**Objetivo:**
Asegurar que los Elementos de Configuración (CI) y los servicios que corresponden a los procesos de negocio, sean monitoreados constantemente, así como descartar y categorizar eventos antes de decidir qué acciones son las adecuadas.

Para lograr el objetivo es necesario desarrollar un sistema de monitoreo que garantice un continuo seguimiento a todas y cada una de las aplicaciones del negocio que se encuentren en producción, igualmente el diseño y desarrollo oportuno de acciones preventivas y cuando sea necesario acciones correctivas, frente a los diferentes incidentes que se puedan presentar en las aplicaciones de negocio.

**Alcance:**
Este procedimiento abarca el monitoreo de los siguientes CI´s, correspondientes a los servicios del negocio:
a) Los elementos de configuración.
b) Las licencias de software.
c) Los principales puntos de seguridad de la información.
d) Las herramientas, infraestructura y otros elementos.

**Términos y definiciones:**

1 ACUERDOS DE NIVEL DE SERVICIO (ANS): Corresponde a los acuerdos sobre las normas de un servicio u producto para el correcto funcionamiento de los sistemas de

2 ADMINISTRADORES DE LOS SERVICIOS DE INFORMÁTICA: : Contratistas o personal que forman parte del grupo de soporte en los diferentes niveles, con experiencia, competentes para optimizar los tiempos de respuesta y los niveles de servicio.

3 CERTIFICADOS DE DISPONIBILIDAD DE LICENCIAMIENTO: Documento mediante el cual se garantiza el principio de legalidad y licenciamiento de un recurso disponible para atender un servicio.

4 BIBLIOTECA DEFINITIVA DE MEDIOS (DML): Contiene versiones aprobadas de CI de software. Puede contener licencias y documentación.

5 CAPACIDAD: Asegurar que los servicios de Tecnología de la Información se vean respaldados por una capacidad de procesamiento, almacenamiento, licenciamiento y respaldo entre otros, correctamente dimensionada.

6 CENTRO DE SOPORTE: Su principal objetivo es ofrecer una primera línea de soporte técnico que permita resolver, en el menor tiempo, las interrupciones del servicio.

7 CI: Elemento o ítem de configuración.

8 CLASIFICACIÓN DE LOS EVENTOS: Existen tres tipos de eventos:

8,1 Evento de Información:
Como su nombre lo indica, la notificación de este tipo de evento solo tiene carácter informativo. Lo que quiere decir que normalmente no necesita que se realice ninguna acción. Estos eventos confirman el estado de un dispositivo o servicio, el éxito de una transacción o actividad, o se usan para generar estadísticas de análisis.

8,2 Evento de Advertencia:
En este nivel, la alerta se usa para indicar que existe una situación que debe ser verificada antes de que evolucione y se transforme en un evento excepcional. Estas actividades inusuales en muchos casos, pueden resolverse por sí solas, sin embargo, no hay que subestimar la importancia de prestarles atención pues son indicios de una situación que requiere mayor vigilancia.

8,3 Evento excepcional:
Se asigna a los eventos cuando indican que el servicio está operando de manera irregular, los indicadores planteados en los acuerdo de gestión definidos, probablemente se incumplan, etc. Las excepciones pueden representar un fallo total, un cese en una funcionalidad o una disminución del rendimiento. Este tipo de eventos normalmente precede a la aparición de un incidente si no se atiende a tiempo.

9 CONCEPTOS ITIL:

9,1 Categorías de Eventos y Reglas de Correlación:
Son criterios y reglas usados para decidir la respuesta adecuada ante determinados Eventos. Las reglas de categorización y correlación se usan como parte de los sistemas de monitorización de Eventos.

9,2 Registro de Evento:
Es un cambio de estado significativo para el manejo de algún componente o servicio de Configuración. El término "Evento" también se usa para referirse a las alertas o notificaciones creadas por algún servicio de TI, Elemento de Configuración o herramienta de monitorización. A menudo, los Eventos requieren acciones por parte del personal operativo de TI, y pueden llevar al registro de ciertos Incidentes.

9,3 Tendencias y Patrones de Eventos:
Cualquier tendencia o patrón identificado durante el análisis de Eventos significativos, los cuales sugieren la necesidad de mejoras a la infraestructura.
Nota Importante: Una característica importante de los eventos es que no degradan la calidad del servicio de TI. Si lo hace, automáticamente deja de ser un evento para convertirse en un incidente.

**Políticas de Operación:**

1 Monitoreo y alertas en tiempo real:
Tener la capacidad de monitorear y relacionar amenazas en tiempo real con el fin de evitar contratiempos o una interrupción del sistema.

