1. **OBJETIVO:** Establecer los pasos necesarios para la identificación y tratamiento de eventos y alertas de TI en caso de que un servicio y/o sistema de información presente condiciones inusuales de operación.

2. **ALCANCE:** Inicia con la generación del evento hasta el cierre y/o escalamiento del mismo. El documento aplica a nivel Nacional.

3. **POLÍTICAS DE OPERACIÓN:**
   - El procedimiento de gestión de eventos y alertas debe ejecutarse de manera continua durante la operación de la infraestructura, plataforma y/o servicios de TI.
   - Toda gestión de eventos y alertas realizada por el Centro de Operaciones de Seguridad (SOC) debe enmarcarse en el actual procedimiento.
   - Los eventos de tipo “Advertencia alta” y/o “excepción” que hayan sido correlacionados y que el análisis correspondiente identifique como potenciales incidentes de seguridad, deberán ser gestionados como incidentes de seguridad de la información para una adecuada y oportuna atención.

4. **DESCRIPCIÓN DE ACTIVIDADES:**

No	Actividad	Descripción de la actividad	Responsable	Registro
		Inicio		
1	Notificar evento	La notificación del evento puede darse en dos vías, una pasiva o una activa. • Para la notificación activa, el elemento de configuración a monitorear envía información referente a una situación de interés previamente establecida al colector de eventos. • Para la notificación pasiva, el colector de eventos realiza una consulta directa sobre el elemento de configuración a monitorear y toma de este la información de interés de acuerdo a parámetros previamente establecidos.	Operador de TI	Notificación registrada en la base de datos colectores de eventos (SIEM)
2	Detectar evento	Una vez se genera la notificación en la base de datos del colector de eventos, esta es detectada por la herramienta SIEM para su correspondiente registro.	Operador de TI	Base de datos SIEM
3	Filtrar evento	Posterior a la detección de los eventos, la herramienta de SIEM realiza un filtrado de los mismos para descartar los que no son de relevantes o falsos positivos de acuerdo a las reglas de filtrado preestablecidas en la herramienta.	Operador de TI	Base de datos SIEM
4 P.C	Categorizar evento	La categorización se realiza de acuerdo a su severidad. Puede darse manual (Intervención humana) o de forma automatizada (Herramienta de SIEM). Las severidades establecidas son las siguientes:	Operador de TI	Base de datos SIEM

No	Actividad	Descripción de la actividad	Responsable	Registro
		• Informativo: Son eventos que no requieren acción alguna. Son almacenados la base de datos del SIEM sin ningún tipo de tratamiento. *Si un evento es categorizado como informativo, se pasa a la actividad 10 del procedimiento.* • Advertencia[1]: Son eventos generados cuando el comportamiento de un servicio y/o dispositivo se aproximan a un umbral predefinido. Cuando se llega a este nivel, la comunicación pude darse a un sistema, grupo o persona responsable del dispositivo y/o servicio para su gestión antes que ocurra una excepción. *Si un evento es categorizado como Advertencia, se pasa a la actividad 6 del procedimiento.* • Excepción: Se presenta cuando un dispositivo o servicio se encuentra operando fuera de los rangos normales de operación establecidos (SLAs, OLAs, niveles mínimos y máximos de servicio, entre otros). *Si un evento es categorizado como Excepción, se pasa directamente a la actividad 6.*		
5	Correlacionar evento	El ciclo de correlación de eventos se lleva a cabo bajo los siguientes parámetros: • Con reglas de negocio (Comportamiento de tráfico, flujos de información, activos críticos, entre otros). • Sin reglas de calificación de riesgo para identificar posibles amenazas en tiempo real. Esta correlación puede realizarse de forma automática o manual (Intervención humana). La correlación manual puede ser realizada también de forma conjunta con los diferentes especialistas de TI y/o seguridad debido a su conocimiento del contexto tecnológico del ICBF.	SIEM Especialista / Analista de TI del Operador de TI Especialista de Seguridad Informática del Operador de TI Analista SOC del Operador de TI	Base de datos SIEM F1.P11.GTI Formato bitácora de eventos SOC
6 P.C	Lanzar respuesta	Si la actividad de correlación reconoce un evento de interés, se debe dar una respuesta a este antes que sea generada una excepción sobre los sistemas y servicios del ICBF monitoreados por el SOC. De acuerdo al tipo de evento pueden darse las siguientes respuestas	SIEM Analista SOC del Operador de TI	Ticket generado en módulo de autoservicio

[1] Para el SOC la categoría de advertencia se divide en baja y alta.

