1 OBJETIVO

Llevar a cabo el tratamiento de los eventos e incidentes de seguridad de la información mediante la definición de estrategias de contención para mitigar el impacto dentro de la operación de los diferentes procesos de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud.

2 ALCANCE

Inicia con el reporte del evento por parte de cualquier servidor público, contratista o tercero a través de los canales definidos en la mesa de servicio de la Dirección de Gestión de Tecnologías de Información y Comunicaciones - DGTIC, continúa con el análisis, priorización y definición de planes de acción para contención, erradicación, recuperación del (los) activo(s) de información afectado(s) y reporte ante las instancias respectivas. Finaliza con el seguimiento periódico de incidentes de seguridad con el fin de establecer planes de mejora.

3 LÍDER DEL PROCEDIMIENTO

Director Gestión de Soporta a la Tecnologías de la Dirección de Gestión Tecnología de Información y Comunicaciones

4 POLÍTICAS DE OPERACIÓN

- El presente procedimiento se encuentra alineado con el Modelo de Arquitectura Empresarial que el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC ha definido.
- Todo evento que afecte los tres pilares de la seguridad de la información: *Disponibilidad, confidencialidad e integridad*, debe ser reportado.
- Las políticas de operación del presente procedimiento se encuentran alineadas con las directrices de la Política Gestión de Eventos e Incidentes de Seguridad que se encuentran dentro de las Políticas Específicas de Seguridad y Privacidad de la Información que la Entidad ha definido.
- Para entendimiento dentro del presente procedimiento las siguientes son los 4 tipos de categorías de Eventos e Incidentes de Seguridad y Privacidad de la Información que se han definido al interior de la ADRES.

CATEGORIA	DESCRIPCIÓN	EJEMPLOS
Acceso no autorizado	Consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o contraseñas, no causando daños inmediatos y tangibles en la víctima, o bien por la	• Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos. • Fuga, robo o pérdida de Información. • Alteración o eliminación no autorizada de la información. • Ingreso de medios de almacenamiento no autorizado. • Modificación no autorizada de información • Filtración de líneas telefónicas para uso indebido • Espionaje y divulgación de información • Phishing de Redes

CATEGORIA	DESCRIPCIÓN	EJEMPLOS
	mera voluntad de curiosear o divertirse de su autor[1].	• Análisis de flujo de datos • Escaneo de redes
Códigos maliciosos	Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos[2].	• Programa Maligno conocido en inglés Malware (Ejemplos: Gusanos, Troyanos) • Spyware • Comunicaciones maliciosas (origen interno o externo) • Correos amenazantes • Botnet • Página Web con código malicioso incrustado • Sitio de alojamiento con código malicioso
Denegación de servicios	Es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos[3]. Dichos ataques se pueden llevar desde el interior o el exterior del objetivo, así como pueden ser dirigidos a un objetivo específico o a una población en general.	• Ataques de día cero • Amplificación de NTP • Saturación: UDP, Ping, Http
Uso inapropiado de recursos	Agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso y que infringen la normatividad de la empresa y las leyes.	• Abuso y mal uso de los servicios informáticos • Transmisión de material pornográfico • Transmisión de material ilegal • Transmisión de material que provoca pánico • Trasmisión de material con contenido abusivo • Préstamo de usuario y contraseña • Infracción de Políticas, normas y procedimientos de seguridad de la información • Abuso de Derechos • Falsificación de Derechos, denegación de acciones • Operaciones Incorrectas • Violación de la Disponibilidad del Personal • Instalación de software Ilegal o no autorizado • Uso indebido del software corporativo Suplantación de identidad

- Las estrategias de contención, erradicación o recuperación que pueden ser usadas en el momento en que se materialice algún incidente que se han definido para la ADRES son las siguientes.

