CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **"Confidencial e Interno".**
El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.
No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. OBJETIVO

Establecer un compendio de eventos críticos, asegurando una vigilancia continua y la adecuada clasificación de estos, proporcionando orientaciones claras al equipo encargado del Monitoreo.

2. ALCANCE

La Gestión de eventos es aplicable a todos los elementos de configuración acordados a cada unidad de negocio en Keralty.

3. DEFINICIONES

- **Responsable del Servicio:** Individuo que ostenta la responsabilidad final ante el cliente y la organización de TI por la entrega de un servicio determinado.
- **Evento:** Cualquier acontecimiento que puede ser identificado y que es relevante para la infraestructura de TI, para la prestación o la evaluación de un servicio. Por ejemplo, las alertas generadas por servicios, configuraciones o herramientas de monitoreo.
- **Alerta:** Señal que se emite cuando se supera un umbral preestablecido, indicando una posible anomalía.
- **Herramientas de Monitoreo Activo:** Herramientas que examinan individualmente los componentes de infraestructura para comprobar su estado y funcionamiento. Si se detectan anomalías, se genera y envía una alerta al equipo responsable.
- **Componente:** Elemento que forma parte de una estructura más amplia, en este caso, de la infraestructura de TI.
- **Incidente:** Cualquier interrupción no prevista en un servicio de TI o una disminución en su calidad, así como cualquier fallo en un elemento de configuración que aún no ha afectado el servicio.
- **Prioridad:** Determinación basada en la urgencia e impacto de un incidente o problema, utilizada para asignar recursos y definir tiempos de respuesta.
- **Problema:** La causa raíz de uno o más incidentes, cuya identificación y resolución se persiguen a través del Proceso de Gestión de Problemas.

- **Proceso:** Secuencia estructurada de actividades orientadas a lograr un objetivo específico, con entradas y salidas definidas.
- **Requerimiento:** Solicitud de un usuario para obtener información, asesoramiento o acceso a un servicio de TI.
- **RFC (Request for Change):** Documento que registra la información de un cambio propuesto a lo largo de sus fases.
- **Procedimiento:** Conjunto de pasos definidos que orientan la ejecución de una tarea.
- **Tipos de Eventos:** Clasificación de eventos en categorías como advertencias, excepciones e informativos, según la naturaleza y la respuesta requerida.
- **Modo Mantenimiento:** Suspensión temporal de la detección de eventos en una o varias herramientas de monitoreo para ciertos componentes.
- **Escalamiento:** Proceso de elevación de un problema, incidente o requerimiento a un nivel superior de atención o gestión, basado en la discrepancia entre los resultados esperados y los obtenidos.
- **AppDynamics:** Plataforma de gestión del rendimiento de aplicaciones que proporciona visibilidad en tiempo real sobre el rendimiento de las aplicaciones, permitiendo a las organizaciones optimizar la experiencia del usuario y mejorar la eficiencia operativa.
- **ThousandEyes:** Herramienta de monitoreo de red que ofrece visibilidad end-to-end sobre la entrega de servicios digitales, ayudando a identificar y resolver rápidamente problemas de rendimiento en redes y aplicaciones a nivel global.

4. POLITICAS Y NORMA APLICABLE

1. Todos los empleados que participan en la Gestión de Eventos de Servicios de TI deben adherirse a las directrices establecidas en este documento.
2. Al identificar un evento, es fundamental comprender su naturaleza, determinar las medidas correctivas pertinentes y llevar a cabo un análisis detallado para clasificarlo adecuadamente (como incidente, problema o cambio).
3. El encargado de la gestión de configuraciones debe asegurar que la Base de Datos de Gestión de Configuración (CMDB) esté al día, facilitando así su consulta por parte del Command Center.

4. Es imprescindible seleccionar y configurar de manera adecuada la herramienta que se empleará para la gestión de eventos.
5. La operación para el manejo y documentación de eventos estará disponible continuamente, las 24 horas del día, los 7 días de la semana.