2 Monitoreo de actividad de usuarios:
Monitorear todas las actividades de las aplicaciones del negocio con el fin de generar alertas sobre infracciones y descubrir malas prácticas y errores.

3 Investigaciones de casos de uso:
Usar el análisis de datos forenses para reducir el riesgo.

4 Detección de amenazas a través del entorno:
Ser capaz de normalizar y correlacionar las diferentes fuentes de datos en un formato común e interpretarlo.

5 Almacenamiento de eventos a largo plazo:
Teniendo en cuenta que a través de logs se transmiten datos de forma ininterrumpida, se debe contar con suficiente espacio para almacenar todo. Se debe realizar un análisis efectivo para poder almacenar muchos datos a largo plazo.

6 Escalabilidad:
Poder cambiar el responsable inicial de soporte asignado a un evento por otra persona con mayor conocimiento y experiencia en el tema a tratar, después de verificar que la atención de la solicitud requiere atención especializada.

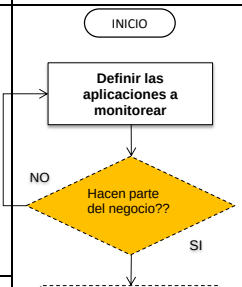
7 Reportes:
Presentar informes cada vez que se genere un evento y cuando se disponga en los ANS. Cumpliendo con las normativas y regulaciones contempladas en el contrato maestro de tecnología.

**Documentos de soporte**

| CÓDIGO | NOMBRE | Actividades | ENTIDAD |
|---|---|---|---|
| **ISO/IEC 12207:2008** | Ingeniería de Sistemas y software - Ciclo de vida de procesos de Software | 1 | ICONTEC |
| **ISO/IEC 15504:2003** | Tecnologías de la Información – Evaluación de Procesos | 1 | ICONTEC |
| **ISO/IEC 15288:2006** | Ingeniería de Sistemas y software - Ciclo de vida de procesos de Sistema. | 1 | ICONTEC |
| **ISO/IEC 9126** | Evaluación de la calidad de software | 1 | ICONTEC |
| **NTC-ISO/IEC 20000-1** | Tecnología de la Información. Gestión del Servicio. Capítulo 10 | 1 | ICONTEC |
| **Decreto 415 de 2016** | Lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones | 1 | MINTIC |
| **MPFT0313F01** | Listado de Aplicaciones y de Herramientas a monitorear que pertenezcan a la línea de negocio | 1,3,4 | EAAB |
| **Ley 1341 de 2009** | Por el cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las Comunicaciones – TIC se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. | 1,3,4,5 | MINTIC |

| | | | |
|---|---|---|---|
| **Anexo 2** | Condiciones Técnicas del Contrato Marco | 1 | EAAB |