[1] Fígoli Pacheco, A. (1999). EL ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS. Accedido desde http://www.buscalegis.ufsc.br/revistas/files/anexos/2778-2772-1-PB.html

[2] ¿Qué es el código malicioso? (2018). Accedido desde https://latam.kaspersky.com/resource-center/definitions/malicious-code

[3] ¿Qué es Ataque de denegación de servicio (DDoS)? - Definición en Whatls.com. (2018). Accedido desde https://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

CATEGORIA	CONTECIÓN	ERRADICACIÓN	RECUPERACIÓN
Acceso no autorizado	• Bloqueo de cuentas de usuario • Apagado del sistema • Desconexión de la red. • Cancelación de permisos a usuario	Instalación de parches a nivel de aplicación y sistema operativo	• Restauración de copias de respaldo. • Definición de permisos a usuario
Códigos maliciosos	• Desconexión de la red. • Apagado del sistema. • Incorporación de reglas de filtrado en el firewall	• Corrección de efectos producidos. • Instalación de parches a nivel de aplicación y sistema operativo	• Restauración de copias de respaldo • Reinstalación del equipo y recuperación de datos
Denegación de servicios	• Desconexión de la red. • Apagado del sistema.	Incorporación de reglas de filtrado en el firewall	• Restitución del servicio caído • Reinstalación del equipo y recuperación de datos
Uso inapropiado de recursos	• Incorporación de reglas de filtrado en el firewall. • Desconexión de la red. • Bloqueo de cuentas de usuario.	Ejecución código interno de Trabajo	Definición de permisos a usuario

No obstante, es viable utilizar alguna estrategia adicional que sea válida para solucionar la materialización de un incidente de seguridad de la información.

- La priorización de los eventos e incidentes de seguridad está dada por la siguiente formula:

$$Prioridad = [Impacto\ Actual * 2.5] + [Impacto\ Futuro * 2.5] + [Criticidad\ del\ activo * 5]$$

De donde:

i. **Impacto**.

Se determina por la siguiente escala.

NIVEL DE IMPACTO	VALOR	DEFINICIÓN
Inferior	0.1	Impacto leve en un activo de información.
Bajo	0.25	Impacto moderado en un activo de información.
Medio	0.5	Impacto alto en un activo de información.
Alto	0.75	Impacto moderado en más de un activo de información.
Superior	1	Impacto alto en más de un activo de información.

a. ***Impacto Actual***: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

b. ***Impacto Futuro***: Depende de la cantidad de daño que puede causar el incidente si no es contenido y erradicado.

Criticidad:
Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados. Tomando como insumo la siguiente tabla:

NIVEL DE CRITICIDAD	VALOR	DEFINICIÓN
Inferior	0.1	Activos de información no críticos, como estaciones de trabajo de usuarios con funciones no críticas
Bajo	0.25	Activos de información que apoyan a un solo proceso de la entidad.
Medio	0.5	Activos de información que apoyan más de un proceso de la entidad.
Alto	0.75	Activos de información pertenecientes a la Dirección de Gestión de Tecnologías de Información y Comunicaciones o estaciones de trabajo de usuarios con funciones críticas.
Inferior	0.1	Activos de información no críticos, como estaciones de trabajo de usuarios con funciones no críticas

Con la información definida se calcula el valor de la prioridad del evento o incidente y se valida frente a la escala *Valor*, a su vez, se estima que el tiempo de respuesta para ser atendido un incidente de acuerdo con la prioridad está dado por la escala *Tiempo de respuesta*.

PRIORIDAD	VALOR	DEFINICIÓN
Inferior	00,00 – 02,49	3 horas
Bajo	02,50 – 03,74	1 hora
Medio	03,75 – 04,99	30 min
Alto	05,00 – 07,49	15 min
Superior	07,50 – 10,00	5 min

- En la ADRES, la gestión de eventos e incidentes debe tener en cuenta las siguientes consideraciones para la recolección de evidencia en el momento en que se detecta un evento o Incidente de Seguridad o Privacidad:

