

Control de Versiones

Versión	Fecha	Autor	Descripción
0	14/12/2016	NEIXAR	Se genera la versión base del proceso de Gestión de Eventos.
1	16/11/2018	NEIXAR	Se incluye código de proceso, se realiza mejora continua a Políticas, Entradas y salidas, Procedimiento, Diagrama, Roles y Responsabilidades, Métricas, Referencias, Glosario, se cambió el apartado 10 "Registros" por "Anexos".
2	29/04/2019	NEIXAR	Se actualiza la imagen y estructura del proceso, se actualiza el Objetivo, Políticas, Diagrama y Glosario.

Objetivo

Detectar la degradación o interrupción de los servicios, por medio de alertas automáticas generadas por las herramientas de monitoreo.

Alcance

El presente proceso sirve de apoyo para gestionar el monitoreo y registro de todos los eventos en la infraestructura tecnológica de los servicios y aplicaciones de TIC que son monitoreados a través del Servicio Administrado para el Modelado y Monitoreo de los Servicios de TIC en el ISSSTE (SAMMSSTIC), a fin de mantener una adecuada operación.

Políticas

Generales

1. La información histórica del monitoreo deberá resguardarse en una Base de Datos y estar disponible en cualquier momento.
2. Solo serán notificados aquellos eventos definidos en las herramientas de monitoreo como críticos.
3. Los tipos de eventos de monitoreo son los siguientes:
 - Alerta
 - Informativo
 - Excepción

Específicas

1. El Responsable del Servicio de TIC en Operación debe definir los eventos, variables, umbrales, frecuencia, reportes de monitoreo, notificaciones y el nivel de acceso a los elementos monitoreados.
2. Se debe considerar el calendario de cambios programados para definir los eventos que deben o no ser monitoreados y filtrados.
3. Todo evento detectado en las herramientas de monitoreo debe quedar registrado en la herramienta de operación o administración del proceso.

Proceso de Gestión de Eventos

4. Todo evento atendido satisfactoriamente debe ser cerrado en la herramienta de monitoreo y administración del proceso.
5. Todo evento tipo excepción que representa una interrupción o degradación al servicio, se debe registrar como un incidente en la herramienta de gestión correspondiente.
6. Los eventos identificados durante ventanas de mantenimiento no serán considerados para el cálculo de niveles de servicio.
7. Los tiempos de indisponibilidad derivados de una ventana de mantenimiento a las herramientas de monitoreo no serán considerados en el cálculo de los niveles de servicio.
8. El Gestor del proceso deberá generar los reportes de indicadores que se requieran en el proceso para identificar oportunidades de mejora.
9. El Dueño del proceso deberá revisar acorde a la frecuencia establecida, los indicadores de desempeño definidos para este proceso, para validar el cumplimiento de los objetivos del mismo o bien, identificar desviaciones y corregirlas.
10. El Dueño del proceso deberá identificar, discutir y proponer mejoras al proceso a través del Proceso de Mejora Continua.

Entradas

Entrada	Criterio Aplicable
Acuerdos de Niveles de Servicio.	N/A
Programa de Capacidad.	N/A
Programa de Disponibilidad.	N/A
Calendario de cambios.	N/A

Roles y Responsabilidades

Rol	Responsabilidades
Dueño del Proceso	<ul style="list-style-type: none"> • Dirigir el proceso de manera eficiente y efectiva. • Garantizar la efectividad y cumplimiento del proceso. • Identificar y corregir las desviaciones del proceso. • Revisar los indicadores de desempeño del Proceso e identificar mejoras.
Gestor del Proceso	<ul style="list-style-type: none"> • Responsable de la gestión operativa del proceso. • Generar las métricas e indicadores clave de desempeño.
Operador de Monitoreo (Proveedor)	<ul style="list-style-type: none"> • Monitorear, medir y reportar los umbrales definidos para cada uno de los servicios. • Monitorear el desempeño y la capacidad del servicio. • Proveer de estatus operacional según sea requerido. • Validar que todos los componentes de la herramienta de monitoreo se encuentren funcionando correctamente y en caso de detectarse alguna desviación de la operación normal, notificarlo.

Proceso de Gestión de Eventos

Coordinador de Monitoreo (Proveedor)	<ul style="list-style-type: none"> Revisar los análisis de tendencias de eventos y reportar al Responsable del Servicio.
Responsable del Servicio de TIC en Operación	<ul style="list-style-type: none"> Asistir en la investigación y diagnóstico de problemas del servicio.

Matriz de Roles y Responsabilidades

La definición de roles y responsabilidades aplicadas en este documento:

Responsable (R): Este rol realiza el trabajo y es responsable por su ejecución.

