

	PROCEDIMIENTO GESTIÓN DE EVENTOS	Código:	OSTI-PR05
		Versión:	03
		Fecha:	18/03/2020
		Página:	Página 1 de 5

1. OBJETIVO

Gestionar en forma adecuada los eventos que se presenten con los diferentes Activos de Información, con el propósito de mitigar el impacto dentro de la operación de los procesos de la ADRES.

2. ALCANCE

El procedimiento como tal, inicia con la manifestación y notificación de ocurrencia de los diferentes tipos de eventos, los cuales se deben registrar para su trámite, validación, gestión y cierre respectivo de los mismos, según prioridades y el impacto que pueda generar dentro de la ADRES.

3. LÍDER DEL PROCEDIMIENTO

Coordinador Grupo Interno Gestión de Soporte a la Tecnologías de la Dirección de Gestión Tecnología de Información y Comunicaciones.

4. POLÍTICAS DE OPERACIÓN

- El alcance de la Gestión de Eventos se enmarca en el monitoreo y seguimiento de:
 - Todos los elementos de configuración.
 - Las licencias de software.
 - Los principales puntos de seguridad de la información
 - La actividad normal de la operación
- Existen tres tipos básicos de eventos: Informativos, de alerta y de excepción y su importancia se puede definir de la siguiente manera:
 - Informativo: No se requiere acción.
 - Alerta: Se ha alcanzado un umbral.
 - Excepción: La operación es anormal.
- 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.
- El Soporte de Tercer Nivel (El proveedor), reporta los eventos mediante correo electrónico y/o a través de herramientas propias de gestión y monitoreo.
- Los eventos reportados se deben registrar en la herramienta que DGTIC disponga para ello (Plantilla y/o herramienta computarizada)
- La ADRES verifica los Acuerdos de Nivel de Servicio (ANS) establecidos en los contratos correspondientes.
- Los horarios de atención de los proveedores tecnológicos de la entidad están inmersos dentro de los acuerdos contractuales.

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	Notificar los Eventos	<p>Cada vez que las herramientas de monitoreo y gestión, de los proveedores o responsables del Soporte de Tercer Nivel, detectan eventos que deben ser notificados, se generan alertas sobre el funcionamiento de los diferentes activos que forman parte de la infraestructura de TI, notificando por medio de correo electrónico al soporte de primer nivel y/o segundo nivel, advirtiéndolo sobre posibles pérdidas o afectación importante en la capacidad y disponibilidad de los elementos de configuración.</p>	Proveedores, Soporte Tercer Nivel	Correo electrónico de notificación de Evento.
PC 2	Validar información y realizar filtrado y clasificación de eventos	<p>Descripción de la Actividad: Recibida una notificación por correo electrónico, se valida la información clasificando los eventos.</p> <p>Descripción del Punto de Control:</p> <p>Cada vez que se reciba una notificación de eventos, se valida la información para clasificarlos mediante la aplicación de filtros. Soporte de primer y/o segundo nivel, validan si el evento puede generar consecuencias futuras respecto a la operación normal o prevista.</p> <p>La clasificación se realiza en tres categorías:</p> <ul style="list-style-type: none"> ✓ Informativo: Un evento que no requiere ninguna acción y que no es una excepción. En la herramienta de monitoreo, Por ejemplo: en caso de recibir alerta de crecimiento de espacios en disco duro, se valida que ésta obedezca a la ejecución de un proceso de negocio. En caso de no estar ejecutándose un proceso de negocio, se debe escalar su tratamiento. ✓ Alerta: Se produce cuando un dispositivo alcanza un umbral predefinido. Avisa a una persona, proceso o herramienta para que pueda controlar la situación y adoptar las acciones oportunas para prevenir una excepción. ✓ Excepción: Indica un comportamiento anómalo de un 	Gestor de operaciones o responsable del Soporte Primer / Segundo Nivel	Plantilla diligenciada o herramienta computarizada.