**Actividades**

| # | Nombre de la actividad | Descripción | Registro | Responsable |
|---|---|---|---|---|
| 1 |  | Realizar la revisión de las aplicaciones, herramientas y software a monitorear, que hagan parte de los servicios del Negocio. Teniendo como base el anexo 2 de las condiciones técnicas del contrato outsourcing.<br><br>Todas las actividades a las que se les debe realizar monitoreo de acuerdo con lo definido en el anexo 2, y que haga parte de los servicios críticos del negocio, deben estar definidas en el formato MPFT0313F01. | Plan de Monitoreo Anexo 2 Condiciones Técnicas del Contrato Marco. | Experto Ejecutor del Servicios (Contrato Marco) / Líder del servicio (EAAB) |
| | Definir periodos de monitoreo para las herramientas, aplicaciones y software que afecten las aplicaciones del negocio | Definir los periodos de Monitoreo. Se debe diligenciar el formato MPFT0313F01, junto con las áreas involucradas, para definir los tiempos de monitorea y las respectivas acciones que estas conllevan. | MPFT0313F01 Listado de aplicaciones y de herramientas a monitorear que pertenezcan a la línea de negocio | Experto Ejecutor de Servicios, Supervisor, Facilitador de calidad de la DSI |
| | Ejecutar actividades de control | Ejecutar los monitoreos en las fechas definidas, hacer seguimiento y registrar todos los eventos. Teniendo como soporte lo definido en la actividad anterior | Herramienta de gestión. | Experto Ejecutor de Servicios, Supervisor, Facilitador de calidad de la DSI |
| 2 | Seguimiento a los resultados del monitoreo<br>NO<br>Se presentan alarmas?<br>SI | Realizar seguimiento a los resultados presentados en el proceso de monitoreo de las aplicaciones.<br><br>Si se presentan alarmas que afecten la funcionalidad de las aplicaciones monitoreadas, realizar el análisis y asignación al responsable correspondiente. | Informe disponibilidad del servicio – Proactive Net | Experto Ejecutor de Servicios, Supervisor, Facilitador de calidad de la DSI |
| 3 | **Registro y nivel de escalamiento del evento** | Los eventos se deben almacenar en la herramienta de gestión que se defina para tal fin, teniendo en cuenta su periodicidad de ocurrencia.<br><br>Los eventos se deben informar de la siguiente manera:<br>a. Evento Informativo. Se registraran en la herramienta BMC Proactive Net para una posterior consulta.<br><br>b Evento de advertencia. Se informa mediante correo electrónico al facilitador de calidad y Líder de la DSI, de la ocurrencia del evento.<br><br>c. Evento excepcional Se informa mediante correo electrónico al Director de la DSI, Líder de la DSI y facilitador de calidad de la ocurrencia del evento incluyendo la criticidad del mismo. | Herramienta de gestión. | Líderes DSI |
| | **Seguimiento y Correlación de Eventos**<br>A | Una vez definido la clasificación de los eventos, se realiza la categorización de los mismos para su seguimiento.<br><br>Evento de información - Se realiza seguimiento a demanda de estos eventos y se deja constancia de su interpretación.<br><br>Evento de advertencia - Se realiza seguimiento mensual de estos eventos una vez se presente el informe de seguimiento de eventos informativos y que requieran acción de mejora, dejando constancia de este seguimiento.<br><br>Evento excepcional - Una vez determinado este tipo de evento, se realiza acción de mejora inmediata, con el fin de evitar que se convierta en un incidente.<br><br>Se identifica si hay correlación del evento, teniendo como base la siguiente información:<br><br>a. Numero de eventos similares<br><br>b. Numero de CI´s, aplicaciones o herramientas que generan elementos similares.<br><br>c. Si el evento presenta alguna excepción | Formato MPFT0313F01<br><br>Herramienta de gestión.<br><br>Informe del evento detectado y su información correspondiente. - Herramienta de Gestión. | Líderes DSI involucrados |

| | | | | |
|---|---|---|---|---|
| 4 |  | d. Nivel de prioridad asignado.<br><br>Notificación a todos los que puedan resultar involucrados cuando se presenten los eventos de advertencia o excepcional.<br><br>Definición y ejecución de las acciones a seguir por parte del experto (s) en el tratamiento del evento.<br><br>Seguimiento a efectividad de las acciones implementadas para e tratamiento del evento.<br><br>Registro del evento en la base de datos definida. | Plan de acción (Actividad, tiempos, recursos y responsables)<br><br>Aprobación de la solución por parte del usuario. | |
| 5 |  | Toda actualización de los eventos ejecutados debe quedar debidamente soportada en la herramienta de gestión.<br><br>El facilitador de calidad realizará un seguimiento bimensual de todos los eventos generados, dejando evidencia en una ayuda de memoria, que será levantada junto con los responsables del evento presentado.<br><br>Los eventos que requieran planes de mejoramiento mediante oportunidades de mejora, únicamente se cierran cuando las evidencias soporten que están terminadas todas las actividades que lo generaron.<br>Estos planes harán parte del informe de Oportunidades de mojara que debe presentar el contratista, mensualmente, en el informe de gestión del contrato.<br><br>El cierre de los eventos que se generen se cierran con las siguientes autorizaciones:<br><br>a. Evento Informativo, no genera cierre.<br><br>b. Evento de advertencia, este evento se cierra automáticamente, una vez las acciones tomadas conllevan al umbral de advertencia al nivel normal.<br><br>c. Evento excepcional, se cierra en el proceso que corresponda ya sea cambio, problema y/o incidente, sea superado. | Informe de seguimiento de eventos - Informe de Gestión.<br><br>Actualización estado de eventos en la herramienta de gestión | Administradores de base de datos de eventos |

**Control de cambios**

| FECHA | DESCRIPCIÓN Y JUSTIFICACIÓN DEL CAMBIO | VERSIÓN |
|---|---|---|
| xx/05/2021 | Creación del documento | 1 |

**Control de revisión y aprobación**

| Elaboración | Revisión | Aprobación |
|---|---|---|
| Héctor Manuel Monroy Moreno<br>Dirección Servicios de Informática<br>Gerencia de Tecnología | Lina María Cruz Silva<br>Director Técnico<br>Dirección Servicios de Informática<br>Gerencia de Tecnología | **Lina María Cruz Silva**<br>Director Técnico<br>Dirección Servicios de Informática<br>Gerencia de Tecnología |
| 08/02/2021 | 03/03/2021 | XX05/2021 |