1. OBJETIVO

Definir un instructivo que permita manejar adecuadamente los incidentes de seguridad de la información a través de un esquema que involucra la preparación, detección y análisis, contención, erradicación, recuperación y la actividad post-incidente.

2. ALCANCE

Este documento entrega los lineamientos para colocar en marcha el Modelo de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, independiente del medio en el que se encuentren los activos de información, sin embargo, el alcance inicial a implantar pretende atender los incidentes de seguridad relacionados con los activos de información que están almacenados y/o son procesados por la infraestructura de Tecnología de Información del IDEAM.

3. NORMATIVIDAD

Ver Normograma.

4. DEFINICIONES

Incidente de Seguridad de la Información: Un incidente de seguridad de la información se define como cualquier evento que compromete o afecta potencialmente el ambiente de seguridad de la información de una organización, en cualquiera de sus principios de confidencialidad, integridad o disponibilidad.

Usuario y/o Cliente: Persona natural o jurídica que requiere o contrata los servicios del Instituto. Será aquella persona que, para ejercer una funcionalidad definida, necesita acceder los datos e información para el normal desempeño de sus actividades. Estos deben cumplir con las políticas de seguridad de la información, y los procedimientos del modelo de seguridad de la información.

Virus Informático: Programa que se auto replique, consuma o perjudique de alguna forma el rendimiento del computador, dañe la memoria, archivos o software.

Activo de información: Cualquier cosa que tiene un valor para la organización. (ISO/IEC 27000:2009).

Recursos Informático: Conjunto de elementos de hardware, software y comunicaciones destinados a un procesamiento de información con características específicas. (Ejemplo: Servidores, Computadores, red de comunicaciones, entre otros).

5. POLÍTICAS DE OPERACIÓN

A continuación, se declaran las políticas de operación para los incidentes de seguridad:

- Se define como único punto de contacto la mesa de ayuda (Help Desk).
- Se deben asignar los roles y responsabilidades para el correcto funcionamiento del plan de atención de incidentes.
- Se debe difundir el plan al personal del Instituto y capacitarlo adecuadamente.
- Un incidente de seguridad de la información se define como un 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 la Política de Seguridad de la Información del Instituto.

6. DESARROLLO

6.1. CARACTERISTICAS DEL MODELO DE ATENCIÓN DE INCIDENTES

El modelo de gestión de incidentes está inmerso en un ciclo de mejora continua y las actividades definidas están basadas en las recomendaciones dadas por diversas organizaciones de la seguridad de la información como son:

a) CERT/CC Incident Reporting Guidelines.
b) NIST Computer Security Incident Handling Guide.
c) SANS Institute
d) ITIL Section Security Management, Incident Management
e) ISO/IEC 27002. Numeral 16 Gestión de los Incidentes de Seguridad de la Información

Tomando como referencia lo definido por el NIST y lo definido en la norma ISO/IEC 27002 el modelo de atención de incidentes está definido por las siguientes actividades:

