CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **"uso 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 registrado en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. OBJETIVO

Definir de forma precisa las actividades y los procesos que se encuentran a cargo de Centro de Cómputo sobre la gestión de Monitoreo. La cual representa una actividad de apoyo, análisis y recolección de información para los diferentes interesados como son los administradores de sistemas, el nivel gerencial, áreas de soporte y desarrollo entre otros. De acuerdo con este objetivo se plantean los objetivos específicos que se listan a continuación:

- Llevar a cabo la configuración, mantenimiento y gestión de los diferentes sistemas de monitoreo del Centro de Cómputo.
- Dar el respectivo manejo a eventos e incidentes presentados sobre la plataforma, divulgando la información a los interesados de forma oportuna, generando los informes respectivos y registrándose para llevar el histórico.
- Identificar las causas raíz de incidentes y de los problemas presentados sobre la infraestructura con base en las evidencias obtenidas desde las herramientas de monitoreo, así mismo, apoyar los análisis que permitan identificar dichas causas.
- Servir como puente entre las áreas de Centro de Cómputo, soporte y desarrollo suministrando información relevante a desarrollo con el fin de mejorar continuamente las aplicaciones.
- Generar los informes que soliciten las diferentes áreas con relación a los diferentes procesos y aspectos de la infraestructura.
- Realizar la gestión de la capacidad en infraestructura para cumplir con las necesidades y demandas presentes y futuras del negocio.
- Proveer datos de componentes o tendencias de servicios que puedan ser utilizadas para optimizar el desempeño de los servicios de TICs.
- Brindar acceso en modo vista a la herramienta de monitoreo que soporten las aplicaciones, previa solicitud por correo y/o mesa de servicio.

2. ALCANCE

Este documento tiene como objetivo determinar unas directrices para la definición, implementación y operación del proceso de monitoreo a nivel de componentes de tecnología con algunas sugerencias para poder tener visibilidad no solo de la plataforma tecnológica, sino de la experiencia de usuario final.

3. DEFINICIONES

Acuerdo de Niveles de Servicio (Service Level Agreement - SLA): Acuerdo escrito entre el proveedor de servicios y el cliente sobre los niveles de servicio acordados entre ambas partes.

Administración de Niveles de Servicio (Service Level Management - SLM): El proceso de definir, acordar, documentar y manejar los niveles de servicio del cliente de TI, que son requeridos y justificados en costo.

Ambiente: Colección de hardware, software, redes de comunicación y procedimientos que trabajan de forma conjunta para proveer un cierto tipo de servicios computacionales. Puede haber uno o más tipos de ambientes en plataformas físicas, por ejemplo, pruebas, producción o desarrollo.

Análisis de Impacto: La identificación de los procesos críticos de negocio, daño potencial y pérdida que pueden causarle al negocio, resultantes de una interrupción en las operaciones de los procesos.

Análisis de Riesgo: Identificar y evaluar el nivel de riesgo, tomando en cuenta los activos expuestos o amenazados.

Aplicaciones: Sistemas de Información que estén bajo el gobierno de soporte y mantenimiento de la Dirección de Informática.

Base de Datos: Información organizada en archivos estructurados pertenecientes a los Sistemas de Información académica, administrativa y financiera de la institución.

Calidad del Servicio: Nivel de servicio contratado o acordado entre el proveedor de servicios y el cliente.

Cambio: Modificación adicional aprobada sobre la línea base de: hardware, red, software, aplicación, ambiente, sistema, o documentación asociada.

Cierre: Cuando un cliente está satisfecho por la resolución del incidente que levantó.

Disponibilidad: Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo. Usualmente es expresado por una relación de disponibilidad, por ejemplo: La proporción de tiempo que el servicio está disponible para uso del servicio por el usuario, dentro del horario de servicio acordado.

Incidente: Cualquier evento que no forma parte usual o normal de la operación diaria del proceso de negocio, que causa o puede causar una interrupción o reducción en la calidad del servicio.

Infraestructura de TI: La suma de los activos de la organización de TI como; hardware, software, unidades de telecomunicación de datos, procedimientos y documentación.

Mesa de Servicios: Métrica: Punto único de contacto dentro de la organización de TI, para los usuarios.

Almacenamiento: Todos aquellos dispositivos, internos o externos, utilizados para almacenar datos e información.

Métrica: Elemento medible de un proceso o una función.

Nivel de Servicio: Expresión de un aspecto del servicio, en términos cuantificables y definitivos.

Operaciones: Todas las actividades y medidas para habilitar y/o mantener el uso de la infraestructura de TI.

P**rioridad:** Secuencia con la que un problema o incidente tiene que ser resuelto, basado en impacto y urgencia.

Problema: Causa principal desconocida de uno o varios incidentes.

Proceso: Serie de acciones, actividades, cambios, etc. conectadas. Realizadas por agentes que tienen el propósito de satisfacer o lograr un objetivo.

