


|   |   |                                     |
|---|---|-------------------------------------|
|  | <b>CORPORACIÓN DE CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO DE LA INDUSTRIA NAVAL MARÍTIMA Y FLUVIAL</b>  |                                     |
|   | <b>PROCEDIMIENTO PARA VERIFICAR Y EVALUAR LOGS DE AUDITORIA GENERADOS POR HERRAMIENTAS TECNOLÓGICAS</b> |                                     |
| Código: P-GESTIC-016  | Versión: 0  | Fecha de Aprobación:<br>18/Sep/2017 |

### 1. OBJETIVO:

Definir los lineamientos necesarios para abordar el tema de evaluación y verificación de logs de auditoria, generados por las plataformas tecnológicas utilizadas en la Corporación de Ciencia y Tecnología Para el Desarrollo de la Industria Naval, Marítima y Fluvial – COTECMAR, estableciendo dentro de éste procedimiento, la periodicidad que debe manejarse con respecto a éste tema.

### 2. ALCANCE:

Aplica para todos los sistemas de información, activos de información y plataformas tecnológicas que tengan activada la opción de generación de logs de auditoria, para lo cual, cada administrador de plataforma activará el procedimiento indicado en el presente documento, con el fin de mantener una verificación y seguimiento constante de los registros que puedan catalogarse como críticos en la plataforma evaluada. De igual forma, éste procedimiento deberá ser activado, cuando se considere que se presentó algún tipo de afectación de la plataforma tecnológica que los genera, siguiendo secuencialmente todos los pasos que se encuentran plasmados en el presente procedimiento.

### 3. CONDICIONES GENERALES:

Este procedimiento se aplica siempre y cuando la plataforma tecnológica o activo de información, se encuentre operativa y solo para los servidores y/o equipo que se encuentren configurados en dicha plataforma.

Garantizar la aplicación de un procedimiento estandarizado y reconocido corporativamente, para el tema de análisis y evaluación de logs de auditoria, ya que estos se constituyen en evidencia para la identificación de un incidente de seguridad.

El estado de los logs para todos los componentes de la plataforma tecnológica que apliquen este procedimiento, debe:

- Asegurar que están activos
- Configurados apropiadamente
- Funcionando como se espera

Los administradores de las plataformas de negocio y apoyo corporativo (ERP, Nómina, Diseño y las que se consideren neurálgicas), deberán registrar como mínimo una vez al mes, un requerimiento de verificación y evaluación de los logs de conectividad y acceso a las plataformas; lo anterior considerando que COTECMAR acoge como buena práctica de seguridad, la evaluación y verificación de las conexiones a las plataformas tecnológicas de soporte al negocio.

#### 4. DEFINICIONES:

**ACTIVO DE INFORMACIÓN:** Todo aquel elemento en que se procesa, almacena o transmite información y que tiene un valor para la Entidad. Ej. Bases de datos, programas de computación, plataforma tecnológica (procesamiento de datos, comunicaciones o seguridad informática), documentos impresos, recursos humanos, entre otros. [BASADO EN ISO 13335].

**ARCHIVO:** Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad, en el transcurso de su gestión, conservados para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia.

**IMPACTO:** Magnitud de la materialización del riesgo.

**INFORMACION:** Datos que poseen significado. Definición tomada de la Norma Técnica Colombiana NTC-ISO9000:2005, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

**LOG:** Es el registro de las acciones y de los acontecimientos que ocurren en una sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica.

**ADMINISTRACIÓN DE LOG:** Proceso mediante el cual se realiza la generación, transmisión, almacenamiento, análisis, monitoreo y reporte de los Logs.

**ANÁLISIS DE LOG:** Estudio de los Logs para identificar eventos de interés o suprimir entradas de eventos insignificantes.

**EVENTO TECNOLÓGICO:** Una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.

**EVIDENCIA DIGITAL:** Información con valor probatorio almacenada o transmitida en forma digital.

**INCIDENTE TECNOLÓGICO:** Es un evento o serie de eventos de seguridad de la información no deseado o no planeado, que afecte la prestación del servicio o reduzca la calidad de la prestación del servicio o que tenga una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

#### 5. DOCUMENTOS DE REFERENCIA:

- ▶ [DIRECTIVA PERMANENTE N° 043 PCTMAR-VPEXE OPTIC - Políticas de seguridad de la información para COTECMAR](#)

#### 6. RESPONSABLES:

- Jefe Oficina De Tecnologías De La Información Y Comunicaciones
- Líder Seguridad de la Información.

## 7. DESCRIPCIÓN NARRATIVA:

7.1 CONTEXTO DE TRABAJO: El contexto en el cual se realiza el trabajo en el que se aplica el presente procedimiento, está delimitado, por el conjunto de aplicaciones y plataformas tecnológicas que dentro de su esquema operativo tienen implementado una metodología de generación de logs de trazabilidad de conectividad y/o de transaccionabilidad.