No	Actividad	Descripción de la Actividad	Responsable	Registro
		<p>servicio o dispositivo, que no cumple con los Acuerdos de Nivel de Servicio (ANS) establecidos por los proveedores. Se deben tomar las acciones necesarias para evitar que a causa de ello se genere en la operación un incidente o problema.</p> <p>¿El evento genera un incidente?</p> <p>SI: Continúa con la siguiente actividad.</p> <p>NO: El Gestor de operaciones o responsable del Soporte Primer / Segundo Nivel registra el evento en una Plantilla y/o herramienta computarizada. De igual forma, se registrarán los casos que se disparen con alertas críticas. Continuar con la actividad No.4.</p>		
3	Reportar incidente	<p>Una vez clasificado el evento, según la prioridad (definido en el catálogo en el cual se configuran los eventos) y si este necesita un tratamiento urgente por el riesgo a que pueda desencadenar una caída o indisponibilidad del sistema, se debe remitir la información del evento mediante correo electrónico al Gestor de Operaciones designado para realizar la Gestión de Incidente o el caso respectivo en la Mesa de Servicios. Ver procedimiento de Gestión de Requerimientos o Gestión de incidentes.</p> <p>FIN DEL PROCEDIMIENTO</p>	Gestor de operaciones o responsable del Soporte Segundo Nivel	Correo electrónico de mesa de servicios
4	Identificar correlación y Opciones de Respuesta	<p>Cada vez que se identifique que el evento no genera incidente, se identifica la correlación y las posibles opciones de respuesta, acción que se genera analizando si existen eventos similares para detectar si aquellos, que aún no han tenido un impacto directo en la infraestructura, pueden llegar a tenerlo en un futuro así, como la importancia del evento en sí mismo y se decide si es necesario tomar medidas. El resultado del análisis se registra en la plantilla y/o herramienta computarizada.</p> <p>Se determinan las opciones de respuesta de acuerdo con el tipo de evento presentado y se remite el evento a Soporte Segundo Nivel designado para el</p>	Gestor de operaciones o responsable del Soporte Segundo Nivel	Plantilla y/o herramienta computarizada

No	Actividad	Descripción de la Actividad	Responsable	Registro
		tratamiento del evento de Infraestructura o Base de Datos.		
5	Aplicar solución del evento	<p>Una vez recibida una designación de tratamiento del evento de Infraestructura o Base de Datos, el funcionario encargado dará solución al evento presentado y realizará el registro dentro de la Plantilla y/o herramienta computarizada.</p> <p>De acuerdo con el tipo de evento se genera dicha solución, y se mantiene el seguimiento constante a fin de evitar una indisponibilidad. Este seguimiento debe mantenerse hasta que las alertas desaparezcan.</p>	Gestor de operaciones o responsable del Soporte Segundo Nivel, designado para el tratamiento del evento de Infraestructura o Base de Datos	Reporte de solución del evento en plantilla o herramienta computarizada
PC 6	Validar estado del evento y generar cierre	<p>Descripción de la Actividad:</p> <p>Posterior a la aplicación de la solución del evento y de su reporte en la plantilla o herramienta, se realiza el cierre del evento en esta misma herramienta.</p> <p>Descripción del Punto de Control:</p> <p>Cada vez que se ejecute la solución planteada a los eventos, se valida el estado del evento, acción que se genera revisando si la ejecución de dicha solución contiene excepciones o alertas importantes o si hace un recuento de tipos de eventos.</p> <p>¿El evento fue tratado correctamente?</p> <p>SI: Cerrar el evento en la herramienta.</p> <p>NO: El Gestor de operaciones o responsable del Soporte de Primer/Segundo Nivel, identifica las correcciones para la mejora continua y se cierra el evento. A su vez estas acciones de mejora se documentan en la Plantilla y/o herramienta computarizada.</p> <p>FIN DEL PROCEDIMIENTO</p>	Gestor de operaciones o responsable del Soporte de Primer/Segundo Nivel	Plantilla y/o herramienta computarizada con cierre del evento.

8. CONTROL DE CAMBIOS

	PROCEDIMIENTO GESTIÓN DE EVENTOS	Código:	OSTI-PR05
		Versión:	03
		Fecha:	18/03/2020
		Página:	Página 5 de 5

Versión	Fecha	Descripción del cambio	Asesor del proceso
01	29 de junio de 2018	Emisión y Publicación inicial	Johanna Bejarano Heredia Gestor de Operaciones OAPCR
02	31 de diciembre 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.	Diana Esperanza Torres Gestor de Operaciones OAPCR
03	18 de marzo de 2020	Actualización de las políticas de operación teniendo en cuenta el cambio de versión del Modelo de Arquitectura Empresarial definido por el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC.	Olga 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:
Edilberto Zamora Alvarado Gestor de Operaciones - Dirección de Gestión de Tecnologías de Información y Comunicaciones	Carlos Andrés Ruiz Romero Coordinador de la Dirección de Gestión de Tecnologías de Información y Comunicaciones	Sergio Andrés Soler Rosas Director de Gestión de Tecnologías de Información y Comunicaciones