Figura 1. Ciclo de vida para la respuesta a Incidentes NIST

6.1.1. PREPARACIÓN

6.1.1.1. Equipo de Atención de Incidentes

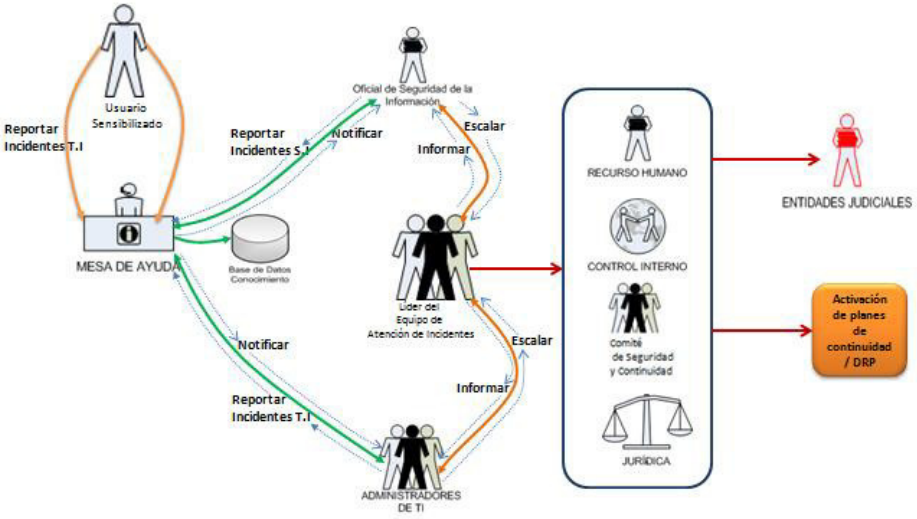


Figura 2. Equipo de Atención de Incidentes

El modelo de atención de incidentes contempla la unificación en la gestión de incidentes de la infraestructura y la de los incidentes de seguridad de la información con el fin de centralizar la atención a los usuarios, es por esta razón que el punto de contacto inicial es la mesa de ayuda, tal como se observa en la Figura 2.

6.1.1.2. Actividades de Preparación

En esta etapa se definen las actividades que le van a permitir al IDEAM desarrollar la capacidad para responder ante los incidentes de seguridad, de igual forma y aunque no es una función del equipo de atención a incidentes se definen mecanismos (Seguridad de sistemas, Seguridad de redes, y Seguridad de aplicaciones) que permitan la prevención de los incidentes.

- **Actividades a desarrollar en esta etapa**

  ○ Identificar y aprovisionar los recursos necesarios en todas las etapas de la atención de incidentes.
  ○ Identificar y definir los lineamientos para prevención de incidentes, dentro de estos lineamientos se encuentran:

  • **Gestión de parches de seguridad:** La entidad debe contar con un programa de gestión de vulnerabilidades (este programa deberá cubrir la aplicación de actualizaciones de seguridad en todos los sistemas). Este programa ayudará a los administradores en la identificación, adquisición, prueba e instalación de los parches.
  • **Aseguramiento de plataforma:** Los hosts y servidores del Instituto deben ser asegurados correctamente. Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones por default (passwords y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar su respectivo banner de advertencia. Los hosts deben tener habilitados sus sistemas de auditoría para permitir el login de eventos.
  • **Seguridad en redes:** Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad (firewall) deben ser revisadas continuamente y las publicaciones WEB deben estar protegidas por el sistema

Web Application Firewall - WAF. Las firmas y actualizaciones de dispositivos de Prevención de Intrusos (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 y con las firmas de actualización al día.

• **Sensibilización y entrenamiento de usuarios:** Usuarios en el Instituto incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones.

- Capacitar a todos los funcionarios en gestión de incidentes teniendo en cuenta su rol dentro de dicho proceso.
- Definir y actualizar las métricas para la evaluación de los indicadores de atención de incidentes.

- **Aprovisionamiento de recursos:** A continuación, se presentan una serie de requisitos adicionales que deben cumplirse durante la fase de preparación en el proceso de atención de incidentes.
  - **Recursos de Comunicación**

    En este numeral se enuncian los elementos necesarios para la comunicación del Equipo de Atención de Incidentes con los demás funcionarios del Instituto.

    Información de Contacto: Se deberá tener una lista de información de contacto de cada uno de las personas que conforman el grupo de atención de incidentes, tales como teléfonos celulares, teléfono fijo (casa y oficina), extensión.

    Información de escalamiento: Se deberá contar con información de contacto para el escalamiento de los incidentes, tales como:

    - Información de los administradores de los servidores y servicios.
    - Información de contacto para la atención de soporte tercerizado especializado para la plataforma tecnológica, Contacto con la Oficina Asesora Jurídica y la Oficina de Control Interno en caso de tener que tomar acciones disciplinarias contra algún funcionario.
    - Contacto con la división de delitos informáticos de la Policía Nacional, para informar sobre cualquier evento de alto impacto a la entidad. El número de contacto es 4266301 y 4266256 “http://www.delitosinformaticos.gov.co/”. Correo electrónico delitosinformaticos@dijin.policia.gov.co o caivirtual@correo.policia.gov.co .

