Agencia para la Reincorporación y la Normalización - ARN

AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA DE GESTIÓN DE EVENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN

BOGOTÁ D.C. JUNIO DE 2021

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los pasos necesarios para la identificación y tratamiento de eventos en el Centro de Operaciones de red y de seguridad, en caso de que un servicio y/o sistema de información presente condiciones inusuales de operación.

2. ALCANCE

Aplica para todos los servicios TI de Agencia para la Reincorporación y la Normalización.

3. DEFINICIONES

ACUERDOS DE NIVELES DE SERVICIO: Identifica y define las necesidades del cliente, a la vez que controla sus expectativas de servicio en relación con la capacidad del proveedor.

ANS: Acuerdos de Niveles de Servicio.

ARN: Agencia para la Reincorporación y la Normalización

BASE DE DATOS DE GESTIÓN DE Configuraciones (CMDB): Es una base de datos donde se relacionan todos los hardware, software, documentación, servicios o recursos.

CENTRO DE OPERACIONES DE RED - NOC: Es el centro desde el cual se efectúa el control de la red. Es responsable de monitorizar las redes en función de alarmas o condiciones que requieran atención especial para evitar impacto en el rendimiento de las redes y el servicio

CENTRO DE OPERACIONES DE SEGURIDAD - SOC: encargado de monitorear la seguridad informática del cliente y generar alertas y eventos en caso de que se identifique situaciones que afecten la seguridad del cliente

CI: elemento de configuración

CMDB: Configuration Management Data Base- Base de Datos de Conocimiento.

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 cliente.

DISPONIBILIDAD: Es la capacidad de un servicio, componente o elemento de configuración para llevar a cabo su función cuando sea necesario.

ELEMENTO DE CONFIGURACIÓN (CI): Cualquier componente u otro activo del servicio que necesite ser gestionado con el objeto de proveer un servicio de TI. Los CI pueden ser hardware, software, documentos y recursos.

EVENTO: Alerta o notificación creada por un servicio de TI, elemento de configuración o herramienta de monitorización. Los Eventos requieren normalmente que el personal de operaciones de TI tome acciones, y a menudo conllevan el registro de Incidentes.

EVENTO ALERTA: Se asigna a aquellos eventos que indican que el servicio se aproxima a un umbral. Su objetivo es notificar a las personas, herramientas o procesos apropiados para que revisen la situación y tomen las medidas necesarias para evitar que se produzca una excepción[1].

EVENTO EXCEPCIÓN: Se asigna a los eventos cuando indican que el servicio está operando de manera irregular: los ANS se han incumplido, etc. Las excepciones pueden representar un fallo total, un cese en una funcionalidad o una disminución del rendimiento. Sin embargo, no tienen por qué ser errores.

EVENTO INFORMATIVO: Se asigna a aquellos eventos que no requieren, en principio, ninguna respuesta y que por tanto no representan una excepción.

GT: Grupos Territoriales.

RFC: Es una solicitud formal para la implementación de un Cambio.

SIEM: Es una herramienta de gestión de incidentes y eventos de seguridad, la cual tiene diferentes componentes como colectores, motor Correlacionador, aplicación de eventos e incidentes y bases de datos.

SOLARWINDS: Herramienta utilizada para monitorear el desempeño de la Infraestructura TI y los servidores enfocados a Datacenter.

SOLICITUD DE CAMBIOS (RFC): Es una solicitud formal para la implementación de un Cambio.

TI: Tecnologías de la Información

[1] http://itilv3.osiatis.es/

4. CONTENIDO Y DESARROLLO

- Toda gestión de eventos realizada por el Centro de Operaciones (NOC – SOC) debe enmarcarse en el actual documento.

- La gestión de eventos debe ejecutarse de con una disponibilidad de 7x24x365, durante la operación de la infraestructura, plataforma y/o servicios de TI.

- 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.

- Los Gestores de eventos son responsables por la correcta ejecución de la guía operacional de Gestión de eventos y es el único empoderado para realizar modificaciones al mismo.