No	Actividad	Descripción de la actividad	Responsable	Registro
		(as cuales deben ser registradas por parte de los analistas del SOC en la bitácora de eventos del SOC): • **Alerta e intervención humana:** Una vez el evento es detectado, este puede ser escalado de forma automática por el SIEM a la mesa de servicio para que se tome acción o de forma manual por los analistas del SOC del proveedor de servicios de TI a través de correo electrónico a los especialistas de TI del proveedor de servicios de TI. Si para dar una respuesta efectiva al evento es requerido el desplazamiento de soporte en sitio para dar atención o un diagnóstico, se realiza el escalamiento correspondiente al Profesional de la Subdirección de Recursos Tecnológicos que apoya la supervisión del servicio de seguridad informática. • **Respuesta automática:** Cuando el evento ya es conocido, así como su tratamiento, la respuesta puede ser dada de manera automatizada si el servicio o elemento de configuración en cuestión reacciona automáticamente al evento (Reinicio de un sistema, bloqueo de un puerto, activación de respaldo, entre otros). • **Gestión de incidentes, problemas y/o cambios:** Algunos eventos presentan situaciones que requieren que sean tratados a través de otros procedimientos debido a su severidad, complejidad y/o impacto. El tratamiento o respuesta puede darse en términos de los procedimientos de incidentes, problemas o cambios. El Profesional de la Subdirección de Recursos Tecnológicos que apoya esta actividad, es quien apoya la supervisión del servicio de seguridad informática.	Especialista de TI del Operador de TI Especialista de Seguridad del Operador de TI Gestor Seguridad Informática del Operador de TI Oficial de seguridad de la Información del Operador de TI Profesional de la Subdirección de Recursos Tecnológicos de la SDG	Correo electrónico de escalamiento de evento F1.P11.GTI Formato bitácora de eventos SOC
7	Revisar respuesta	Los eventos tipo “Advertencia - baja”, “Advertencia – alta” o de excepción deben ser revisados semestralmente para identificar tendencias, estadísticas y oportunidades de mejora. La revisión será realizada por los diferentes especialistas de acuerdo al elemento de configuración asociado al evento registrado. Esta información puede ser tomada de la herramienta de gestión de servicios o de la bitácora de eventos del SOC. El Profesional de la Subdirección de Recursos Tecnológicos que apoya esta actividad, es quien	Especialista de TI del Operador de TI Especialista de Seguridad del Operador de TI Gestor Seguridad Informática del Operador de TI Oficial de seguridad de la Información del Operador de TI	F9.P1.MI. Formato acta de reunión

No	Actividad	Descripción de la actividad	Responsable	Registro
		apoya la supervisión del servicio de seguridad informática.	Profesional de la Subdirección de Recursos Tecnológicos de la SDG	
8	Avalar cierre de evento	Una vez tratado el evento, los responsables de dar atención al mismo (De acuerdo al tipo de elemento de configuración afectado) proceden a dar el aval de cierre correspondiente vía correo electrónico al Analista SOC del proveedor de servicios de TI. El Profesional de la Subdirección de Recursos Tecnológicos que apoya esta actividad, es quien apoya la supervisión del servicio de seguridad informática.	Especialista de TI del Operador de TI Especialista de seguridad del Operador de TI Gestor Seguridad Informática del Operador de TI Oficial de seguridad de la Información del Operador de TI Profesional de la Subdirección de Recursos Tecnológicos de la SDG	Correo electrónico
9	Cerrar evento	Una vez dado el aval de cierre del evento, el analista de SOC procede a realizar el respectivo cierre en la bitácora de eventos del SOC.	Analista SOC del Operador de TI	F1.P11.GTI Formato bitácora de eventos SOC
		Fin		

P.C.: Punto de Control

5. **RESULTADO FINAL:** Evento identificado, registrado, tratado y cerrado.