5. PROCESO Y PROCEDIMIENTO RELACIONADOS

- **Gestión de Cambios:** La Gestión de Eventos contribuye al proceso de Mejora Continua del Servicio, generando propuestas de cambio basadas en la correlación y análisis de eventos, lo cual permite optimizar los servicios y prevenir futuros incidentes.
- **Gestión de Configuración:** Este proceso se beneficia directamente de la Gestión de Eventos al utilizar la información detallada de la configuración y los activos para identificar y resolver eventos de manera más eficaz, garantizando la integridad y la disponibilidad de los servicios.
- **Gestión de Problemas:** La identificación de patrones y tendencias en los eventos facilita la postulación, análisis e investigación de las causas raíz de los problemas, mejorando así la estabilidad de los servicios al prevenir la recurrencia de incidentes.
- **Gestión de Incidentes y Solicitudes:** Los eventos que resultan en interrupciones no planificadas o fallos en los componentes de infraestructura (CIs) requieren una coordinación estrecha con la Gestión de Incidentes y Solicitudes para restaurar el servicio de manera rápida y eficiente, minimizando el impacto en los usuarios y en el negocio.

6. RESPONSABILIDADES

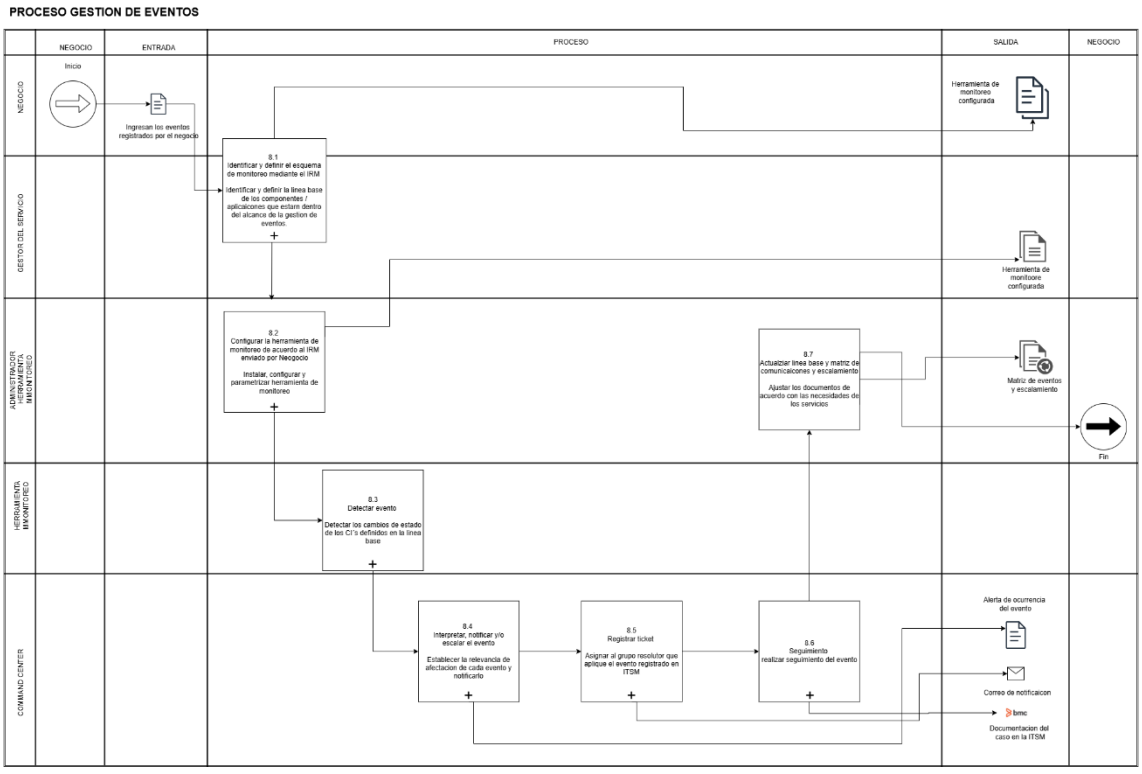
- **Responsable del proceso:**
  - **Líder de Monitoreo y control de TI:** Encargado de asegurar que el procedimiento de Gestión de Eventos se cumpla, se mantenga actualizado y se mejore continuamente.