  - **Hardware y Software**

    Para la atención de incidentes, el IDEAM se sugiere la adquisición de los siguientes elementos:

    - Portátiles Forenses: Equipos de cómputo portátiles que deben tener instalados herramientas como analizadores de protocolos, software de adquisición de imágenes y debe estar provisto de hardware especializado para la instalación de discos de análisis en modo de lectura.

- Analizadores de protocolos. Este tipo de herramientas permitirá realizar análisis del tráfico al interior de la red del Instituto.
- Software de adquisición. Para poder recolectar evidencia de los medios.
- Kit de respuesta de incidentes. Con el fin de poder atender incidentes de manera rápida y preparada.
- Software de análisis forense. Que permite realizar análisis especializado de los medios y la evidencia recolectada.
- Medios de almacenamiento. Se deben prever discos de alta capacidad de almacenamiento para poder almacenar la evidencia recolectada.

- **Recursos para el análisis de incidentes**

  - Listado de puertos. Se debe tener una lista de todos los puertos conocidos “well-know” y de los puertos utilizados por ataques.
  - Diagramas de red. Para una rápida ubicación de los recursos existentes y para el seguimiento de un ataque en curso.
  - Líneas Base. Se debe levantar la información de los servidores, tales como nombre, dirección IP, parches, aplicaciones y usuarios configurados, con el fin de determinar el estado normal de los mismos y poder identificar de manera rápida un incidente de seguridad. Las líneas base deberán someterse a un sistema de administración de actualizaciones que permita identificar y documentar nuevos cambios a la plataforma con su debida justificación y responsable de la ejecución del cambio.
  - Comportamiento de la red. Se debe realizar un análisis de las conexiones de red, para poder identificar un comportamiento normal. Este deberá incluir:
    - Puertos utilizados por los protocolos de red.
    - Horarios de utilización pico y valle.
    - Direcciones IP que generan más tráfico.
    - Direcciones IP que más reciben peticiones.

- **Recursos para la mitigación de incidentes**

En este punto se consideran los elementos necesarios para la contención y mitigación de incidentes:

  - Revisión de las estrategias de continuidad implementadas.

6.1.2. REPORTE, DETECCIÓN Y ANÁLISIS

6.1.2.1. Detección de Incidentes

Identificación y gestión de elementos Indicadores de un incidente

Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido generalmente algunos de estos elementos son:

- Alertas en la consola de administración del firewall
- Alertas en la consola de antivirus
- Alertas de equipos de seguridad perimetral
- Número elevado de conexiones en los servidores.
- Reporte de los usuarios sobre cualquier anomalía sobre los activos de información.

- Reporte de los administradores sobre cualquier anomalía sobre los activos de información
- Un administrador del sistema observa un archivo con caracteres extraños en su nombre.
- Otros

En la siguiente tabla se identifican las fuentes generadoras de eventos que apoyan la identificación de incidentes de seguridad:

Tabla No. 1. Fuentes de información para la detección de incidentes de seguridad informática