  i. En el momento de hacer la recolección de la evidencia se debe tener en cuenta que existen dos tipos: (i) Identificable a simple vista. *Ej. Captura de imágenes, logs de acceso de consulta abierta*. (ii) Oculta a simple vista *Ej. Log de acceso sobre las bases de datos con acceso restringido*.
  ii. Encontrar la evidencia digital que relacione directa o indirectamente tanto un recurso tecnológico (Hardware, Software) como un usuario con el evento o incidente.
  iii. Reconstruir la sucesión de los acontecimientos a partir de los hechos sobre los cuales se encuentre evidencia obtenida de mecanismos de auditoría propios de los recursos tecnológicos involucrados.
  iv. Los hallazgos deben ser documentados mediante la utilización de imágenes y la copia de archivos que sirvan como evidencia.
  v. Los registros de auditoría (logs) de los sistemas de información, sistemas operativos, hardware, entre otros deben ser utilizados como insumo para detectar y obtener evidencia de los eventos e incidentes de seguridad, para lo cual es indispensable que se cuente con la fecha y hora de la creación y modificación (si la hay) de los registros.
  vi. El registro fotográfico y de vídeo puede llegar a ser útil para obtener evidencia frente a los eventos e incidentes de seguridad relacionados con acceso físico (autorizado y no autorizado) a las instalaciones.
  vii. Se deben evitar los siguientes errores, que son muy comunes dentro de la recolección de la evidencia a nivel de estaciones de trabajo:
    a. Añadir datos al sistema.
    b. "Terminar" procesos del sistema.
    c. Detener servicios del sistema.
    d. Usar herramientas o comandos no confiables.
    e. Actualizar el sistema operativo antes de recolectar la evidencia.

f. Continuar trabajando con el equipo luego de presentarse el incidente.
g. Apagar el equipo cuando se observa actividad sospechosa, porque esto elimina cualquier rastro del incidente y proporciona pérdida de evidencia digital que puede ser muy relevante y que está almacenada en medios volátiles como la Memoria RAM del componente.
Si es estrictamente necesario apagar la estación de trabajo, esto se debe hacer desconectando la fuente eléctrica (el cable de poder) desde la toma ubicada en la canaleta de cableado estructurado. De esta forma, es posible dejar el sistema exactamente como estaba en el último instante, evitando que él mismo realice la limpieza de datos que se hace comúnmente con el apagado normal.

- En caso de ser necesario escalar el caso, o cuando se requieren conocimientos técnicos específicos sobre la cadena de custodia de la evidencia de un incidente de seguridad, el siguiente es el directorio de contacto definido para la ADRES.

ENTIDAD	CONTACTO	
CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	Correos	ponal.csirt@policia.gov.co
	Página Web	https://cc-csirt.policia.gov.co
	Teléfonos	(+571) 5159090/ 5159586
Equipo de Respuesta a Emergencias Cibernéticas del Gobierno Nacional - CSIRT de gobierno	Correos	csirtgob@mintic.gov.co
	Teléfonos	018000910742 - opción 4
CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	Correos	contacto@colcert.gov.co
	Página Web	http://www.colcert.gov.co/
	Teléfonos	(+571) 295 98 97
Policía Nacional de Colombia	Correos	caivirtual@delitosinformaticos.gov.co
	Página Web	https://caivirtual.policia.gov.co/

- Dentro del contexto de este procedimiento, se entiende como Líder de Seguridad de la Información al Gestor de Operaciones o Contratista que desempeña las responsabilidades definidas dentro del Manual de Políticas de Seguridad y Privacidad de la Información asignadas al perfil "Líder de Seguridad".
- Dentro del contexto de este procedimiento, el **Comité de Incidentes** estará compuesto por:
  a. Director(a) de la dirección de Gestión de Tecnologías de Información y Comunicaciones
  b. Jefe de la Oficina Asesora de Planeación y Control de Riesgos.
  c. Jefe de la Oficina de Control Interno.
  d. Director(a) de la dirección Administrativa y Financiera
- El presente procedimiento está alineado con los siguientes objetivos de controles ISO 27000:
  (i) A16.1.1 - Responsabilidades y procedimientos. Determina los diferentes responsables que están involucrados dentro de la gestión de incidentes dentro de la organización.
  (ii) A16.1.2 - Notificación de los eventos de seguridad de la información. Detalla la forma en cómo se debe hacer la notificación y seguimiento de los casos expuestos.
  (iii) A16.1.5 - Respuesta a los incidentes de seguridad. Detalla la forma en cómo se debe hacer el cierre de los incidentes de seguridad.