Proceso de Negocios: Grupo de actividades de negocio comprometidas por una organización, persiguiendo un fin u objetivo común Los típicos procesos de negocios incluyen recepción de órdenes, servicios de mercadotecnia., venta de productos, servicios de entrega, distribución de productos, facturación por servicios, contabilización por dinero recibido. Un proceso de negocio normalmente depende del soporte de varias funciones de negocio, por ejemplo: personal de Tecnología de Información, alojamiento, estos muy rara vez operan aislados, siempre hay interdependencia entre ellos.

Proveedor: Organización encargada de proveer los servicios de TI.

Recursos: Ayudan a proveer los requerimientos de los clientes de TI. Los recursos son usualmente computadoras y equipo relacionado, software, facilidades (edificio, sites, etc.) y gente.

Requerimiento de Servicios: Cada servicio que no sea una falla, provisto por la infraestructura de TI.

Servicio de TI: Conjunto de facilidades de TI y de no TI, proveídos por el servidor de dichos servicios, que satisface con una o varias necesidades de los clientes y que el cliente lo percibe como un todo.

Sistema: Compuesto integral que consiste de uno o más procesos, hardware, software, facilidades y gente, que tiene la capacidad de satisfacer una necesidad u objetivo.

Solución o Soporte Remoto: Incidente o problema solucionado sin la necesidad de presencia física de un elemento del staff de soporte.

Tiempo de indisponibilidad: Periodo de tiempo que un servicio o dispositivo está fuera de servicio, dentro de los tiempos de servicio acordados.

Usuario: Persona que utiliza los servicios diarios.

4. CONTENIDO

LINEAMIENTOS

- El administrador de monitoreo no administra otros sistemas, como los sistemas operativos, plataformas virtuales, consolas de administración de máquinas físicas, redes y bases de datos, se limita a la administración de la herramienta de consulta y gestión.

- El administrador de monitoreo no realiza despliegues, ni pruebas de carga sobre las aplicaciones, sin embargo, apoya en la toma de datos para verificar el impacto de los cambios y medir los límites de carga de las aplicaciones.

- El administrador de monitoreo no realiza cambios sobre ninguna plataforma, sin embargo, apoya en la propuesta de acciones de mejora con el fin de entregar mejor rendimiento y estabilidad a las aplicaciones del negocio, esto no se limita a algunas plataformas, ya que este es un rol transversal que debe apoyar las diferentes capas de infraestructura.

- Cualquier solicitud dentro de las funciones del Administrador de Monitoreo proveniente de la Dirección de Centro de Cómputo, Gerencia de Infraestructura y/o Vicepresidencia de Tecnología.

- Se establecerá un programa de formación continua para los operadores de

monitoreo, enfocado en las últimas tecnologías y prácticas de monitoreo. Además, se realizarán simulacros de incidentes regularmente para asegurar que el equipo esté bien preparado para manejar situaciones adversas eficientemente.

ESQUEMA DEL SERVICIO DE MONITOREO

Para un adecuado esquema de monitoreo se recomienda lo siguiente:

- El proceso de monitoreo debe ser responsabilidad de una única área y tener un responsable asignado.

- Los responsables de plataforma y/o de los servicios deben especificar los eventos, procesos o servicios a monitorizar y el tratamiento que debe darse dependiendo la falla o alerta presentada.

- La estructuración del servicio de monitoreo debe contemplar las herramientas necesarias para esta actividad, de acuerdo al alcance que se defina así:

    - Monitoreo de Hardware
    - Monitoreo de Sistemas Operativos
    - Monitoreo de Bases de Datos
    - Monitoreo de red
    - Monitoreo de ambientes virtuales
    - Monitoreo de servidores de aplicación
    - Monitoreo de aplicación
    - Monitoreo de experiencia de usuario final.

- Cada evento debe contener las acciones automáticas de alertamiento al responsable o instrucciones a la Mesa de Ayuda o al operador para la atención de primer nivel.

- Para eventos atendidos por Mesa de Ayuda u Operadores que requieran escalamiento a terceros, se debe proveer los datos para su comunicación, ANS acordados y las matrices de escalamiento respectivas.

- Esta información debe ser insumo para el cálculo de los indicadores de disponibilidad y análisis de capacidad.

- Se debe generar estadísticas a partir de esta información para ser evaluadas por los responsables respectivos y a partir de esto definir planes de mejoramiento.

- La ocurrencia repetitiva de eventos solucionados debe ser registrada por el gestor de incidentes y problemas para el análisis respectivo.

- Se deben generar reuniones periódicas entre el responsable de este proceso y los responsables de la plataforma o servicio para analizar el comportamiento integral de lo monitorizado y definir estrategias al respecto.

- Se debe evaluar constantemente el comportamiento presentado para identificar eventos no detectados y efectuar un ajuste constante a las herramientas de monitoreo.

- La modificación en la configuración del monitoreo (Umbrales, alarmas, herramientas o procesos de aplicación) debe ser evaluada por Arquitectura y/o el administrador de Monitoreo.