Fuente	Descripción
Logs de alertas en el firewall	Estos logs pueden ayudar a identificar posibles problemas en la red de perímetro externo (internet) como accesos no autorizados y tráfico anormal bloqueado por el FW.
Monitoreo del tráfico de internet (Control ancho de banda)	Indica la existencia de un comportamiento anormal en el tráfico en el canal de Internet.
Alertas de caídas de servidores y servicios. También aplica a estaciones de trabajo de usuarios consideradas sensibles	Indican indisponibilidades con los servicios en servidores, equipos en usuarios o posibles problemas con la red.
Logs y eventos consola Antivirus	Ayudan a identificar el estado de actualización de los antivirus de los clientes y los virus detectados en toda la infraestructura. Se debe considerar la centralización de alarmas a nivel de los antivirus.
Reporte por personal interno	Los reportes por personas externas a través de la mesa de ayuda , el Líder de Gestión de Incidentes o el Jefe de Infraestructura que indiquen alguna sospecha de incidente en la infraestructura.
Logs de alerta e información del proxy para salida a Internet	Indican la presencia de algún equipo Interno infectado por virus, gusano y que sea generador de tráfico SPAM.
Eventos del Directorio Activo	Identifican posibles intentos de acceso no autorizado a los sistemas del Instituto.
Eventos de los motores de bases de datos core en la entidad	Estas alertas pueden permitir la identificación de acciones no permitidas a nivel de las bases de datos configuradas
Logs de servidores, equipos de red y aplicaciones	Permiten monitoreo de actividad así como accesos realizados por los usuarios

6.1.2.2. Reporte

La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

A continuación, se describe el proceso de notificación que deberá ser seguido en el IDEAM:

- Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo a Mesa de Ayuda a través de la herramienta definida para tal fin.
- Mesa de Ayuda realizará el primer filtro para identificar si corresponde a un incidente de seguridad o está relacionado con requerimientos propios de la infraestructura de TI. Si el incidente es catalogado como un requerimiento de TI se procederá a su normal atención de acuerdo a los procedimientos establecidos. En caso de ser catalogado como un incidente de seguridad se notificará al Oficial de Seguridad para que tome las decisiones correspondientes al proceso de Atención de Incidentes. Mesa de Ayuda será el encargado de realizar el seguimiento del Incidente hasta su cierre definitivo.
- Los incidentes que no relacionan activos informáticos, tienen un manejo directo por parte del Oficial de Seguridad de la Información, quien notificará a los entes que puedan ayudar a la resolución del mismo.

- El personal de mesa de ayuda que reciba la notificación del usuario deberá completar el formato de E-SGI-SI-F004 FORMATO REPORTE DE INCIDENTES DE SEGURIDAD que se encuentra disponible en el Sistema de Gestión Integrado, en el grupo Gestión del SGI, carpeta SGI y finalmente abrimos la carpeta de Formatos:

FORMATO PARA REPORTE DE INCIDENTES DE SEGURIDAD IDEAM			
Fecha de notificación:		Hora notificación:	
Estado incidente:			
DATOS DE LA PERSONA QUE NOTIFICA			
Apellidos y Nombres:			
Área:		Correo Electrónico:	
Teléfono Interno:		Teléfono particular:	
INFORMACIÓN SOBRE EL INCIDENTE			
Fecha en que se observó:		Hora en que se observó:	
Marque con una X las opciones que considere aplicables:			
Uso indebido de información crítica		Ingeniería social, fraude o phishing.	
Uso prohibido de un recurso informático o de red del IDEAM.		Modificación no autorizada de un sitio o página web del IDEAM.	
Divulgación no autorizada de información personal.		Eliminación insegura de información.	
Intrusión física.		Modificación o eliminación no autorizada de datos.	
Destrucción no autorizada de información.		Anomalía o vulnerabilidad técnica de software.	
Robo o pérdida de información.		Amenaza o acoso por medio electrónico.	
Interrupción prolongada en un sistema o servicio de red.		Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)	
Modificación, instalación o eliminación no autorizada de software.		Robo o pérdida de un recurso informático del IDEAM.	
Acceso o intento de acceso no autorizado a un sistema informático.		Otro no contemplado. Describa:	
INFORMACIÓN SOBRE EL INCIDENTE			
Descripción del incidente:			
Si el incidente: • Se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. • Se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. • Se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con Mesa de Ayuda o a través de correo electrónico			
Describa brevemente del incidente:			
El incidente aún está en progreso: SI ( ) No ( )			
Detalle de las personas que han accedido al sistema afectado desde la presentación del incidente:			
Sistema, computadora o red afectada:			
Localización Física:			
Describa brevemente la información contenida en el sistema:			
¿Existe copia de respaldo de los datos o software afectado?		Si ( ) No ( )	
¿El recurso afectado tiene conexión con la red del IDEAM?		Si ( ) No ( )	
¿El recurso afectado tiene conexión a Internet?		Si ( ) No ( )	
Sistema operativo:			