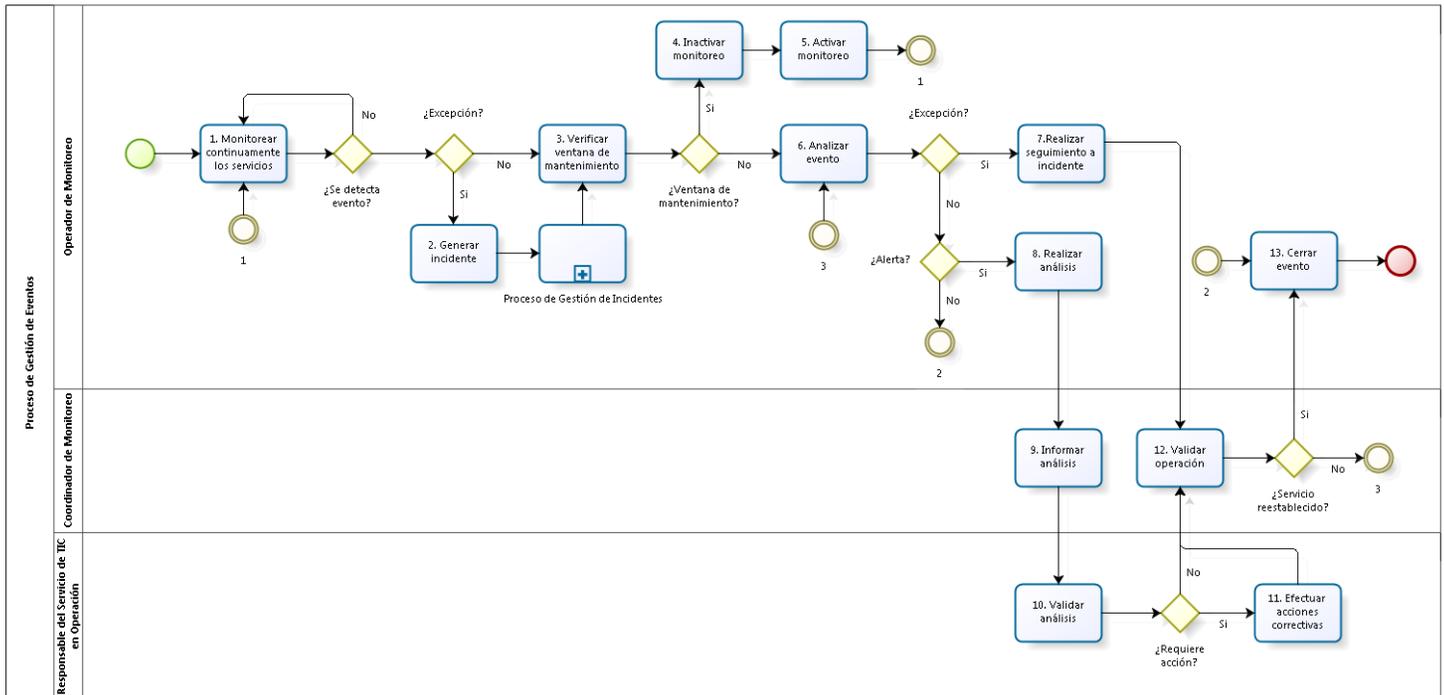
Aprobador (A): Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Es quien debe asegurar que se ejecutan las tareas asignadas.

Consultado (C): Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información.

Informado (I): Este rol debe ser informado sobre el progreso y los resultados del trabajo.

Tarea	Operador de monitoreo	Coordinador de monitoreo	Responsable del Servicio de TIC en Operación
1. Monitorear continuamente los servicios	R	A	
2. Generar incidente	R	A	I
3. Verificar ventana de mantenimiento	R	A	
4. Inactivar monitoreo	R	A	
5. Activar el monitoreo del servicio en herramienta	R	A	
6. Analizar evento	R	A	
7. Realizar seguimiento a incidente	R	A	
8. Realizar análisis (correlacionar eventos similares)	R	A	
9. Informar análisis		A,R	I
10. Validar análisis			R
11. Efectuar acciones correctivas			R
12. Validar operación	R	A	C

Diagrama del Proceso



Descripción Detallada del Proceso

ID	Responsable / Participantes	Entradas	Actividad / Descripción	Salidas
1	Operador de Monitoreo	Programa de Capacidad, Programa de Disponibilidad, Acuerdos de Nivel de Servicio	<p>Monitorear continuamente los servicios</p> <p>Monitorea y vigila, con apoyo de la herramienta de monitoreo, los servicios de TIC y su infraestructura: ¿Se detecta evento?</p> <ul style="list-style-type: none"> ➤ Si, ¿Excepción? <ul style="list-style-type: none"> ○ Si, ir al paso 2 ○ No, ir al paso 3 ○ No, ir al paso 1 	Evento
2	Operador de Monitoreo	Evento	<p>Generar incidente</p> <p>Se genera incidente de manera automática. Ir al Proceso de Gestión de Incidentes Ir al paso 3</p>	Ticket INC