- Algunos eventos presentan situaciones que requieren que sean tratados a través de otras gestiones como incidentes, cambios y/o problemas, debido a su severidad, complejidad y/o impacto. El tratamiento o respuesta debe darse en términos de estas gestiones

- Los Gestores de Eventos realizan las actividades para madurar dicha gestión realizando las siguientes actividades:

    - ✓ Informe mensual
    - ✓ Aplicación de acciones de mejora
    - ✓ Medición de ANS
    - ✓ Seguimiento a umbrales existentes
    - ✓ Seguimiento a Backlog
    - ✓ Levantamiento de información para servicios nuevos.

5. DESCRIPCIÓN DE ACTIVIDADES

No.	Actividad	Descripción
1	**Listar y mapear los servicios a Monitorear**	Los líderes de cada servicio y el Gestor de Eventos, describirán los servicios que serán monitoreados, y sus respectivos anexos. Con el fin de conocer el alcance de estos.
2	**Validar tipo de servicio y Definir CI a Monitorear**	Los líderes de cada servicio y Gestor de Eventos deben validar el tipo de servicio, si corresponde a un servicio existente o un servicio nuevo. • Si el servicio es nuevo continua actividad 3. • El servicio ya existe continua actividad 9. De igual manera, definen los elementos de configuración que serán monitoreados.
3.	**Registrar en la herramienta de gestión el C.I. a monitorear**	Los líderes de cada Servicio definen los umbrales a parametrizar, la frecuencia del monitoreo y la configuración de cómo será la correlación de los CI con solicitud de caso en la herramienta Aranda asignado al Gestor de Eventos.
4.	**Solicitud formal para subir CI con umbrales a gestión**	Los líderes de cada Servicio con apoyo del Gestor de Eventos deben gestionar la solicitud de cambio formal a través de un RFC registrado como cambio en la herramienta de gestión para realizar la configuración de todas las definiciones en las herramientas de monitoreo.
5.	**Modelar Servicio en las Herramientas de Monitoreo**	El Administrador de los sistemas de Monitoreo realiza el modelamiento del servicio en las herramientas de monitoreo de acuerdo con los requerimientos entregados por la ARN.
6.	**Revisar y aprobar el correcto funcionamiento de los eventos**	El proceso incluye como actores al líder del nuevo servicio, líder NOC y SOC y al Gestor de eventos para la inclusión de un servicio nuevo, se debe enviar un correo al gestor de eventos indicando nombre del nodo., dirección IP., tipo de servicio al cual pertenece, umbrales de alerta (medios y críticos), destinatarios del mensaje al momento de presentarse un evento o incidente. Desde Gestión de Eventos se revisará la información y de existir inconsistencias se devolverá al servicio para las correcciones, el mismo será enviado corregido de nuevo al gestor quien dará el visto bueno.
7.	**¿Requiere Afinamiento?**	Los líderes de cada servicio y el Gestor de Eventos determinan si la configuración de los eventos requiere afinamiento: • Si requiere afinamiento, pasa a la actividad 5. Modelar Servicio en la Herramienta de Monitoreo. • No requiere afinamiento, pasa a la actividad 8. Verificar la Implementación de Monitoreo.
8.	**Verificar la Implementación de Monitoreo**	El Gestor de Eventos y la Supervisión o a quien se designe, verifica la implementación del monitoreo.
9.	**¿Monitoreo Adecuado?**	Se determina si el monitoreo es adecuado: • Si el monitoreo es adecuado, continúa en la actividad 10. Reporte satisfactorio. • No es adecuado el monitoreo, continúa en la actividad 1. Listar y mapear Servicios a Monitorear.