- Las herramientas de monitoreo utilizadas no deben ser intrusivas, es decir, no deben afectar el rendimiento o la operación de la plataforma o servicio monitorizado.

El monitoreo de la disponibilidad del servicio de TI corresponde a una de las actividades principales de la de la Disponibilidad, debido a que desde el momento de la interrupción del servicio de TI hasta su recuperación y puesto en funcionamiento el incidente pasa por distintas fases que deben ser analizadas individualmente.

Fases:

- Tiempo de detección: Tiempo que transcurre desde que ocurre el fallo hasta que la organización TI tiene constancia del mismo.

- Tiempo de respuesta: Tiempo que transcurre desde la detección del problema hasta que se realiza un registro y diagnóstico del incidente.

- Tiempo de reparación/recuperación: Periodo de tiempo utilizado para reparar el fallo o encontrar una solución temporal al mismo y devolver el sistema al estado anterior a la interrupción del servicio.

Para asegurar que se cumplan los niveles de disponibilidad establecidos en los SLA es importante realizar un monitoreo adecuado a los servidores, ya que estos soportan los servicios que brinda la empresa.

- Se debe revisar y actualizar periódicamente los procedimientos de respuesta a incidentes para garantizar una gestión eficiente y rápida de los mismos. Esto incluirá la implementación de más niveles de automatización en la detección,

registro y respuesta a eventos, asegurando así una reducción significativa en el tiempo de inactividad y mejora en la continuidad del negocio.

SEGURIDAD Y PRIVACIDAD EN MONITOREO

Evaluación de Riesgos en Monitoreo

- Implementar revisiones semestrales de riesgos utilizando herramientas como análisis de vulnerabilidades y pruebas de penetración enfocadas en los sistemas de monitoreo.

Protección de Datos Generados por Monitoreo:

- Aplicar cifrado en reposo y en tránsito para los datos sensibles recogidos por las herramientas de monitoreo.

- Establecer controles de acceso basados en roles para limitar el acceso a los datos de monitoreo solo al personal autorizado y capacitado.

Gestión de Acceso a Herramientas de Monitoreo:

- Realizar auditorías regulares de los registros de acceso para detectar y responder a accesos no autorizados o anomalías.

Educación y Concienciación sobre Seguridad en Monitoreo:

- Organizar sesiones trimestrales de capacitación en seguridad para el personal de monitoreo, cubriendo temas como mejores prácticas de seguridad, reconocimiento de amenazas y procedimientos de respuesta a incidentes.

PLANES DE FORMACIÓN Y CAPACITACIÓN

- **Objetivo**: Asegurar que todos los operadores involucrados en el monitoreo están completamente capacitados en las políticas actualizadas y las herramientas de monitoreo para mejorar la efectividad y eficiencia del proceso de monitoreo.

  Programa de Capacitación:

- El programa de capacitación incluirá sesiones regulares para los operadores nuevos y existentes, diseñadas para cubrir todos los aspectos relevantes de la política de monitoreo y el uso efectivo de las herramientas asociadas.

Métodos y Herramientas de Capacitación

Las capacitaciones se realizan utilizando una combinación de métodos presenciales y en línea para facilitar el acceso y la comodidad de los participantes. Para los cursos autoguiados y las sesiones en vivo, se utilizarán las mismas plataformas, complementadas con el autoaprendizaje, que permiten interacción en tiempo real. Los materiales de apoyo incluirán tutoriales en video, y documentos de referencia rápida, específicamente diseñados para las herramientas de monitoreo que se utilizan en nuestras operaciones, como Zabbix, ThousandEyes, APM Broadcom, y AppDynamics. Estos materiales se centrarán en las funcionalidades y mejores prácticas de cada herramienta para asegurar una comprensión profunda y eficaz de su aplicación en el monitoreo de nuestra infraestructura.

5. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
11/04/2018	Actualizaciones de información	1
17/09/2021	Modificación documento Alberto Salinas - René Barrera	2
23/09/2022	Actualización política	3
24/08/2023	Revisión	4
14/05/2024	Se actualiza el ítem de contenido, se agrega lo siguiente: SEGURIDAD Y PRIVACIDAD EN MONITOREO y PLANES DE FORMACIÓN Y CAPACITACIÓN. El documento se revisa en el marco de la actualización del SGSI año 2024, se realiza inclusión de la sigla del país y la compañía en el código del documento	5

Tabla 1 Control de cambios

6. FLUJO DE APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ
Nombre: Felipe Andrés Melo Amaya Área/Proceso: Centro de Cómputo Fecha:11/04/2018	Nombre: Luisa Gineth Castaño Perea Área/Proceso: Director(a) de operaciones y comunicaciones TI Fecha:14/05/2024	Nombre: Javier Galván Área/Proceso: Gerencia corporativa de tecnología Fecha:20/05/2024

Tabla 2 Flujo de aprobación

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