**Proceso de Gestión de Eventos**

ID	Responsable / Participantes	Entradas	Actividad / Descripción	Salidas
3	Operador de monitoreo	Calendario de cambios	Verificar ventana de mantenimiento Verifica si existe alguna ventana de mantenimiento, que pudiera causar la afectación y/o degradación del servicio: ¿Ventana de mantenimiento? ➤ Si, ir al paso 4 ➤ No, ir al paso 6	N/A
4	Operador de monitoreo	N/A	Inactivar monitoreo El operador debe inactivar el monitoreo del servicio en la herramienta de monitoreo por el tiempo que dure la ventana de mantenimiento al servicio o CI que se verá afectado por la ventana.	N/A
5	Operador de monitoreo	N/A	Activar el monitoreo del servicio en herramienta Una vez finalizado el cambio, el operador de monitoreo debe verificar que se siga monitoreando el servicio o C.I. que estuvo dentro de la ventana de mantenimiento. Ir al paso 1	N/A
6	Operador de Monitoreo	Evento	Analizar evento Analiza el evento: ¿Excepción? ➤ Si, ir al paso 7 ➤ No, ¿Alerta? <ul style="list-style-type: none">○ Si, ir al paso 8○ No, Informativo, ir al paso 13	N/A
7	Operador de Monitoreo	Ticket INC	Realizar seguimiento a incidente Realiza el seguimiento al incidente generado previamente por las herramientas de monitoreo. Ir al paso 12	N/A
8	Operador de monitoreo	N/A	Realizar análisis (correlacionar eventos similares) Derivado de las alertas notificadas por las herramientas de monitoreo, el operador deberá de realizar el análisis con el cual se logre identificar un posible impacto a la disponibilidad y/o capacidad a los servicios o CI's configurados en las herramientas.	Análisis de Alertas

**Proceso de Gestión de Eventos**

ID	Responsable / Participantes	Entradas	Actividad / Descripción	Salidas
9	Coordinador de Monitoreo	N/A	Informar análisis Una vez realizado el análisis de las alertas se deben informar al dueño del servicio para que tome las acciones correspondientes.	Correo electrónico, Análisis de Alertas
10	Responsable del Servicio de TIC en Operación	Correo electrónico, Análisis de Alertas	Validar análisis El Responsable del Servicio de TIC en Operación con base al análisis generado por parte de monitoreo deberá identificar y decidir si se requiere aplicar alguna acción para solventar el evento: ¿Requiere acción? ➤ Si, ir al paso 11 ➤ No, ir al paso 12	N/A
11	Responsable del Servicio de TIC en Operación	N/A	Efectuar acciones correctivas El Responsable del Servicio de TIC en Operación realiza las acciones correctivas para solventar el evento.	N/A
12	Coordinador de Monitoreo	N/A	Validar operación Verifica que el servicio esté operando en condiciones normales y/u óptimas: ¿Servicio restablecido? ➤ Si, ir al paso 13 ➤ No, ir al paso 6	N/A
13	Operador de monitoreo	N/A	Cerrar evento Se cierra el o los eventos de manera automática en las herramientas de monitoreo y en la herramienta de gestión que fueron alertados. Fin del Procedimiento	N/A

Salidas

Entrada	Criterios de Aceptación
Correo electrónico	N/A
Evento	N/A
Análisis de alertas	N/A

Reportes

Los reportes del Proceso de Gestión de Eventos tendrán la siguiente estructura:

- Nombre
- Objetivo
- Frecuencia
- Fuente
- Distribución

Métricas

Para obtener información clave del proceso, se utilizarán las siguientes métricas:

MÉTRICA	FRECUENCIA
Número de eventos por tipo	Mensual
Número de eventos por severidad	Mensual
Número de eventos	Mensual

Indicadores clave de desempeño (KPI's)

Para medir la eficiencia del proceso, se utilizarán los siguientes indicadores clave de desempeño:

KPI	DESCRIPCIÓN	MÉTODO DE CÁLCULO	FRECUENCIA	META
% de eventos críticos por aplicación sustantiva	Medir la tendencia de eventos que se presentan por aplicación sustantiva	$((\text{Número de eventos por aplicación}) / (\text{Número total de eventos}) * 100)$	Mensual	N/A
% de disponibilidad por aplicación crítica	Medir la disponibilidad de las aplicaciones críticas	$(\text{Suma del tiempo disponible de las aplicaciones críticas} / 100) * 100$	Mensual	N/A

