es importante documentar claramente cómo todas las pruebas, incluidos los sistemas en peligro que han sido preservados

Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como por ejemplo el código malicioso, posterior a la erradicación se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual los administradores de TI deben restablecer la funcionalidad de los sistemas afectados y realizar un aseguramiento que permita prevenir incidentes similares en el futuro.

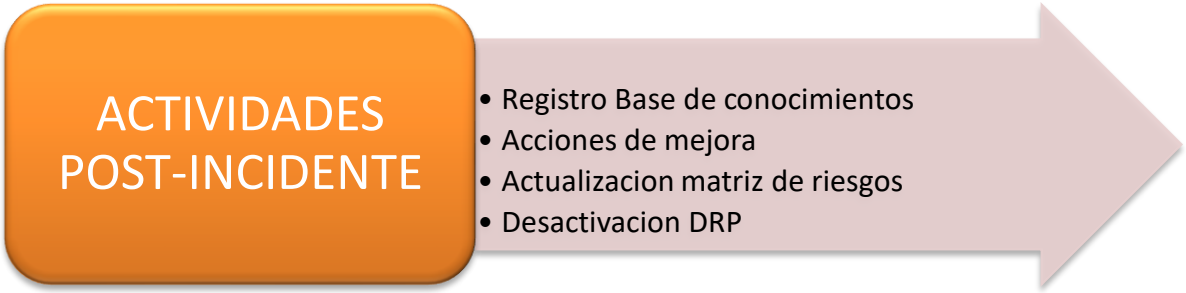
Incidente	Ejemplo	Estrategia de contención
DoS (denegación de servicio)	SYN Flood	Reconfigurar el router efecto del flooding. para minimizar el
Uso no autorizado	Utilizar los equipos de cómputo del IDEAM para lucro personal	Comunicar a todos los funcionarios las políticas de uso de los recursos de TI. Implementar monitoreo de uso de los pc's
Vandalismo	Defacement a un sitio web	Aplicar los parches y actualizaciones de seguridad, reconfiguraciones

La recuperación puede incluir acciones tales como la restauración de copias de seguridad de los sistemas, la reconstrucción de los sistemas a partir de cero con versiones limpias, la instalación de parches, cambio de contraseñas, y reforzar la seguridad del perímetro de red (Firewall, listas de control de acceso en routers). También es conveniente emplear a menudo niveles más altos de la red o el sistema de registro de seguimiento como parte del proceso de recuperación.

La restauración de los servicios afectados puede requerir frecuentemente de la puesta en marcha de procedimientos de recuperación y quizás de contingencia y continuidad

Incidente	Ejemplo	Estrategia de contención
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web

5.5. Actividades post-incidente



Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores de gestión

5.5.1. Registro Base de conocimiento

Dentro de las actividades de la atención es la de aprender y mejorar. Cada equipo de respuesta a Incidentes debe evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, y las lecciones aprendidas.
Mantener un proceso de "lecciones aprendidas" después de un incidente grave, y periódicamente después de los incidentes menores, es sumamente útil en 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.
- Los procedimientos documentados.
- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente
- similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.

El proceso de lecciones aprendidas puede 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 los procedimientos para el manejo de incidentes en determinados intervalos.

Otra importante actividad después de la ocurrencia de un incidente de seguridad es crear un informe de seguimiento para cada incidente, pues esto puede ser muy valioso para uso futuro, pues este informe proporciona una referencia que puede ser utilizada para ayudar en el manejo de incidentes similares.

Un estudio de los hechos post incidente puede evidenciar debilidades y amenazas de seguridad, así como los cambios en las tendencias del incidente. Estos datos pueden ser tratados en el proceso de evaluación de riesgos, que conducirá a la selección y aplicación de controles ya sean tecnológicos o de otra naturaleza que permitan dar respuesta a los incidentes de seguridad de la información

5.5.2. Indicadores de gestión para la atención de incidentes

Para medir el desempeño del Grupo de Atención de Incidentes y del sistema en general proponemos básicamente los siguientes indicadores:

Indicador	Descripción
Número de Incidentes Seguridad Atendidos	Da un indicador de la cantidad de incidentes atendidos por el Grupo de Atención de Incidentes.
Número de Incidentes de Seguridad atendidos por cada tipo de Incidente y por Prioridad.	Provee una estadística de la tipología y prioridad de los incidentes atendidos. Esto puede ayudar para determinar cuál es el incidente más crítico para poder tomar medidas de mitigación del mismo. También se recomienda mirar los incidentes de tipo Otros para determinar si se crea o no un nuevo tipo de incidente.
Tiempo promedio de atención de cada tipo de Incidente y por Prioridad del mismo.	Permite verificar el cumplimiento de los SLA.
Tiempo promedio de solución de cada tipo de Incidente y por Prioridad del mismo.	Ayuda a encontrar demoras en solución de tipos de incidentes.
Número de Incidentes detectados por cada fuente.	Permite verificar la efectividad de cada fuente de detección de intrusos. Para este caso si para la fuente “Reporte por personal interno” el número de incidentes detectados es muy alto, se deben plantear y recomendar nuevos mecanismos de detección de incidentes.
Número de Incidentes en los cuales el plan de Recuperación de Desastres ha sido activado.	Permite verificar si los procedimientos de erradicación de incidentes son efectivos y confiables.
Número de Incidentes Contenidos.	Da un indicador sobre la necesidad de aislar o no los sistemas afectados.
Número de Incidentes por Sistema Afectado.	Permite identificar sistemas de información demasiado vulnerables para así plantear nuevos mecanismos de protección para esos sistemas de información

5.5.3. Desactivación de centro de datos alterno DRP

Ver. E-SGI-SI-M004 MANUAL PLAN RECUPERACIÓN DESASTRES.pdf publicado en sgi.ideam.gov.co

6. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	06/03/2013	Creación de los lineamientos.
02	28/11/2014	Actualización Nuevo Formato de Instructivo.
03	05/04/2018	Se actualiza, versión y codificación para cumplimiento con el decreto 415
04	25/05/2019	Actualización del documento
05	25/05/2021	Se actualiza el proceso de acuerdo a los roles definidos en la entidad, el formato de registro de incidentes y los lineamientos de la auditoria externa
06	25/08/2021	Actualización del documento para incluir la activación del DRP en el instructivo
07	10/12/2021	Actualización del documento de acuerdo a la resolución 1519 de 2020 MinTIC

ELABORÒ:	REVISÒ:	APROBÒ:
Harbey Martínez Guerrero Oficial de Seguridad IMPRECTICS - IDEAM	**Eduardo Ramírez Acosta** Coordinador GAESI Oficina de Informática	**Alicia Barón Leguizamón** Jefa Oficina de Informática