- **Responsables de las actividades del proceso:**
    - **Líder de Monitoreo y control de TI:**
        - Divulgar el proceso de Gestión de Eventos.
        - Asegurar la operatividad de las herramientas de monitoreo.
        - Verificar el monitoreo de todos los dispositivos relevantes.
        - Analizar eventos significativos y tomar acciones correspondientes.
- **Administrador de herramientas de monitoreo:**
    - Parametrizar la herramienta de monitoreo según el esquema establecido.
    - Colaborar en el análisis de eventos importantes.
    - Ajustar parámetros de monitoreo basados en análisis de eventos.
- **Operador Command Center:**
    - Monitorear componentes según lo definido en la Gestión de Eventos.
    - Registrar eventos significativos.
    - Comunicar la ocurrencia de eventos a los interesados.
    - Escalar incidentes al especialista correspondiente.
- **Gerente de Negocio/dueño de la aplicación:**
    - Informar sobre los componentes de configuración de los servicios incluidos en la gestión de eventos.
- **Especialista:**
    - Analizar e investigar eventos, y restaurar servicios.
    - Documentar acciones de restablecimiento.
    - Supervisar el impacto de las medidas correctivas.
- **Analista de Mesa de Servicios (cuando aplique):**
    - Notificar al Command Center sobre incidentes que necesiten atención.
    - Mantener comunicación con operadores para seguimiento de incidentes.

7. EQUIPOS Y HERRAMIENTAS

- Herramienta de Gestión de Servicios
- Herramienta de Gestión de configuración
- Herramientas de monitoreo

8. FLUJO DE PROCEDIMIENTO



9. DETALLE DEL PROCEDIMIENTO

- Identificar y definir el esquema de monitoreo

Responsable	**:**	Gestor de servicio, Cliente
Objetivo	**:**	Identificar y definir la línea base que componen los servicios que estarán bajo el alcance de la gestión de eventos.
Acciones	**:**	• El negocio define e identifica los elementos de configuración que deben cubrirse con el proceso de Gestión de Eventos. En caso de existir una previa documentación en el contrato u oferta técnico-económica se tomará como base esta información. • Determinan los atributos, respectivos umbrales y los tipos de eventos que se incluirán en el esquema de monitoreo, • Para cada tipo de evento se deben definir las acciones a tomar y el sistema de notificaciones • La línea base y Matriz de comunicaciones se deberá socializar con todos los interesados.
Entregable	**:**	Línea base, Matriz de comunicaciones y escalamiento
Plazo	**:**	Nuevos negocios y/o países que incluyan servicio Command center
Trazabilidad	**:**	Pendiente

Tabla 1 Identificación y definición del esquema de monitoreo

- Configurar herramienta de monitoreo

Responsable	:	Administrador herramienta de monitoreo
Objetivo	:	Instalar, configurar y parametrizar herramienta de monitoreo.
Acciones /Entregables	:	• -De acuerdo con lo definido en la línea base y matriz de comunicaciones se debe instalar y configurar los parámetros a los elementos definidos. • -Se deberán definir los informes requeridos para realizar el seguimiento de los CI´s en cuanto a disponibilidad, continuidad, capacidad y seguridad. • De acuerdo a la definición al IRM (Ingreso, Retiro o Modificación) se debe notificar al administrador de la herramienta de monitoreo, de acuerdo al documento. • La línea base y Matriz de comunicaciones se deberá socializar con todos los interesados.
Plazo	:	La línea base y Matriz de comunicaciones se deberá socializar con todos los interesados.
Trazabilidad	:	Notificaciones parametrizadas

Tabla 2 Configuración herramienta de monitoreo

- Detectar evento

Responsable	:	Herramienta monitoreo
Objetivo	:	Detectar los cambios de estado en los CI's definidos en la línea base
Acciones	:	Con base en las configuraciones realizadas, la herramienta de monitoreo detectará los cambios de estado presentados por los diferentes CI
Entregable	:	Alerta de ocurrencia del evento.
Plazo	:	Según parametrización de herramienta
Trazabilidad	:	Registros en la herramienta de monitoreo