6.1.2.3. Análisis Inicial del Incidente

Las actividades de análisis del incidente involucran lo siguiente:

- **Perfilar redes y sistemas:** Tener conocimiento de las características normales tanto a nivel de red (cantidad de tráfico, uso de ancho de banda) y sistemas (cheksums de archivos críticos de sistema).
- **Entender comportamientos normales:** Los administradores de TI deben tener conocimiento total sobre los comportamientos de la infraestructura que están administrando.
- **Usar centralización de logs y crear una política de retención y almacenamiento de logs:** La información de logs de equipos de red, servidores, aplicaciones debe ser centralizada en equipos dedicados al almacenamiento de este tipo de archivos.
- **Efectuar correlación de eventos:** A partir de la información recolectada de los logs de los sistemas, se pueden descubrir patrones de comportamiento anormales y facilitar la identificación de la causa del incidente.
- **Mantener los relojes sincronizados:** Para un correcto análisis de un incidente todos los equipos deben encontrarse sincronizados con una única fuente de tiempo. Esto facilita la correlación y análisis de logs.
- **Mantener y usar una base de conocimientos:** La base de conocimiento hace parte de la información definida en la etapa de preparación. Enlaces a páginas relacionadas con información sobre nuevas vulnerabilidades, información de servicios habilitados en los equipos hacen parte de esta base de conocimiento. Esta herramienta facilita el proceso de gestión de un incidente.
- **Usar motores de búsqueda y sitios de seguridad para investigaciones:** Bases de datos como el CVE (*Common Vulnerabilities and Exposures) facilitan el tratamiento de incidentes de seguridad.*
- **Analizadores de protocolos (sniffers) para recolectar datos:** Permiten el análisis e identificación de patrones anómalos en el tráfico de red de la entidad.
- Adquirir y usar la experiencia en el manejo de incidentes
- Crear matrices de diagnóstico para los agentes de Mesa de Ayuda y los administradores menos experimentados.
- Buscar asistencia de especialistas.

Los pasos anteriores ayudan a analizar los incidentes en proceso de tal forma que se puedan clasificar, tratar, priorizar y escalar de manera adecuada.

6.1.2.4. Categorización del Incidente

La Mesa de ayuda clasifica los incidentes en cuanto a su prioridad, a partir del impacto y urgencia según el criterio descrito en el Acuerdo de Nivel de Servicio. El criterio considera el costo potencial de la no-resolución del incidente, los posibles perjuicios causados a usuarios o empleados y las implicaciones legales.

Al clasificar los incidentes se puede determinar cuáles necesitan atención más urgente y en qué orden. La prioridad no trata simplemente de poner los incidentes en cola para su resolución; también trata sobre los recursos (tiempo, personal, destreza, investigación y soporte de terceros) que se asignarán a la resolución. En términos prácticos, podría llegarse a decidir, por ejemplo, que un incidente de baja prioridad no se resuelva en el tiempo objetivo, para así permitir que un incidente de más alta prioridad pueda tratarse dentro de su objetivo.

- **Priorización del incidente**

La priorización del incidente puede ser normalmente determinada tomando en cuenta la urgencia del incidente (que tan rápido el negocio necesita la solución del incidente) y el nivel de impacto

que causa. Una indicación de impacto es a menudo (no siempre) el número de usuarios siendo afectado.

También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes “sencillos” se tramitarán cuanto antes.

Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente.