7.2 INICIO DEL PROCEDIMIENTO: Para el inicio del presente procedimiento, se debe considerar, que dentro del cumplimiento y ejecución de éste, se plantea la siguiente periodicidad para las plataformas y aplicaciones que son empleadas para el cumplimiento de las actividades misionales y de apoyo de la corporación, así:

- Aplicaciones operativas (Aveva), Mensualmente, los primeros 5 días del mes, para lo cual, el administrador de la plataforma, generará el archivo de LOGS, y continuará con el procedimiento establecido.
- Aplicaciones administrativas (ERP y Nómina), Mensualmente, los primeros 5 días del mes, para lo cual, cada administrador de plataforma, generará el archivo de LOGS, y continuará con el procedimiento establecido.
- Aplicaciones de Apoyo: Para el caso de las aplicaciones de apoyo, se deberá generar el archivo de LOGS que se requiere analizar, en el momento que sea requerido y/o por solicitud del gerente de la dependencia usuaria o por solicitud del administrador de la plataforma, quien deberá especificar dentro del requerimiento que debe subir a SIMAC, que es lo que se está buscando y cuales son los indicios que soportan éste requerimiento.

7.3 GENERACIÓN DEL ARCHIVO DE LOGS: Es responsabilidad del administrador de la plataforma ó herramienta tecnológica, el generar el archivo de LOGS y registrar el requerimiento de evaluación y verificación del mismo en la herramienta SIMAC; para ésta actividad, deberá emplear las opciones que cada plataforma o herramienta tienen prevista para ésta actividad, verificando que como mínimo, para las actividades de verificación y trazabilidad, tengan como mínimo los siguientes datos:

- Fecha de conexión
- Hora de conexión
- Usuario
- Sistema accedido
- Transacción realizada
- Terminal utilizada

7.4 REGISTRO DEL REQUERIMIENTO EN SIMAC: Posterior a la generación de los archivos de LOGS, el administrador de la plataforma o sistema de información, deberá realizar el registro en la plataforma SIMAC, para lo cual deberá especificar, el motivo por el cual realiza éste requerimiento en el sistema y en caso de ser diferente a un requerimiento rutinario, indicar las circunstancias que se consideraron o conllevaron a realizar éste tipo de requerimiento.

**7.5 RECEPCIÓN Y VALIDACION DEL ARCHIVO DE LOGS:** Posterior a la inscripción del registro en la plataforma SIMAC, el funcionario a cargo del área de Seguridad de la Información, realizará una validación del requerimiento y del archivo recepcionado, con el fin de realizar una validación inicial del estado y contenido del archivo y determinar si es útil para abordar y dar respuesta a los requerimientos planteados en el registro SIMAC; de requerirse o si no es claro el requerimiento o archivo, el analista de seguridad solicitará nuevamente el archivo al administrador de la plataforma y cargará el nuevo archivo a la plataforma SIMAC, para continuar con el flujo del proceso.

**7.6 VERIFICACIÓN Y BÚSQUEDA DE REGISTROS SOSPECHOSOS:** En el desarrollo de éste punto, el analista de seguridad de la información, realiza la verificación, búsqueda y correlación de los registros que se encuentran en el archivo recibido en el requerimiento; de no ser un requerimiento rutinario de control, tomará como base de evaluación, los indicios y/o requerimientos puntuales del administrador de la plataforma, con el fin de encaminar el esfuerzo de búsqueda, a la puntualización de los factores expuestos por el administrador. Dentro del desarrollo de ésta actividad, el analista de seguridad de la información, establece si hay o no mérito para continuar con una evaluación y correlación mas profunda de los eventos identificados, para lo cual continua con el flujo del proceso; de no encontrar méritos de valor, registra sus conclusiones en la plataforma SIMAC, cierra el caso y da por terminado el proceso de evaluación y seguimiento.

**7.7 ACCIONES DE COORDINACIÓN CON EL ADMINISTRADOR DE LA PLATAFORMA:** Cuando el proceso de verificación y búsqueda de registros sospechosos, se encuentra algún registro que amerite la activación de acciones mas puntuales, por parte de los administradores de la plataforma o sistema de información analizado, el analista de seguridad de la información establecerá un canal directo con el administrador de la plataforma, con el fin de solicitar nuevos registro o la opinión técnica sobre el hallazgo identificado.

**7.8 GENERACIÓN Y EVALUACIÓN PROFUNDA DE LOGS Y SEGUIMIENTO TRANSACCIONAL:** Posterior a las coordinaciones que realiza el analista de seguridad de la información, con el administrador de la plataforma, se realiza la generación de nuevos registros de logs, puntualizando en transacciones críticas de la plataforma evaluada, con el fin de establecer un nivel de relación entre los hallazgos y las actividades transaccionales puntuales, determinando un nivel de criticidad e impacto dentro de la plataforma o sistema de información analizada.