5 REQUISITOS LEGALES: Ver Normograma del proceso.

6 DEFINICIONES: Ver glosario general.

7 DESARROLLO DEL PROCEDIMIENTO

No	Actividad	Descripción de la Actividad	Responsable	Registro
1	Identificar y asignar el evento de Seguridad y Privacidad de la Información	El encargado de soporte de primer nivel o de segundo nivel, una vez que un caso ha sido catalogado como Incidente de Seguridad conforme con el procedimiento de Gestión de Incidentes, asigna el caso al Líder de Seguridad de la Información dentro del Módulo de Mesa de Servicio.	Gestor Operativo Encargado de Soporte primer nivel/Encargado de Soporte segundo nivel	Caso dentro del Módulo de Mesa de Servicio
2 **PC**	Validar pertinencia de clasificación	Una vez se le haya asignado un caso, con el propósito de determinar si es un Incidente de Seguridad toma como insumo las categorías de incidentes definidas en las políticas de operación del presente procedimiento. ¿Es considerado como evento o incidente de Seguridad? **SI**: Se continuará con la siguiente actividad y adicionalmente se reportará la materialización de un Riesgo de Seguridad de la Información conforme con lo definido en el procedimiento de gestión de riesgos. **NO:** Se recategorizará el caso determinando si es un requerimiento o incidente conforme con lo definido dentro del procedimiento gestión de requerimientos. Toda acción realizada deberá quedar registrada dentro del Módulo de Mesa de Servicio.	Líder de Seguridad de la Información	DIES-FR14 Registro de materialización de riesgo Caso recategorizado dentro del Módulo de Mesa de Servicio
3	Recolectar y manejar evidencia del evento de Seguridad y Privacidad de la información	El Líder de Seguridad de la Información junto con las personas que este crea pertinentes, una vez ha confirmado el evento o incidente de Seguridad de la Información inicia la recolección de pruebas realizando la debida cadena de custodia de la(s) evidencia(s). Para esto debe tomar las consideraciones definidas dentro de la política de operación del presente procedimiento frente a la recolección de evidencia. Adicionalmente, si se requiere se puede solicitar apoyo de las entidades especializadas en recolección de información como evidencia forense.	Líder de Seguridad de la Información	Pruebas recolectadas
4 **PC**	Valorar criticidad y nivel de del incidente de	El Líder de Seguridad de la Información, una vez cuente con la evidencia necesaria del Evento o Incidente de Seguridad, con el propósito de definir la priorización para la	Líder de Seguridad de la Información	Caso valorado en el Módulo de

No	Actividad	Descripción de la Actividad	Responsable	Registro
	Seguridad de la Información	resolución de este; establece tanto el impacto como la criticidad conforme con las políticas de operación definidas en el actual procedimiento. ¿Es priorizado con nivel Alto o Superior? **SI:** el Líder de Seguridad de la Información le notificará al director de Gestión de Tecnología de Información y Comunicaciones para que convoque vía correo electrónico o telefónicamente el [COMITÉ DE INCIDENTES] para que de manera conjunta se determine las acciones a seguir. **NO**: Será el Líder de Seguridad de la Información junto con las personas que crea pertinentes quienes definirán el plan a seguir. Toda evidencia frente a la priorización del incidente deberá ser relacionada dentro del caso en el Módulo de Mesa de Servicio.		Mesa de Servicio Correo electrónico de Convocatoria COMITÉ DE INCIDENTES.
5	Definir estrategia de contención	Los responsables que se hayan determinado después de la valoración del incidente de Seguridad de la Información, con el propósito de realizar las recuperaciones necesarias, definen la estrategia de contención del incidente. Para lo cual, se debe tener en cuenta: i. Daño potencial de activos de información por causa del evento o incidente teniendo en cuenta la criticidad del activo. ii. Preservación de la evidencia. iii. Tiempo y recursos internos y externos necesarios para la estrategia. iv. Efectividad de la estrategia. v. Duración estimada de las medidas a tomar. vi. Características de las posibles fuentes de ataque. vii. Activación del Procedimiento de Recuperación de desastres. viii. Tiempo (Hábil y no hábil) para llevar a cabo la solución. ix. Recurso humano necesario para implementar la solución. Este recurso está tanto a nivel técnico como operativo. x. Implicaciones reputacionales, económicas y legales. xi. Definir y notificar a responsables para llevar a cabo la estrategia de solución Adicionalmente, se deben definir si se requiere o no ejecutar alguna acción desde	[COMITÉ DE INCIDENTES] o Líder de Seguridad de la Información	GEDO-FR05 "Formato acta de reunión"

