Supersalud	**GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN**	**CÓDIGO**	DIMN13
	MANUAL PARA LA PRESTACIÓN DEL SERVICIO PARA LA ATENCIÓN DE INCIDENTES	**VERSIÓN**	1
		FECHA	30/01/2023

Manual para la prestación del servicio para la atención de incidentes

Superintendencia Nacional de Salud

Fecha del documento (30 – 01 – 2023)

Contenido

Índice de Tablas

Índice de Ilustraciones

Objetivo

Identificar y gestionar los incidentes en TI recibidos por las dependencias o interesados, mediante la aplicación de metodologías y tratamiento estandarizado para la interpretación y solución del incidente, con el propósito de cumplir con los incidentes del usuario bajo las condiciones y alcance definidos en los Acuerdos de Niveles de Servicio de TI y así se cumpla la expectativa de la entidad y se asegure que estos servicios prestados se realicen de forma efectiva y eficiente.

Alcance

El uso del presente documento aplica para todos los procesos del Sistema Integrado de Gestión, a la operación de la entidad y la prestación del servicio para la atención de incidentes con la recepción, registro, categorización del requerimiento, continua con el análisis, interpretación, administración una vez realizada dicha gestión termina con la solución y registro del incidente solicitado y da cumplimiento a los lineamientos establecidos en la Norma Técnica Colombiana NTCGP – 1000 (desarrollada para aplicar sistemas de gestión de calidad en el sector público) en especial en el numeral 6.3 Infraestructura, para los literales b) herramientas, equipos y sistemas de información (tanto hardware como software) para la gestión de los procesos, y c) servicios de apoyo (tales como transporte o comunicación).

Políticas de Operación

Este documento apoya a la Subdirección de Tecnología de la Información en la atención y resolución de incidentes, alineado con las mejores prácticas de ITIL®. Identifica y establece los incidentes recibidos en TI define el tratamiento que debe realizarse con el objeto de cumplir con lo requerido por el usuario bajo las condiciones y alcance definidos en los Acuerdos de Niveles de Servicio.

Generalidades

La Subdirección de Tecnología de la Información debe poner a disposición servicios tecnológicos que cumplan las expectativas de la entidad y debe asegurar que estos servicios prestados se realicen de forma efectiva y eficiente, es por ello que la atención de incidentes de Tecnologías de la Información en la Supersalud, deberá cumplir con cada uno de los siguientes criterios:

- Trabajar para asegurar la prestación de mesa de servicio
- Detectar cualquier alteración en los servicios de Tecnologías de la Información.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el Acuerdo de Nivel de Servicio (SLA) correspondiente.

Esta actividad requiere un estrecho contacto con los usuarios, por lo que el Centro de Servicios (Service Desk) debe jugar un papel esencial en el mismo.

El siguiente diagrama resume las actividades en la gestión de incidentes; estas actividades se encuentran diagramadas de manera más específica en la actividad clave de éxito Gestionar TI:

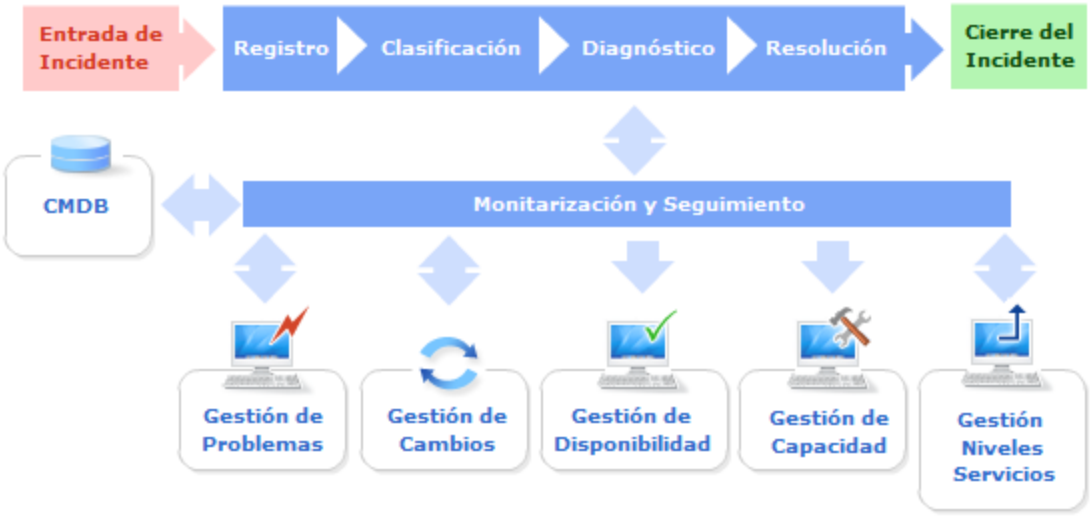

Ilustración 1 Actividades en la gestión de incidentes.

