Seguridad del documento

La clasificación de seguridad de la información de este documento, se ha establecido como bajo. Se ha creado y organizado con la expectativa de que esté a disposición de las unidades administrativas del Gobierno del Estado de México (GEM) que lo requieran, pero debe protegerse de la manipulación no autorizada.

Términos de uso

Se espera que el contenido del Estándar para la Administración de Incidentes, se modifique conforme la evaluación, revisión y aprobación de los mismos, es decir, debe ser considerado como un documento de trabajo dentro del Gobierno del Estado de México.

Revisiones

Fecha	Autor	Versión	Descripción
03/06/2013	Marco A. Reyes G.	0.1	

Tabla de contenido

1. Introducción

En la terminología de la Administración de Servicios, un incidente es definido como cualquier evento que no es parte de la operación estándar de un servicio, y el cual causa o puede causar una interrupción o reducción en la calidad del servicio.

En el escenario ideal, la Administración de Incidentes es provista por la Mesa de Servicio y los grupos de soporte (2º y 3er nivel). Los usuarios contactan a la Mesa de Servicio, el registro del incidente es creado, esta información es actualizada y pasa a los diferentes grupos dependiendo de la especialización requerida (este paso deberá ser implementado en la organización de acuerdo a los recursos humanos y tecnológicos con los que se cuenta). Durante la vida del incidente son identificados diferentes estados, que notifican el progreso y permiten reportar como son manejados los incidentes. Todos los grupos involucrados en el proceso Administración de Incidentes tienen la responsabilidad de monitorear o revisar continuamente y asegurar que los incidentes vayan cambiando de estatus en cuanto a su atención.

Durante la vida de un incidente, este puede ser asignado a diferentes grupos pero siempre quedará bajo la responsabilidad de la Mesa de Servicio, la cual monitoreará todos los incidentes para asegurar que los tiempos establecidos en los Acuerdos de Niveles de Servicio sean cumplidos.

2. Objetivo del Proceso

Asegurar que todos los incidentes son resueltos y restaurar los servicios lo más rápido posible, acorde a la definición de prioridades y dentro de los tiempos acordados prevaleciendo el principio “tiempo mínimo de interrupción”.

Los objetivos específicos del proceso de Administración de Incidentes de la DGSEI son:

- Registrar todos los incidentes que ocurran
- Resolver los incidentes lo más rápido posible
- Restaurar el servicio lo más pronto posible dentro de los tiempos acordados de los SLAs y otros acuerdos
- Registrar todas las actividades ejecutadas relacionadas con los incidentes, que han sido reportados
- Proporcionar información al proceso de Administración de Problemas para tomar acciones y prever futuras recurrencias.

3. Definiciones

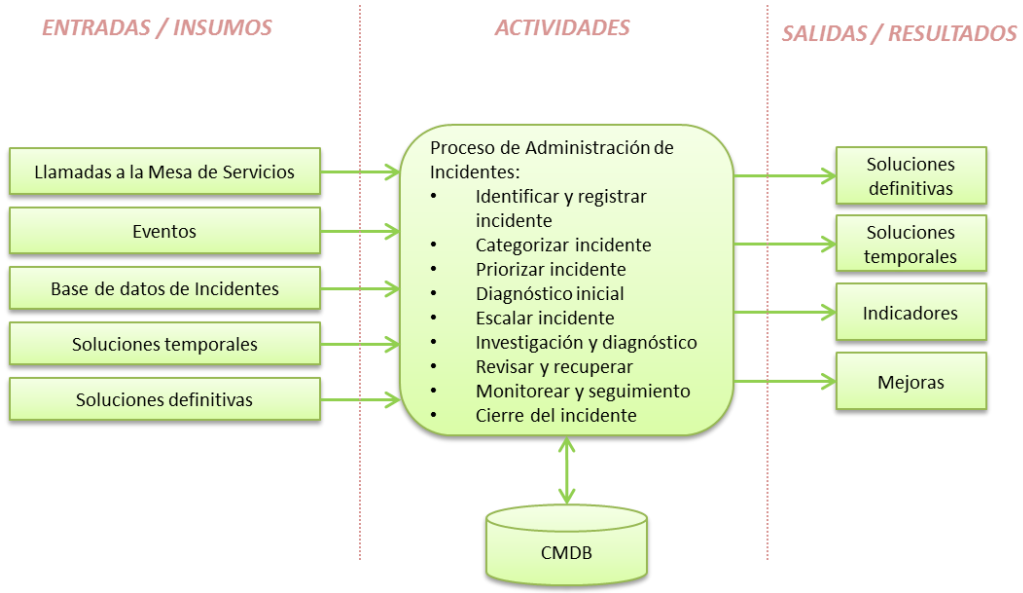
Estas definiciones están propuestas como parte del glosario utilizado dentro de la Administración de Incidentes, sin embargo la organización deberá evaluar su uso, considerar aquellas que les sean aplicables y agregar las que sean necesarias en el desarrollo del proceso.