La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Para priorizar los incidentes se han considerado las siguientes variables:

- **Urgencia del incidente:** Depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente los acuerdos de nivel de servicio acordados y del tiempo que puede pasar desde detectado el incidente hasta que se produzca el impacto definido en la variable anterior. Se propone a IDEAM la siguiente definición:

Nivel Urgencia	Definición
Baja	Se ha detectado una actividad anormal que puede afectar cualquier sistema de información o estación de trabajo o activo de información
Media	Se ha detectado una actividad anormal que afecta sistemas de información, o activos de información requeridos por procesos no misionales de la entidad
Alta	Se ha detectado una actividad anormal que afecta sistemas de información, o activos de información requeridos por procesos misionales de la entidad

- **Impacto del Incidente:** Determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.

Nivel Impacto	Definición
Bajo	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo o activo de información no sensible.
Medio	Impacto moderado en uno de los componentes de cualquier sistema de información, estación de trabajo o activos de Información.
Alto	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo. Activo de información sensible.

De las anteriores definiciones de urgencia e impacto se define la siguiente tabla:

		IMPACTO		
		ALTO	**MEDIO**	**BAJO**
URGENCIA	**ALTO**	1	2	3
	MEDIO	2	3	4
	BAJO	3	4	5

6.1.3. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Es importante para el IDEAM 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 los activos de información; Así mismo esta estrategia debe tener en cuenta los riesgos aceptables en relación con los incidentes de seguridad.

6.1.3.1. Contención:

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.

6.1.3.2. Erradicación y Recuperación:

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 para minimizar el efecto del flooding.
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

6.1.4. ACTIVIDAD 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.

6.1.4.1. Lecciones Aprendidas

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,

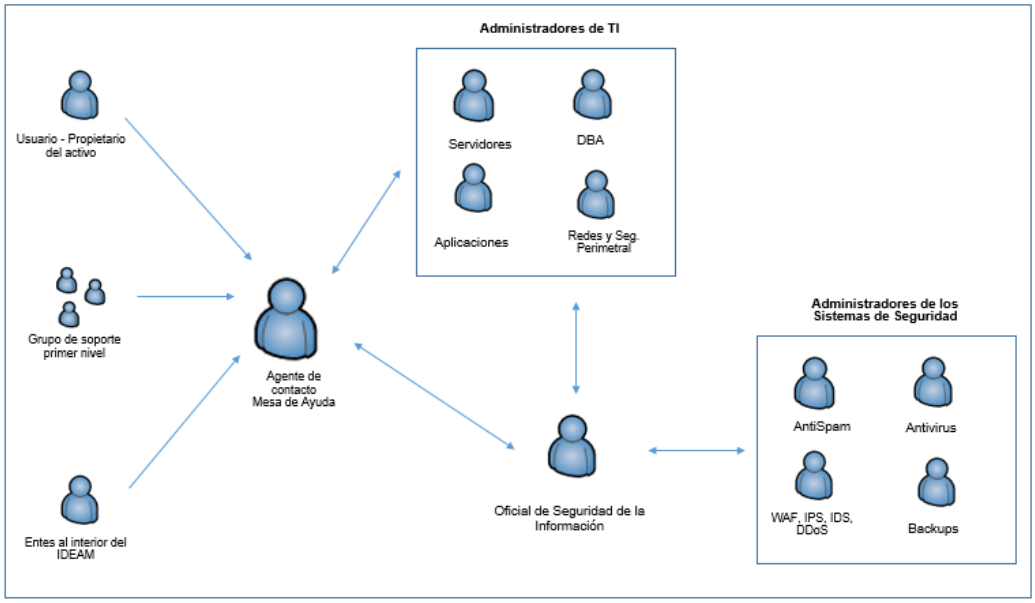
que el equipo de respuesta a incidentes debe revisar toda la documentación y los procedimientos para el manejo de incidentes en determinados intervalos.

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

6.2. ROLES DEFINIDOS PARA LA ATENCIÓN DE INCIDENTES DE SEGURIDAD

A continuación, se presentará una descripción de los actores que según el modelo propuesto deben intervenir en el proceso de atención de Incidentes, para cada actor se presentará una breve descripción sobre su perfil y la función dentro del proceso de respuesta a incidentes de seguridad de la información.