Fuente: ITIL®-Gestión de Servicios TI

Roles que participan en las actividades

Para la atención de incidentes deben existir los siguientes roles:

- **Gestor de incidentes:** Asegurar que se cumpla con calidad el flujo de trabajo del proceso, políticas y procedimientos de la Administración de Incidentes

- **Analista nivel 1 de incidentes:** Recibir llamadas de servicio, registrarlas, dar soporte inicial y realizar escalamientos a los grupos responsables de su atención

- **Analistas de niveles superiores:** Apoyar que se cumpla el proceso mediante la resolución de llamadas de servicio que le sean asignadas.

Actividades de la Gestión de Incidentes

Documentar el incidente

Actividades para ejecutar en la Documentación del incidente

El Analista y/o Profesional de Tecnologías de la Información deberá:

- Identificar información del incidente, para ello leerá la información suministrada por el usuario o por la herramienta de monitoreo del sistema, en la cual se aprecia la narrativa del usuario en la que manifiesta el incidente presentado.

- Registrar información del incidente y en aras de garantizar que la información asociada se encuentra completa para la atención del incidente de ser necesario contactar al usuario y realizar preguntas que ayuden a aclarar el incidente reportado, dando coherencia al mismo.

- Categorizar el incidente para así dar un nivel de prioridad mayor a los incidentes que tengan un mayor impacto para la entidad.

- Identificar los servicios afectados que se encuentren relacionados con el incidente reportado y así asignar una prioridad para reestablecer la operación del servicio afectado.

Criterio - Atención de incidentes

Actividades para ejecutar en la Atención de incidentes

El Analista y/o Profesional de Tecnologías de la Información deberá:

- Validar si el incidente reportado debe ser tratado como un incidente mayor, debido a su afectación a uno de los servicios críticos de la entidad.

- Realizar un análisis para determinar si es un incidente mayor, debe ser basado en la cantidad de usuarios afectados, la criticidad del servicio afectado y su tiempo de afectación o caída del servicio, es decir cuando es reportado un incidente por la no disponibilidad de un servicio tecnológico y la situación esté afectando más del 30% de los usuarios que hacen uso del servicio; o cuando un servicio tecnológico no esté disponible durante 30 minutos para los funcionarios que lo necesitan para desempeñar sus funciones

- Escalar los incidentes mayores de acuerdo a lo descrito en la actividad clave de éxito ***Gestionar TI***, en lo correspondiente a “Gestionar problemas y cambios” , para que un grupo especializado se encargue y agilice su solución.

- Cuando un caso no es categorizado como un Incidente Mayor, debe consultar en los registros de la base de datos de conocimiento, Base de Datos de Errores conocidos o manuales operativos, en busca de información que agilice el tratamiento de un incidente y permita proponer una solución.

- Determinar las actividades a realizar y si la solución temporal o permanente al incidente reportado por el usuario, lo puede realizar el primer nivel de servicio.

- En caso de no poder ser solucionado por el primer nivel de servicio debe identificar los servicios, activos y usuarios de tecnologías de la Información afectados por el incidente y analizar y definir el equipo de Soporte de 2do. Nivel al que se le escalará el incidente.

El especialista nivel 2 deberá:

- Investigar la causa raíz del incidente mediante la revisión de manuales de operación, instructivos, llamadas al cliente que permitan la identificación de la causa del incidente y determinar una potencial solución. Esta investigación se debe realizar con relación a los ítems de configuración afectados y deberá cubrir la validación de canales de comunicación del servicio, número de usuarios afectados y plataformas que soportan el servicio.

- Realizar las actividades necesarias para dar una solución temporal o permanente al incidente reportado por el usuario. En caso de que no se

encuentre una solución exitosa o la solución del incidente sea temporal, este debe ser escalado a la actividad clave de éxito gestión de problemas para su tratamiento.

- Realizar cambios aprobados en los casos que haya incidentes que lo requieran de acuerdo con lo descrito en la actividad clave de éxito ***Gestionar TI***, en lo correspondiente a “Gestionar problemas y cambios.”

- Notificar en caso de que el incidente no pueda ser resuelto por él y deberá escalarlo al proveedor/fabricante para que éste se encargue de la solución del incidente. De forma complementaria, se debe monitorear que el fabricante brinde una solución en el menor tiempo posible y facilitarle la información y recursos que requiera para solucionar el incidente.

- El proveedor con el apoyo de los profesionales especializados de las áreas operativas de la entidad se encargará de resolver el incidente y posteriormente notificará al analista de primer nivel para realizar las actividades de cierre del incidente.

El Analista y/o Profesional de Tecnologías de la Información deberá:

- Reunir toda la información relacionada con la solución del incidente (actas de cambio, aceptación del área usuaria, modificar el estado del incidente), para el respectivo registro en la base de datos de errores conocidos y su documentación en la base de datos de conocimiento.

- Notificar al usuario mediante correo electrónico la resolución del incidente para que éste responda por medio de la encuesta de satisfacción la evaluación del servicio prestado. Si el usuario no manifiesta su inconformidad en las posteriores 48 horas a la solución del caso, éste será cerrado.