- **CI:** Por sus siglas en inglés Configuration Item (Elemento de Configuración). Es el componente de una infraestructura que está o estará bajo el control de la Administración de Configuraciones. Pueden variar en complejidad, tamaño y tipo desde un sistema entero hasta un módulo o un componente menor de hardware, software y documentación.
- **CMDB:** Por sus siglas en inglés Configuration Management Data Base (Base de Datos de Administración de Configuraciones). Base de Datos usada para almacenar los Registros de Configuración durante todo su Ciclo de Vida. El Sistema de Administración de Configuración (CMS) mantiene una o más CMDBs, y cada una de estas bases almacena atributos de los Elementos de Configuración y Relaciones con otros CIs.
- **CMS:** Por sus siglas en inglés Configuration Management System (Sistema de Administración de Configuraciones). Conjunto de herramientas y bases de datos que se usan para gestionar los datos de Configuración de un Proveedor de Servicios de TI. La CMS también incluye información sobre Incidentes, Problemas, Errores conocidos, Cambios y Ediciones; y puede contener datos sobre los empleados, Suministradores, ubicaciones, Unidades de Negocios, Clientes y Usuarios. La CMS cuenta con herramientas para recopilar, almacenar, gestionar, actualizar y presentar datos sobre todos los Elementos de Configuración y sus Relaciones. El CMS es mantenido por la Administración de Configuraciones y es usado por todos los Procesos de Administración del Servicio de TI.
- **Escalamiento funcional:** Escalamiento de tipo horizontal, el cual se refiere esencialmente a la acción de dirigir y asignar los incidentes.
- **Escalamiento jerárquico:** Escalamiento de tipo vertical, el cual se refiere a la necesidad de encontrar mayor autoridad, poder y/o recursos. Usualmente se lleva a cabo bajo el escenario de circunstancias como incidentes mayores y/o probable incumplimiento de tiempos acordados.
- **Administración de Incidentes:** Se ocupa de la restauración del servicio lo antes posible una vez que este se interrumpió y trata únicamente la restauración del servicio, no la determinación y sus causas.
- **Impacto**: Es el nivel hasta donde se interrumpe la provisión de los servicios dentro de la organización, puede indicarse a través del número de CIs afectados y/o la cantidad de interrupciones de los procesos clave del negocio; se basa en la escala del daño potencial a los clientes del negocio.
- **Incidente:** Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción en la calidad del mismo.

- **Incidente Mayor:** Es aquel donde el grado de impacto al usuario es extremo, o bien la suma de incidentes menores, dado el porcentaje de usuarios afectados o el tiempo de interrupción del servicio lo convierten en incidente mayor.
- **ISO/IEC 20000:2011:** Norma internacional para la gestión de servicios de TI y promueve la adopción de un enfoque de proceso integrado para la entrega de los servicios administrados. La norma está alineada y es totalmente compatible con el esquema ITIL.
- **ITIL/Information Techonology Infraestructure Library:** Biblioteca de Infraestructura de Tecnologías de Información, la cual establece un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información.
- **KPI/ Key Preformance Indicator/Indicador** Clave de Desempeño: Son indicadores que se establecen para medir el comportamiento del proceso y asegurar que se cumplan los factores críticos de éxito.
- **Mejora:** Tomar las acciones necesarias para lograr un progreso continuo en el desempeño de los procesos.
- **OLA:** Por sus siglas en inglés Operational Level Agreement (Acuerdo de Nivel Operacional). Acuerdo entre un Proveedor de Servicios de TI y otra parte de una misma Organización. Un OLA da soporte a la prestación por parte del Proveedor de Servicios de TI de los Servicios de TI a los Clientes. El OLA define los bienes o los Servicios que serán prestados y las responsabilidades de ambas partes.
- **Prioridad:** Preferencia que se le debe dar a un incidente que se tiene que resolver, basándose en el impacto sobre la organización y en la urgencia.
- **Resolutor:** Persona especialista, responsable de atender un incidente.
- **RFC:** Por sus siglas en inglés Request For Change (Solicitud de Cambio). Propuesta formal para que se realice un Cambio. Un RFC incluye detalles del Cambio propuesto, y puede ser registrada en papel o en soporte electrónico.
- **SLA:** Por sus siglas en inglés Service Level Requeriment (Acuerdo de Nivel de Servicio). Acuerdo entre un Proveedor de Servicios de TI y un Cliente. El SLA describe el Servicio de TI, documenta las Metas de Niveles de Servicio y especifica las responsabilidades del Proveedor de Servicios de TI y del Cliente.
- **TI:** Por sus siglas en inglés Information Technology (Tecnología de la Información).
- **Ticket:** Solicitud de soporte con un número identificador, que se abre cuando el cliente reporta un incidente o realiza una solicitud de servicio a través de la Mesa de Ayuda, el cual es asignado a un resolutor (responsable) para su atención.
- **Urgencia:** Velocidad con la que se tiene que resolver el incidente, esta basa en el tipo de incidente, grado de afectación y cliente impactado.