No.	Actividad	Descripción
10.	**Reporte satisfactorio**	El Gestor de Eventos determina si el monitoreo es adecuado y pasa a la actividad 11.
11.	**Recolectar eventos**	El Centro de operaciones y el líder de servicio empezará a recibir las notificaciones de eventos detectadas por las herramientas de monitoreo, estas notificaciones irán con copia al líder del servicio al mismo tiempo que se debe realizar gestión telefónica.
12.	**Identificar, Clasificar y Correlacionar Eventos**	El Centro de operaciones y el líder de servicio identifican el evento, la herramienta clasifica los eventos para definir qué tipo de afectación es, luego se correlacionan los eventos que notifiquen la misma causa para ser solucionado por parte de los responsables del servicio.
13.	**¿Tipo de Evento?**	El Centro de operaciones determina el tipo de evento: • Si es evento tipo Informativo (Normal, Mayor y Menor), pasa a la actividad 14. • Si se trata de una alarma, pasa a actividad 15. Se es un evento critico continua a actividad 17.
14.	**Registrar y cerrar automáticamente eventos informativo o alarma**	Se procede a registrar, realizar gestión telefónica con los líderes del servicio afectado y cerrar de forma automática el evento reportado puede ser informativo si viene de la actividad 13 o alarma si viene de la actividad 15. Fin del proceso
15.	**¿Intervenir?**	El Centro de operaciones determina si la alerta requiere intervención humana: • Si es evento tipo alarma y requiere intervención pasa a actividad 16 Si no requiere intervención pasa a la actividad 14.
16.	**Gestionar manualmente eventos tipo alarma**	La intervención del Centro de operaciones debe establecer comunicación con el personal que la ARN indique para validar fallas que comprometan el estado del servicio.
17.	**Registrar y ejecutar tratamiento a eventos críticos**	De acuerdo con lo detectado en el punto 16, el centro de operaciones realiza la intervención humana, con el fin de identificar e implementar las acciones necesarias para la información y/o notificación del evento.
18	**Cierre de eventos**	Una vez notificado el evento a los responsables se procede a hacer la gestión a la bitácora correspondiente.

5.1 ENTRADAS

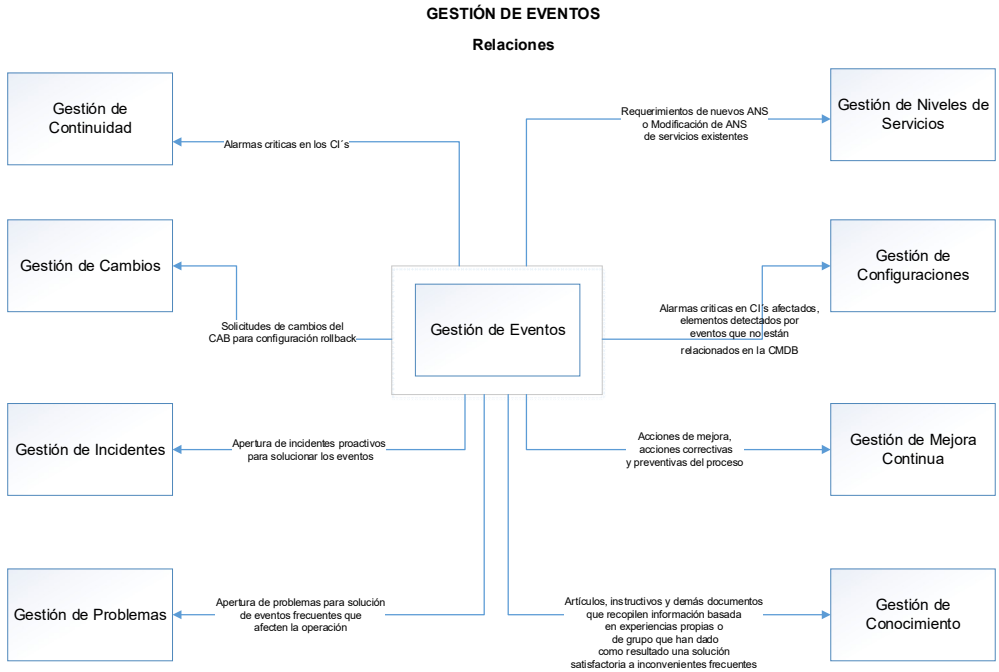
Proveedor	Entrada
Gestión de Capacidad	Necesidad de Configuración de Eventos para Monitorear la Capacidad.
Gestión de la Disponibilidad	Necesidad de Configuración de Eventos para Monitorear la Disponibilidad.
Gestión de Cambios	Implementación de Cambios que Generan Notificaciones de Eventos.
Gestión de Acuerdos de Niveles de Servicios	ANS de Referencia para Configurar Umbrales.