**7.9 TOMA DE ACCIONES DE MITIGACIÓN Y BLOQUEO DE EVENTOS IDENTIFICADOS:** Cuando el hallazgo da lugar a la activación de acciones de mitigación y bloqueo, el analista de seguridad de la información, en coordinación el con administrador de la plataforma y/o sistema de información afectado, determinan las acciones a seguir y definen los bloqueos que hay que aplicar, para contener las acciones que puedan generarse por los accesos y modificaciones que se identificaron en la actividad de análisis y evaluación.

**7.10 EXPOSICIÓN DEL HALLAZGO Y ACCIONES TOMADAS:** El objetivo principal del desarrollo de ésta actividad, es mantener informado al propietario de la información, sobre las actividades identificadas y las acciones iniciales tomadas, con el fin de que por ningún motivo, se presente desinformación y/o mal manejo del evento.

7.11 EVALUACIÓN DE ACCIONES DE CAUSA Y EFECTO DEL HALLAZGO: Dentro de la ejecución del proceso abordado, se considera integrar la evaluación de impacto y ejecución de actividades de mitigación, para lo cual, se evalúa en profundidad, las circunstancias de causa y efecto de los hallazgos identificados, para lo cual, el analista de seguridad y el administrador de la plataforma, plantean una serie de ideas, que conllevaron a la materialización del evento identificado; posteriormente, se adelanta una evaluación de las acciones tomadas, determinando que éstas son lo suficientemente efectivas, para evitar que el evento identificado que materialice nuevamente, para lo cual, se realizan actividades de eficiencia de las acciones tomadas, con el fin de determinar que si son eficientes para frenar el evento identificado.

7.12 DILIGENCIAMIENTO FORMATO DE REPORTE DE INCIDENTE DE SEGURIDAD: Considerando que los procedimientos asociados a la seguridad de la información, están alineados con las políticas de seguridad de la información corporativa, posterior al proceso de contención y mitigación del incidente de seguridad, se debe diligenciar el formato de "Reporte de incidente de seguridad de la información", actividad que debe ser adelantada por el líder de seguridad de la información y el administrador de la plataforma o sistema de información afectado, para posteriormente radicarlo en la Oficina de Tecnologías de la Información y de requerirse, sea expuesto ante el comité de seguridad de la información.

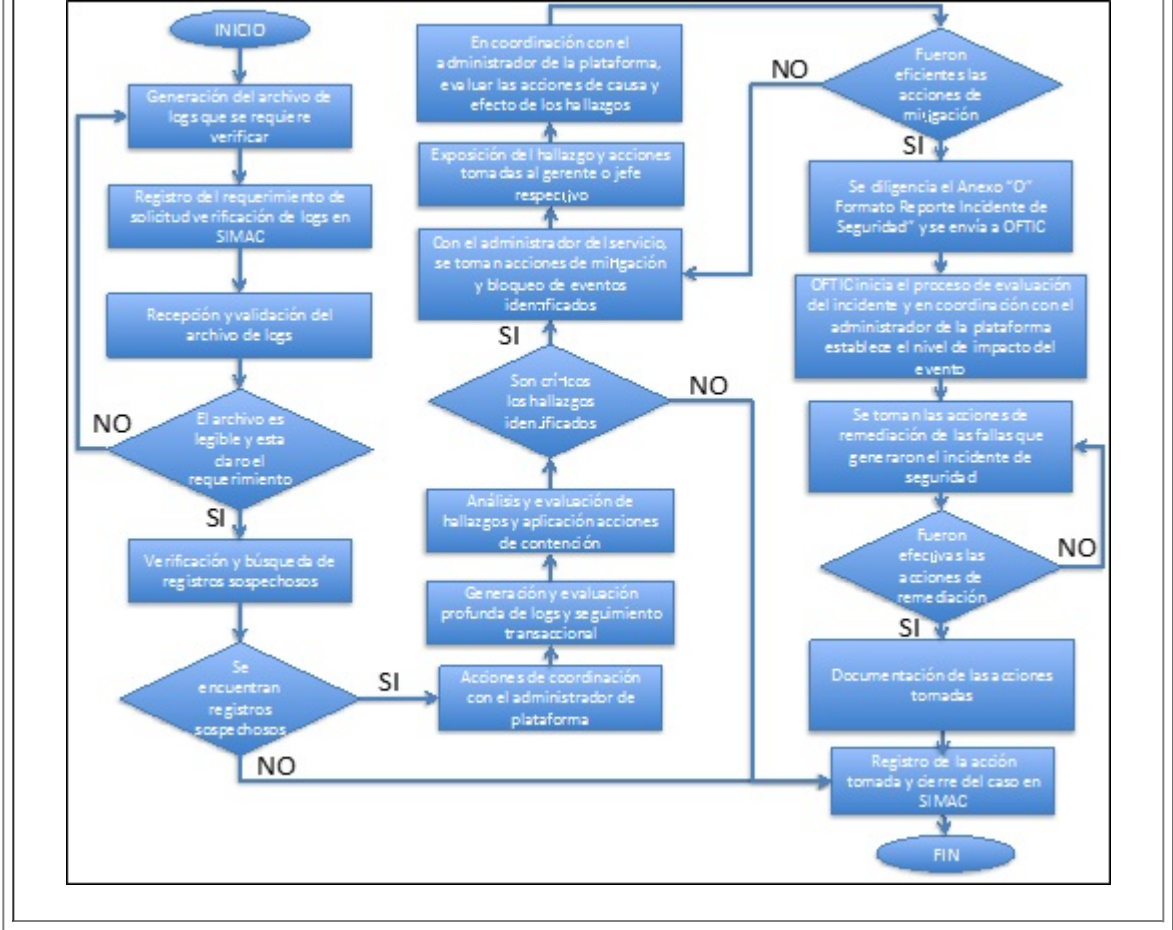
7.13 EVALUACIÓN DEL INCIDENTE Y DEFINICIÓN DEL NIVEL DE IMPACTO DEL EVENTO: El objetivo de ésta actividad, es determinar las causas probables del incidente y el impacto que se genera por la materialización del eventontecnologico, determinando en costo reputacional, financiero y/u operativo, el alcance de la materialización del evento, planteando acciones de remediación para que éste no se presente nuevamente.