Anexos

1. N/A.

Referencias

1. Plan Nacional de Desarrollo 2013-2018.
2. Programa para un Gobierno Cercano y Moderno 2013-2018 (PGCM).

Proceso de Gestión de Eventos

3. ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, última reforma publicada DOF 23-07-2018.
4. Biblioteca de Infraestructura de Tecnologías de Información (ITIL v3, 2011)
Procesos relacionados:
 - Proceso de Gestión de Niveles de Servicio
 - Proceso de Gestión de la Capacidad
 - Proceso de Gestión de la Disponibilidad
 - Proceso de Gestión de Incidentes

Glosario de términos y definiciones

Concepto	Definición
Alerta.	Se asigna a aquellos eventos que indican que el servicio se aproxima o rebasa un umbral definido. 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.
Dueño del proceso.	Es la persona responsable final (que debe rendir cuentas) y garantizar que un proceso es adecuado para el propósito.
Entradas.	Los elementos/productos del trabajo en un proceso que se consideran necesarios para soportar la operación de un proceso. Son los que posibilitan la toma de decisiones clave, proveen un registro y traza de auditoría de las actividades del proceso y posibilitan el seguimiento en caso de un incidente. Se definen al nivel de práctica de gestión clave y pueden incluir algunos productos de trabajo usados únicamente dentro del proceso y son, comúnmente, entradas esenciales para otros procesos.
Evento.	Es un cambio de estado que tiene importancia para la Gestión de Servicios de TIC u otro elemento de configuración. El término también se utiliza en el sentido de una alerta o notificación creada por cualquier servicio de TIC, elemento de configuración o herramienta de monitoreo.
Evento Informativo.	Son aquellos eventos que no requieren, en principio, ninguna respuesta y que por tanto no representan una excepción
Excepción.	Se asigna a los eventos cuando indican que el servicio está operando de manera irregular: los SLAs y OLAs se han incumplido. Las excepciones pueden representar un fallo total, un cese en una funcionalidad o una disminución del rendimiento y se debe generar de manera automática un Incidente
Gestor del proceso.	Es el rol responsable de la gestión operativa de un proceso.
Incidente.	Es una interrupción no planificada de un servicio de TI o la reducción en la calidad de un servicio de TI.
Indicadores Clave de Desempeño (KPI).	Es una métrica que se utiliza para ayudar a gestionar un servicio de TIC, proceso, plan, proyecto u otra actividad. Los indicadores claves de desempeño se utilizan para medir el logro de los factores críticos de éxito.
INSTITUTO o ISSSTE.	Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado
MAAGTICSI.	Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información.
Matriz RACI.	Es un modelo usado para ayudar a definir los roles y responsabilidades de un proceso.
Métrica.	Es algo que se mide y se informa para ayudar a gestionar un proceso, servicio de TIC o actividad.
Monitoreo.	Es una observación repetida de un elemento de configuración, servicio de TI o proceso para detectar eventos y para asegurar que el estado actual sea conocido.
Procedimiento.	Es un documento que contiene pasos que especifican cómo llevar a cabo una actividad. Los procedimientos se definen como parte de los procesos.

Proceso de Gestión de Eventos

Programa de Capacidad.	Es un programa para asegurar que los requerimientos actuales y futuros de la capacidad de servicios de TIC pueden ser proporcionados de una manera rentable.
Programa de Disponibilidad.	Es un plan para asegurar que los requerimientos actuales y futuros de la disponibilidad de servicios de TIC pueden ser proporcionados de una manera rentable.
Rol.	Es un conjunto de responsabilidades, actividades y autoridades asignadas a una persona o equipo. Un rol se define en un proceso o función.
Salidas.	Los elementos/productos del trabajo en un proceso que se consideran necesarios para soportar la operación de un proceso. Son los que posibilitan la toma de decisiones clave, proveen un registro y traza de auditoría de las actividades del proceso y posibilitan el seguimiento en caso de un incidente. Se definen al nivel de práctica de gestión clave y pueden incluir algunos productos de trabajo usados únicamente dentro del proceso y son, comúnmente, entradas esenciales para otros procesos.
Servicio (TIC).	Es un servicio relacionado a las Tecnologías de la Información que puede ser proporcionado por recursos internos o por un proveedor y combina elementos tecnológicos, de comunicación, personas y procesos.
TIC.	Las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.
Ticket.	Registro de solicitud, incidente, problema, o cualquier otra actividad que el usuario y/o los responsables de la Infraestructura y Servicios de TIC reportan a través de una herramienta (Mesa de Servicio Central)
Ventana de mantenimiento.	Para realizar operaciones de mantenimiento en sistemas de destino, puede definir ventanas de mantenimiento durante momentos de inactividad para que no afecten a la ejecución de flujos de trabajo en los destinos.

Firmas

Elaboró	Aprobó
Nombre Miguel Ángel Lomelí Valderrábano	Nombre
Cargo Analista de Modelado de Aplicaciones	Cargo Jefatura de Servicios de Planeación
Fecha 29/04/2019	Fecha 29/04/2019
Firma	Firma