4. Insumos

La siguiente imagen muestra el resumen del proceso de Administración de Incidentes, definiendo con detalle las entradas y salidas del mismo.



La definición de las entradas o insumos del proceso son:

- **Llamadas a la Mesa de Servicio**: llamadas telefónicas realizadas por los usuarios reportando el incidente detectado, que será registrado por la mesa de servicio (o el área que designe la organización), para su diagnóstico y solución.
- **Eventos**: A partir del monitoreo de la infraestructura de los servicios, las lecturas destacadas de dicho monitoreo serán lanzadas para su registro y atención.
- **Base de datos de incidentes**: Serie de incidentes registrados en la base de datos de la herramienta de Administración de Incidentes, que serán utilizados como apoyo para la solución de incidentes nuevos, ya que pueden existir incidentes similares resueltos, donde la solución puede ser utilizada para resolver los nuevos incidentes. En caso de no contar con herramienta automatizada, se deberá implementar en papel u otro software el control necesario.
- **Soluciones temporales**: Atención de un Incidente para el cual no hay disponible aún una solución definitiva. Las soluciones se documentan en los Registros de Incidentes, si se cuenta con una herramienta automatizada, se registra en la Administración de Incidentes y Administración de Problemas respectivamente.
- **Solución definitiva**: Eliminación total de un Incidente o Problema al identificar su causa raíz. Las soluciones para los Problemas se documentan en los Registros de Errores Conocidos y las soluciones para Incidentes que no tienen asociados Registros de Problemas se documentan en los Registros de Incidentes en la herramienta de Administración de Incidentes y Administración de Problemas respectivamente.

5. Resultados

Las salidas o resultados del proceso de Administración de Incidentes son las siguientes:

Las principales salidas del proceso son las **Soluciones Definitivas y Temporales**, ya que dan respuesta a uno o varios Incidentes reportados a través de la Mesa de Servicio, sin embargo el proceso también tendrá como salidas:

- **Indicadores y reportes** generados del proceso
- **Mejoras del proceso**, que deberán incluir acciones preventivas y correctivas

6. Interacción con otros procesos

El siguiente diagrama muestra las principales relaciones del proceso de Administración de Incidentes con otros procesos de la Administración de Servicios ISO 20000, considerando este diagrama como el escenario ideal.

Relación con:	Información que entrega a Administración de Incidentes	Información que recibe de Administración de Incidentes
Mesa de Servicios	Registro de incidente a partir de llamadas telefónicas	N/A
Administración de Eventos	Lectura del monitoreo que debe manejarse como incidente.	N/A
Administración de Problemas	Base de datos de errores conocidos, donde se almacenan las soluciones temporales y definitivas de problemas e incidentes relacionados.	Registro de incidentes, para contar con el detalle de las fallas o degradación de desempeño de los servicios.
Administración de Configuraciones	Información de los CIs, que están relacionados con el incidente.	N/A
Administración de Cambios	Una vez aplicada la solución del incidente, la cual fue coordinada por Administración de Cambios, éste le notifica a Administración de Incidentes, que ha sido aplicada la solución.	Registro de RFC que levanta la Administración de Incidentes, para que se apliqué una solución de un incidente.
Cumplimiento de Requerimientos	N/A	Registro que viene de la mesa de servicios, pero al momento de clasificar sea requerido atenderse como requerimiento y no como incidente.
Administración de Niveles de Servicios	SLAs que incluyen los tiempos que debe cumplir Administración de Incidentes.	Métricas de cumplimiento de los objetivos estipulados con los SLAs.

7. Políticas

Las políticas se definen para normar el proceso de la Administración de Incidentes. Éstas están basadas en las necesidades de la organización y las mejores prácticas, quedando a validación y mejora permanente por parte del dueño y administrador del proceso.