Actividades en el Monitoreo de incidentes

Actividades para ejecutar en el Monitoreo de incidentes El Analista y/o

El Analista y/o Profesional de Tecnologías de la Información deberá:

- Monitorear histórico de incidentes validando que todos los incidentes se hayan cerrado correctamente y se les haya dado una solución efectiva. Con el monitoreo del histórico de incidentes se pueden identificar casos que han sido recurrentes y así escalar el incidente a la actividad clave de éxito Gestión de Problemas, con el fin de buscar una solución definitiva al incidente repetitivo.

- Validar el listado de incidentes activos, verificando que el tiempo de respuesta no sobrepase los niveles de servicio acordados, validando la satisfacción del usuario con el servicio prestado.

- Determinar los incidentes que sobrepasen el límite de tiempo en un nivel de servicio y escalarlo al siguiente nivel para que reciba un tratamiento respectivo por parte de un profesional o grupo especializado relacionado al tipo de incidente.

- Cuando la solución la debe ejecutar el proveedor / fabricante deberá realizar un seguimiento del cumplimiento de los plazos acordados y a la solución de incidentes ejecutada. El gestor de incidentes, se deberá encargar de hacer seguimiento a los incidentes escalados al proveedor / fabricante y así garantizar que se dé una solución efectiva dentro de los plazos establecidos en los acuerdos del servicio. En caso de incumplimiento por parte del proveedor / fabricante, se deben remitir a las sanciones estipuladas en el contrato del servicio.

Definiciones

- ✓ **ANS de TI Acuerdos de niveles de servicio de TI:** Acuerdos de niveles de servicio – Es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

- ✓ **ALO: Acuerdos de niveles de operación –** Se trata de un acuerdo entre la oficina de tecnologías de la información y otra dependencia solicitante. Brinda apoyo en la prestación de servicios al solicitante por parte de la oficina de tecnologías de la información, define los bienes y servicios que se proveen y las responsabilidades de ambas partes.

- ✓ **Base de Datos de Conocimiento:** Base de datos que contiene los conocimientos de la entidad, tales como manuales, procedimientos, políticas, entre otros. Por medio de esta base de datos se analizan, almacenan y se comparte la información al interior de la entidad, con el fin de mejorar la eficiencia en algunos procesos y reducir la necesidad de redescubrir la información

- ✓ **Base de Datos de Errores Conocidos:** Esta base de datos es administrada por la Gestión del Problemas y utilizada por Gestión del Incidente para la solución de incidentes repetitivos.

- ✓ **Ciclo de vida del Incidente:** Fases detalladas en el ciclo de vida de un Incidente. Las fases son detección, diagnóstico, reparación, recuperación y restauración.

- ✓ **Detección de Incidentes:** La detección de incidentes es una etapa en el ciclo de vida del incidente, lleva a conocer el incidente al proveedor de servicios. La detección puede ser automática, o puede ser resultado de un incidente comunicado por un usuario.

- ✓ **Diagnóstico de Incidentes:** Etapa en el ciclo de vida de un incidente. El propósito de diagnóstico es identificar una Alternativa para dar solución a un Incidente.

- ✓ **ITIL (Information Technology Infrastructure Library):** Biblioteca de Infraestructura de Tecnologías de Información.

- ✓ **Plataforma web CA:** Software web para reportar los incidentes o servicios que requieran los usuarios de la Superintendencia Nacional de Salud.

- ✓ **Prioridad:** Categoría empleada para identificar la importancia relativa de un incidente. La Prioridad se basa en el Impacto y la Urgencia, y es utilizada para identificar los plazos requeridos para la realización de las diferentes acciones. Por ejemplo, un ANS de TI podría indicar que los Incidentes de Prioridad 2 deben ser resueltos en menos de 12 horas

- ✓ **Requerimiento:** Un requerimiento es una descripción de una condición o capacidad que debe cumplir un sistema, ya sea derivada de una necesidad de tal manera que le sea útil a los funcionarios o a los usuarios finales.

- ✓ **Restauración del servicio:** La restauración del servicio, es la toma de acción para restaurar un servicio de TI a los usuarios tras reparar y recuperarse de un incidente.

- ✓ **Soporte Técnico:** El soporte técnico se define como todas las actividades humanas que se deben realizar para corregir una o más fallas técnicas que los equipos puedan presentar con relación al hardware, software y sistemas de información cuando son operados por los usuarios.

- ✓ **SLA -Service Level Agreement**: Acuerdo de Nivel de Servicio: Describe un servicio de Tecnologías de la Información, documenta los objetivos de nivel de servicio y especifica las responsabilidades del proveedor de servicios de Tecnologías de la Información y del cliente.

- ✓ **TI:** Tecnología de la Información.

- ✓ **Nivel 1:** Servicio prestado por un técnico de mesa de ayuda, los cuales se basan en un conjunto de recursos técnicos y humano que permitirán dar soporte a diferentes usuarios informativos de la entidad. Estos servicios pueden ser prestados personalmente, telefónico o remotamente.

- ✓ **Nivel 2:** La prestación del servicio es ofrecida por un analista, técnico o profesional especializado en un tema específico por la oficina de tecnologías de la información.

- ✓ **Nivel 3:** Son los incidentes que la mesa de ayuda ni por la Oficina de Tecnologías de la Información pueden solucionarlos, ya que son servicios categorizados por garantías.