6.2.1. Usuario

- Es un funcionario, empleado contratista o tercero con acceso a la infraestructura del IDEAM, quien debe estar educado y concientizado sobre la Política de Seguridad de la Información y políticas derivadas, así como en los procedimientos de atención de incidentes.
- Tomar nota sobre los detalles importantes ante la presencia de eventos (por ejemplo, tipo de incumplimiento o violación, disfunción que se presenta, mensajes en la pantalla, comportamiento extraño);
- No ejecutar ninguna acción propia sino reportarla inmediatamente al punto de contacto (Mesa de Ayuda).
- Este no es un actor que pertenece directamente al ciclo de atención, pero cumple un papel importante en la detección de incidentes.

6.2.2. Mesa de Ayuda

- Encargada de recibir las solicitudes por parte de los usuarios sobre posibles incidentes (En este caso el agente de Mesa de Ayuda).
- Realizar el registro en la base de conocimiento y debe ser la encargada de escalarlos al Oficial de Seguridad o al personal de TI según sea el cado
- Debe contar con capacitación en Seguridad de la Información (con un componente tecnológico fuerte) y debe conocer perfectamente la clasificación de incidentes y el procedimiento de escalamiento y notificación de incidentes.
- Este actor es el punto inicial de contacto para de los usuarios reporten lo incidentes, da un tratamiento inicial y escala el incidente para que sea tratado.

6.2.3. Administradores de TI

- Apoyar a Líder de Gestión de Incidentes en la obtención de fuentes de evidencia, configuración de herramientas y modificaciones necesarias en los Recursos de Información para propósitos de la investigación del incidente.
- Notificar al Líder de Gestión de Incidentes sobre eventos anómalos en sus plataformas tecnológicas que puedan ser fuente para un incidente de seguridad.
- Configurar y mantener los activos informáticos en el IDEAM. También debe ser notificado por el agente de Mesa de Ayuda sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad.
- Contar con capacitación en Seguridad de la Información (con un componente tecnológico fuerte no solo en su plataforma si no en redes y erradicación de vulnerabilidades).
- Conocer perfectamente la clasificación de incidentes y los procesos de escalamiento de incidentes. Adicionalmente debe contar con una capacitación en técnicas forenses, específicamente en recolección y manejo de evidencia.

Los administradores son considerados parte del fundamental del Proceso de Atención de Incidentes, ya que pueden jugar un papel fundamental en los procesos de análisis, contención y erradicación, y actividades Post-Incidente. Estos administradores podrán solicitar apoyo de un experto forense, al líder del Grupo de Atención de Incidentes en caso de no poder manejar el incidente por completo.

6.2.4. Administrador de los sistemas de Seguridad:

- Son las personas encargada de administrar, revisar y afinar los dispositivos o aplicativos de seguridad, tales como, el firewall (de perímetro externo como interno), Web Application firewall – WAF, Sistemas de Prevención de Intrusos (IPS internet, WAN y granja de servidores), protocolo de parchado, sistema de Backups, servidor AAA, routers, sistemas de Gestión y Monitoreo, herramienta de antispam y antivirus.
- Debe ser notificado por el agente de Mesa de Ayuda sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de Mesa de Ayuda sobre el incidente. Se recomienda que los administradores de esta tecnología sean conocedores de Seguridad de la Información (con un componente tecnológico fuerte en redes y erradicación de vulnerabilidades) y debe conocer perfectamente la clasificación de incidentes y los procesos de escalamiento de incidentes.

Estos actores juegan un papel fundamental en la detección de incidentes de TI, ya que ellos están en la capacidad de detectar incidentes en proceso y comenzar con los procesos de

recolección de evidencia y análisis de los incidentes. En algunos casos estarán en la capacidad de prevenir las consecuencias de un Incidente.