7.14 TOMA DE ACCIONES DE REMEDIACIÓN DEFINITIVA DEL EVENTO: Como actividad de valor del presente procedimiento, está la toma de acciones de remediación del evento, el cual no solo se enfoca en la plataforma o sistema de información afectado, sino también en las plataformas y sistemas que interactúan con la plataforma afectada, para lo cual, el analista de seguridad de la información, entrará en contacto directo con los administradores de las demás plataforma y coordinará la aplicación de reglas, restricciones y filtros necesarios, para evitar que el hallazgo identificado se replique a otras plataformas y/o sistemas de información; ésta actividad se debe revisar y evaluar, hasta que el incidente queda plenamente subsanado en todas las plataformas.

7.15 DOCUMENTACIÓN DE LAS ACCIONES TOMADAS: Posterior a las acciones de contención, mitigación y remediación del evento, se consolida el formato de "Reporte de incidente de seguridad de la información", el cual obra como archivo documental del incidente identificado, el cual deberá reposar en la carpeta de documentación de incidentes.

7.16 REGISTRO DE ACCIONES TOMADAS Y CIERRE DEL CASO EN SIMAC: Una vez concluida la actividad de documentación, se deberá registrar en SIMAC, las acciones tomadas sobre el caso de verificación de LOGS, haciendo un resumen de las acciones tomadas, para posteriormente cerrar el caso.

7.17 FLUJOGRAMA: Flujograma Procedimiento para Verificar y Evaluar Logs de Auditoría



8. ASPECTOS AMBIENTALES:

N/A

9. ASPECTOS DE SEGURIDAD Y SALUD EN EL TRABAJO:

Ver MATRIZ DE IDENTIFICACIÓN DE PELIGROS, VALORACIÓN Y EVALUACIÓN DE RIESGOS

10. REGISTROS Y ANEXOS:

N/A

LISTA DE VERSIONES

| VERSIÓN                        | FECHA                                    | RAZÓN DE LA ACTUALIZACIÓN               |
|--------------------------------|--|---|
| ELABORÓ                        | REVISÓ                                   | APROBÓ                                  |
| Nombre: Indiris Peroza Taborda | Nombre: CC Rafael Antonio Velasco Gaitan | Nombre: Angelica Maria Silva de la Ossa |

|  |   |  |
|--|---|--|
| <b>Cargo:</b> Analista<br>Gestion De<br>Calidad<br><b>Fecha:</b> 13/Jun/2017 | <b>Cargo:</b> LÍDER FUNCIONAL<br>FI<br><b>Fecha:</b> 27/Jul/2017<br><br><b>Nombre:</b> CN Carlos Daniel<br>Isaza Morales<br><b>Cargo:</b> JEFE OFICINA DE<br>TECNOLOGÍAS DE<br>LA INFORMACIÓN<br>Y<br>COMUNICACIONES<br><b>Fecha:</b> 15/Sep/2017 | <b>Cargo:</b> LÍDER GESTIÓN<br>DE CALIDAD<br><b>Fecha:</b> 18/Sep/2017 |
|--|---|--|