6. **DEFINICIONES:**
   - **Evento –** Un cambio de estado que tiene un significado para la administración de un elemento de configuración o servicio.
   - **Trigger –** Es un indicador que una acción o respuesta a un evento es necesario.
   - **Alerta –** Es una advertencia que un umbral ha sido alcanzado o algo ha cambiado (Un evento ha ocurrido).
   - **SIEM –** Es una herramienta de gestión de incidentes y eventos de seguridad, la cual tienes diferentes componentes como colectores, motor correlacionador, aplicación de eventos e incidentes y bases de datos. Es el corazón del servicio de SOC.
   - **SOC –** Centro de operaciones de seguridad, encargado de monitorear la seguridad informática del ICBF y generar alertas y eventos en caso de que se identifique situaciones que afecten la seguridad del ICBF.
   - **SDG:** Sede de la Dirección General.
   - **Elemento de configuración:** Elemento presente en el entorno tecnológico y es importante controlar para proporcionar un servicio (Por ejemplo, servidores, aplicaciones, equipos de seguridad informática entre otros).

- **Condiciones inusuales de operación:** Resultados obtenidos frente a los estándares de diseño, acuerdos de niveles de servicio, acuerdos de nivel de operación u otras condiciones tecnológicas establecidas, con el propósito de mantener la confidencialidad, integridad y disponibilidad de los activos de información monitoreados por el servicio de SOC del ICBF.
- **Herramienta de Gestión de Servicios:** Son todos los sistemas, aplicaciones, controles, soluciones de cálculo, metodología, etc., que ayudan a la gestión de una empresa; para el caso de TI para el manejo y control de servicios es el software en donde se documentan los servicios de gestión tecnológica como Incidentes, Requerimientos, Problemas, Controles de Cambios, etc, todas estas correspondientes a Tecnologías de Información; algunas de las Herramientas que se encuentran hoy en día en el mercado son:
  - Altiris de Symantec • IBM Service Management de IBM
  - CA Service Desk Manager de CA Technologies
  - Service Manager de Hewlett Packard
  - Aranda's Service Desk de Aranda Software
- Mesa de Servicio: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Dirección de Información de Tecnología se informa de las necesidades que tienen los funcionarios en cuanto a los recursos informáticos a nivel nacional.

7. DOCUMENTOS DE REFERENCIA:

- Guía técnica colombiana GTC-ISO/IEC 27035.
- Norma técnica colombiana NTC-ISO-IEC 27001.
- P3.GTI Procedimiento Gestión de Cambios de Emergencia de Tecnologías de la Información.
- P4.GTI Procedimiento Gestión de Cambios de Tecnologías de la Información.
- P5.GTI Procedimiento Gestión de Incidentes de Seguridad de la Información.
- P7.GTI Procedimiento de Gestión de Problemas de Tecnología.

8. RELACIÓN DE FORMATOS:

CÓDIGO	NOMBRE DEL FORMATO
F9.P1.MI.	Formato acta de reunión
F1.P11.GTI	Formato bitácora de eventos SOC

9. ANEXOS:

N/A

10. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio

30/06/2017	P11.GTI V1	Elaboración del documento
30/06/2017	P11.GTI V1	Se actualiza rotulado de información de acuerdo con lo dispuesto en la Guía para la rotulación de la información.
26/03/2017	P11.GTI V2	Se realiza ajuste en los responsables de las actividades, de acuerdo con las orientaciones brindadas por la Subdirección de Mejoramiento Organizacional para el Levantamiento de Cargas.