Proveedor	Entrada
Gestión de Configuración	CMDB Actualizada
Gestión de Mejora Continua	Planes de Mejora sobre el proceso

5.2 SALIDAS

Salida	Cliente
Apertura de Incidentes para solucionar Eventos.	Gestión de Incidentes proactivos
Apertura de Problemas para solucionar Eventos.	Gestión de Problemas
Solicitudes de Cambios para solucionar Eventos.	Gestión de Cambios
Acciones de Mejora y Correctivas del proceso	Gestión de Mejora Continua
Solicitudes de Cambios para Configurar los Eventos en la Herramienta de Monitoreo.	Administrador de Herramientas de Monitoreo

6. RELACIONES



7. INFORMES PERIÓDICOS (ENTREGABLES)

Nombre	Descripción	Periodicidad	Cliente
Informe de Gestión	Informe con los detalles de la gestión del proceso para el periodo	Mensual	ARN

8. RESPONSABILIDADES

Rol	Responsabilidades
Gestor de Eventos	• Apoyar a los Líderes de Servicios para enlistar los servicios a monitorear. • Verificar los acuerdos de niveles de servicios para tomarlos como referencia para la determinación de los umbrales. • Apoyar a los Líderes de Servicios en la definición de los elementos a monitorear, el establecimiento de umbrales, la frecuencia del monitoreo, las líneas base de los servicios y la correlación de eventos. • Apoyar a los Líderes de Servicios en la definición de las notificaciones y acciones para los eventos. • Verificar la implementación del monitoreo de todos los servicios T.I. • Apoyo en la Detección, Identificación y Resolución de Eventos.
Líder de Servicio	• Listar los servicios a monitorear. • Verificar los acuerdos de niveles de servicios para tomarlos como referencia para la determinación de los umbrales. • Definir los elementos a monitorear, el establecimiento de umbrales, la frecuencia del monitoreo, las líneas base de los servicios y la correlación de eventos. • Definir las notificaciones y acciones para los eventos. • Realizar las solicitudes de cambios para configurar y pasar a producción la configuración de los eventos en la herramienta de monitoreo. • Implementar y validar las acciones de mejora necesarias para la resolución de los eventos.
Centro de Operaciones	• Detectar, Identificar, Clasificar, Correlacionar y comunicar los eventos.

Rol	Responsabilidades
	• Informar y / o notificar a líderes de servicios o a proveedores de acuerdo con la matriz de escalamiento. • Sugerir acciones de mejora necesarias para la resolución de los eventos. • Monitoreo de las consolas de Administración y gestión de la infraestructura del servicio. • Reporte de Eventos de Seguridad Generados por el servicio. • Reporte de Incidentes de Seguridad generados por el servicio.
Administrador de Herramientas de Monitoreo	• Configurar en las herramientas de monitoreo las definiciones de los servicios.

9. MATRIZ RACI

La definición de la matriz de responsabilidades se constituye como una herramienta práctica y útil cuando se establecen las obligaciones que tiene cada uno de los actores del proceso.

Cuando se diseña un proceso o un servicio es imperativa la definición clara de los roles que hacen parte de estos y las responsabilidades que cada uno tiene en su ciclo de vida, por esto se hace necesaria la conformación de una matriz RACI que represente la asignación de estas responsabilidades. RACI es el acrónimo empleado para las cuatro funciones principales de:

- **Responsible (Ejecutor):** La persona o personas responsables por la ejecución de la actividad.
- **Accountable (Dueño):** Este es el rol encargado de aprobar el trabajo realizado y a partir de este momento es quien responde a las directivas o instancias superiores por el trabajo.
- **Consulted (Consultado):** Son las personas que son consultadas y en quienes se busca una opinión.
- **Informed (Informado):** Son los grupos de personas a quienes se informa sobre el progreso y resultados del trabajo.

En la siguiente matriz se asignan las responsabilidades de cada rol dentro del proceso Gestión de Eventos:

ROL / Actividad	Gestor de Eventos	Líder de Servicio	Centro de Operaciones	Administrador de Herramientas de Monitoreo
Seleccionar Servicios a Monitorear	CI	A		R
Verificar ANS de los Servicios	CI	R - A		C
Definir Elementos, Umbrales, Frecuencia, Línea Base y Correlación	CI	R - A		R - C
Definir Notificaciones y Acciones para los eventos	CI	R - A	I	R - C
Realizar Solicitud de Cambio (RFC)	CI	R - A		R - I
Modelar Servicio en la Herramienta de Monitoreo	R	A	C	C - I
Verificar la Adecuada Implementación del Monitoreo	R	R - A		C
Identificar, Clasificar y Correlacionar Eventos	CI	R - A	R	C
Registrar y Cerrar Evento	CI	RA	I	C