No	Actividad	Descripción de la Actividad	Responsable	Registro
		el componente legal y contractual o a nivel de pólizas de Seguros, para lo cual se comunicará al jefe de la oficina Asesora Jurídica y/o al Director Administrativo y Financiero según corresponda, para que se definan la actuación a seguir. Como soporte a esta actividad quedará la definición de la estrategia dentro del formato de acta de la ADRES		
6	Implementar solución frente al evento o incidente de seguridad	El responsable que se definió como necesario para la implementación de la estrategia de solución, ejecuta la estrategia definida en la actividad anterior. La evidencia de las acciones ejecutadas debe ser registrada en el Módulo de Mesa de Servicio. En caso de presentarse alguna incidencia relevante en el momento de estar desarrollándose las actividades definidas, se debe comunicar inmediatamente al grupo que definió la solución para replantear las acciones a seguir.	Gestor (es) Operativo (s), contratistas o terceros responsable de la estrategia de solución	Caso en el Módulo de Mesa de Servicio
7	Reportar a las instancias respectivas	El director de la DGTIC para incidentes de Seguridad catalogados como alto o superior o el Líder de Seguridad de la Información para los demás incidentes, una vez se inicie la estrategia de solución frente al evento o incidente de seguridad y con el fin de dar cumplimiento al reporte ante instancias respectivas, cuando aplique, realizará la novedad respectiva, conforme con lo definido en las políticas de operación del presente procedimiento.	Director DGTIC	Soporte de registros en los canales de reporte instancias respectivas
8	Realizar seguimiento posterior a los incidentes de seguridad	Periódicamente el Líder de Seguridad de la Información junto con el grupo de trabajo que el director de la DGTIC designe analizan los eventos e incidentes que se hayan presentado para: i. Definir esquemas más efectivos con el fin de responder ante situaciones que afecten la seguridad y la privacidad de la información dentro de la entidad. ii. Mantener la documentación de los eventos e incidentes de seguridad y privacidad de la Información. iii. Mantener actualizada las bases de datos de conocimientos. iv. Evaluar avances frente a los planes de mejora producto de la materialización de riesgos de Seguridad de la Información. v. Incluir dentro de las capacitaciones que se definan en el marco del Plan de Seguridad y Privacidad de la información de la entidad	Líder de Seguridad de la Información	GEDO-FR05 "Formato acta de reunión"

No	Actividad	Descripción de la Actividad	Responsable	Registro
		sensibilización y lecciones aprendidas relacionas a eventos e incidentes de Seguridad de la Información. Los avances y tareas que se definan dentro de dichas reuniones deberán quedar registradas dentro del formato de acta vigente que tenga definido la Entidad; esta información será entregada al director de Gestión de Tecnología de Información y Comunicaciones para que dentro de los comités correspondientes o en la definición de planes institucionales sean tenidos en cuenta los hallazgos identificados y solucionados dentro del objeto de la presente actividad. **FIN DEL PROCEDIMIENTO**		

8 CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Asesor del proceso
01	29 de junio de 2018	Emisión y Publicación inicial	Johanna Bejarano Gestor de Operaciones -OAPCR
02	08 de noviembre de 2019	Actualización del procedimiento de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 del Departamento Administrativo de la Función Pública – DAFP. Se redefinen las actividades del procedimiento en general teniendo en cuenta la inclusión de la Mesa de Servicios de la Dirección de Gestión de Tecnologías de Información y Comunicaciones. Eliminación de la guía Consideraciones para eventos e incidentes de seguridad y privacidad de la información incluyendo los aspectos básicos de esta dentro de las políticas de operación del presente procedimiento.	Ricardo Andrés Varón Villareal. Gestor de Operaciones – OAPCR
03	*18 de marzo de 2020*	Actualización de las políticas de operación teniendo en cuenta versión del Modelo de Arquitectura Empresarial definido por el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC.	Olga Marcela Vargas Asesor OAPCR
03	*9 de julio de 2020*	Actualización código por cambio de nombre del proceso de GSTE a OSTI. No se genera nueva versión debido a que no se modifica contenido del procedimiento y por lo tanto no requiere aprobación por parte del líder del proceso.	Olga Vargas Asesor OAPCR

9 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Juan Carlos Escobar Baquero Gestor de Operaciones - Dirección de Gestión de Tecnologías de Información y Comunicaciones	**Carlos Andrés Ruiz Romero** Gestor de Operaciones – Grupo Gestión Soporte a las Tecnologías	**Sergio Andrés Soler Rosas.** Director de Gestión de Tecnologías de Información y Comunicaciones