Tabla 3 Detección de eventos

- Interpretar, notificar y/o escalar el evento

Responsable	:	Operador Command center
Objetivo	:	Establecer la relevancia, afectación del evento y notificarlo
Acciones	::	• Generadas por la herramienta por la herramienta de monitoreo son analizadas • En la matriz de escalamiento se debe enviar correo y notificar a/las áreas encargadas • Se notificará de acuerdo a la matriz de escalamiento
Entregable	:	Correo notificación
Plazo	:	ANS acordado con el negocio
Trazabilidad	:	Información registrada en la ITSM

Tabla 4 Interpretación, notificación y escalamiento de eventos

- Registrar ticket

Responsable	**:**	Operador Command center / Herramienta de monitoreo
Objetivo	**:**	Asignar al grupo resolutor que aplique el evento registrado en ITSM BMC.
Acciones	**:**	• Crear un caso en la ITSM • Asigna mediante la ITSM el caso registrado de acuerdo con la matriz de comunicaciones. • En caso de incidentes la gestión continúa en gestión de incidentes
Entregable	**:**	Documentación del caso en la ITSM.
Plazo	**:**	ANS acordado con el negocio
Trazabilidad	**:**	Información registrada en el caso de la ITSM – Herramienta de Monitoreo

Tabla 5 Registro de tickets

- Seguimiento

Responsable	:	Operador Command center
Objetivo	:	Realizar seguimiento del evento
Acciones	:	• Verificar en la herramienta de monitoreo que el evento no persista.
Entregable	:	Alerta de ocurrencia del evento
Plazo	:	Ans acordado con el cliente
Trazabilidad	:	Registros en la herramienta de monitoreo

Tabla 5 Seguimiento

- Actualizar línea base y matriz de comunicaciones y escalamiento

Responsable	:	Administrador de la herramienta y/o Jefe Command Center
Objetivo	:	Ajustar los documentos de acuerdo a las necesidades de cada Negocio
Acciones	:	1. Enviar a cada gerente del negocio la matriz de escalamiento y comunicaciones 2. En caso de requerir actualización se notificará a ambas partes de los cambios 3. Actualizar en caso de que aplique
Entregable	:	Alerta de ocurrencia del evento
Plazo	:	Ans acordado con el cliente
Trazabilidad	:	Registros en la herramienta de monitoreo

Tabla 6 Actualización línea base y matriz de comunicación y escalamiento

10. MATRIZ RACI

R- Responsable (ejecutor): la persona o personas responsables de ejecutar esta Actividad

A - 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.

C - Consulted (Consultado): Son las personas que son consultadas y en quienes se busca una opinión.

I - Informed (Informado): Son los grupos de personas a quienes se informa sobre el progreso y resultados del trabajo.

	Gestor del servicio	Jefe Command Center	Administrador herramienta de monitoreo	Negocio	Operador Command center	Especialista
8.1 Identificar y definir el esquema de monitoreo	R	A	I	R	-	C
8.2 Configurar herramienta de monitoreo	I	A/C	R	I	I	I
8.3 Detectar evento	I	A	C	I	R	C
8.4 Interpretar, notificar y/o escalar el evento	I	A	-	I	R	C
8.5 Registrar ticket	I	A	-	I	R	C
8.6 Seguimiento	C	A	-	I	R	C
8.7 Actualizar línea base y matriz de comunicaciones y escalamiento	C	R/A	R	I	C	-

Tabla 7 Matriz Raci

11. ANEXO A. Documento IRM

- https://docs.google.com/spreadsheets/d/116R7NAa495QVjRvUD-hiipcnHCCF9aL9/edit?usp=sharing&ouid=112580271660809162306&rtpof=true&sd=true

12. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
27/09/2022	Creación documento	1.0
24/08/2023	Revisión	2.0
03/05/2024	Se reestructuró el documento, se realiza inclusión de la sigla del país y la compañía en el código del documento.	3.0
09/01/2025	Adición formato IRM (ingreso-retiro-modificación)	4.0

Tabla 8 control de cambios

13. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Felipe Andrés Melo Área/Proceso: Operaciones TI Fecha:03/05/2022	Nombre: Luisa Gineth Castaño Perea Área/Proceso: Director de operación y comunicaciones TI Fecha: 09/01/2025	Nombre: Luisa Gineth Castaño Perea Área/Proceso: Director de operación y comunicaciones TI Fecha: 14/01/2025

Tabla 9 Flujo de aprobación

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.