6.2.5. Oficial de Seguridad

Responsable por la correcta ejecución de los procedimientos de manejo de incidentes en cada una de sus etapas, coordinar actividades por parte de los responsables asignados, adicionalmente el Oficial de Seguridad de acuerdo a sus competencias y recursos deberá llevar a cabo los roles de Líder de gestión de incidente de Seguridad y Analista Forense, debido a que estos cargos no han sido incorporados dentro del manual de funciones de la Oficina Informática.

Líder de Gestión de Incidentes de Seguridad

- Responde a las consultas sobre los incidentes de seguridad de impacto crítico de forma inmediata.
- Revisa y evalúa los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos.
- Notificar en caso de que un incidente afecte un activo de información del Instituto al propietario y custodio técnico designado.
- Convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, recurso humano, Oficina Asesora Jurídica, Oficina de Control Interno, Oficina Asesora de Planeación, Líder del SGSI).
- Estar atento al cumplimiento de los perfiles mencionados y el cumplimiento de los procedimientos y mejores prácticas y de estar en capacidad de disparar si lo amerita planes de contingencia y/o continuidad.
- Responsable por la correcta ejecución de los procedimientos de manejo de incidentes, en cada una de sus etapas, coordinar actividades por parte de los responsables asignados.
- Realizar en coordinación con el Equipo de Atención de Incidentes las actividades de respuesta y tratamiento del incidente durante todo su ciclo de vida (detección y análisis, contención, erradicación, recuperación y actividades post-incidente).
- Debe verificar y estar atento a la ejecución de los procedimientos forenses para la recolección, almacenamiento y manejo de evidencia.

Analista Forense

Es un experto en el tema forense, quien debe estar disponible en caso de que un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) requiera una investigación completa para solucionarlo y determinar los siguientes Ítems

- ¿Qué sucedió?
- ¿Dónde sucedió?
- ¿Cuándo Sucedió?
- ¿Quién fue el Responsable?
- ¿Cómo sucedió?

Este actor debe ser un apoyo para los demás actores en caso de dudas sobre los procedimientos y debe ejercer un liderazgo técnico en el proceso de atención de Incidentes de seguridad de la información.

Debe contar con un profundo conocimiento forense (estudios de postgrado o certificaciones de la industria) y servir de apoyo en los procesos al interior del grupo en cuanto a capacitación continua, simulacros de incidentes para probar la capacidad del equipo y revisión de los

indicadores del equipo. Este actor se recomienda que se contrate de manera permanente y puede ser incorporado bajo un contrato de outsourcing.

6.2.6. Otros Actores

Seguridad Física: Ante un incidente de seguridad de la información, seguridad física apoyara las actividades de contención en caso de hurto o acceso no autorizado a los activos de información.

Propietario del activo: Debe participar, apoyar las actividades y acciones requeridas durante el proceso de atención del incidente. Apoya al grupo asignado en el proceso de investigación, y coordinar la ejecución de las recomendaciones.

Jurídica: Asesorar al grupo de investigación en temas de carácter jurídico, con el fin de validar las condiciones de las evidencias recolectadas, establecer el marco legal del incidente y entablar las acciones disciplinarias o demandas correspondientes.

Control Interno: Velar por la independencia de la investigación realizada y participar como un miembro del equipo de investigación asignado, cuando amerite.

6.3. 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.

7. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	06/03/2013	Creación de los lineamientos.
02	28/11/2014	Actualización Nuevo Formato de Instructivo.
03	23/11/2017	Se actualiza, versión y codificación para cumplimiento con el decreto 415.
04	10/04/2018	Actualización del documento.
05	23/10/2018	Actualización del documento.

ELABORÓ:	REVISÓ:	APROBÓ:
Luis Alejandro Pinilla Peralta **Oficial de Seguridad de la Información**	Eduardo Ramirez Acosta **Profesional Especializado Oficina de Informática**	Leonardo Cardenas Chitiva **Jefe Oficina de Informática**