- El proceso de Administración de Incidentes es revisado cada seis meses para realizar la mejora continua del mismo.
- La integridad y verificación de la información de Incidentes será revisada mensualmente por el Administrador de Incidentes.
- Todos los incidentes deben ser reportados lo más pronto posible para llevar a cabo las acciones de análisis y diagnóstico para su solución.
- Los medios válidos y autorizados para reportar los incidentes son:
    - Vía telefónica
    - Oficio
- Todo incidente debe ser registrado y documentado hasta que concluya su atención.
- Se califica la urgencia basada en el usuario que solicita el servicio, nivel jerárquico que ocupa, tiempo en que es detectado el incidente, servicio que está siendo afectado, y tiempo máximo acordado en el SLA; el cual es calificado como alto, medio o bajo.
- El resolutor deberá consultar los Incidentes que le fueron turnados y darles atención conforme a los SLAs acordados.
- El incidente no se podrá cerrar a menos que se haya reestablecido el servicio, con la validación del cliente.
- Todo incidente mayor será atendido de manera inmediata bajo la responsabilidad del Administrador de Incidentes.
- Se considera un incidente mayor cuando el impacto y/o urgencia se califica de manera automática como alto.
- Un Incidente será cancelado cuando el usuario no sea localizado en tres ocasiones, durante un periodo de 24 horas. De requerir el servicio el usuario, deberá generar una nueva solicitud.
- Cuando participe un proveedor en la solución de los incidentes, las actividades desarrolladas por este deberán ser documentadas por el resolutor que tenga a su cargo el Incidente.
- Todos los involucrados en el proceso de Administración de Incidentes ser deben apegar a los tiempos y prioridad para la escalación de los Incidentes.

8. Responsabilidades

En este apartado se proponen la siguientes figuras/roles, sin embargo estas serán definidas por la propia organización de acuerdo a sus necesidades.

Administrador de Incidentes, funciones:

- Comunicar y difundir el proceso dentro de la organización
- Planea la estrategia de implantación y mejora continua de la Administración de Incidentes
- Implementa y mantiene el proceso de incidentes (incluyendo documentación)
- Monitorea las métricas del proceso de Administración de Incidentes para su mejora continua
- Toma decisiones sobre el proceso de Administración de Incidentes cuando interactúa con otros procesos
- Asigna actividades a los Especialistas
- Coordinar la definición y planeación del Punto Único de Contacto
- Vigilar el cumplimiento de los acuerdos de niveles de servicio (SLAs)y Acuerdos de Nivel Operativo (OLAs) relacionados
- Vigilar que la asignación de los tickets de servicio sea de acuerdo a las políticas
- Vigilar que los requerimientos de los usuarios sean atendidos de acuerdo a los niveles de servicio
- Vigilar la atención de los usuarios y su satisfacción para proporcionar una buena imagen
- Generar reportes gerenciales del comportamiento del proceso que van a servir para la mejora continua

1er Nivel de Soporte (Especialista de Mesa de Servicio), funciones:

- Recibir las llamadas de servicio de acuerdo al protocolo de atención telefónica
- Registrar las llamadas de servicio en papel o herramienta automatizada asignando número de ticket
- Resolver las llamadas de servicio que están dentro de su competencia
- Asignar resolutor para atención de incidente
- Realizar seguimiento en los incidentes registrados
- Validar con el usuario que el incidente fue atendido
- Mantener una comunicación abierta con el Administrador de Proceso de Incidentes
- Cerrar tickets de registro de incidentes

El **2º y 3er Nivel de Soporte**, funciones:

- Atender los requerimientos de incidentes de servicio
- Investigar y diagnosticar los incidentes
- Evaluar y atender los requerimientos de servicio e incidente

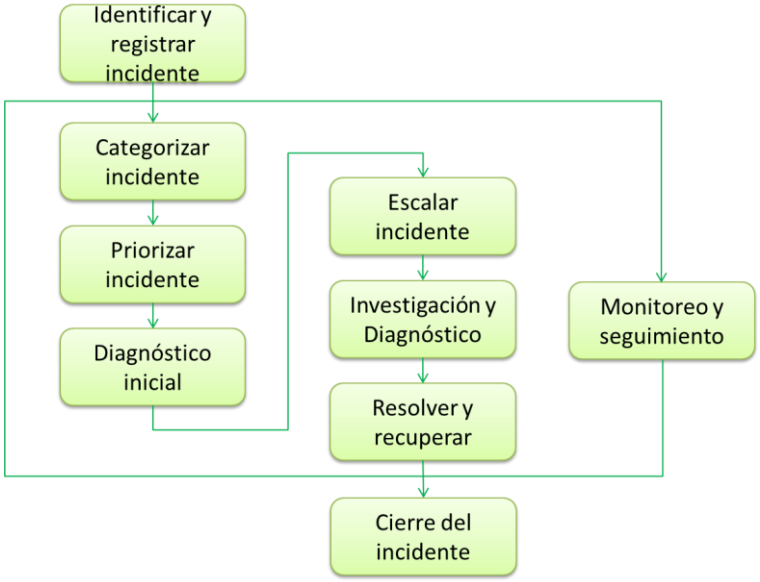
- Solicitar requerimientos de cambio cuando es necesario
- Escalar al proveedor y comunicar los Incidentes que no pueden ser resueltos.
- Restaurar los servicios afectados
- Probar las soluciones
- Mantener una comunicación abierta con el Administrador de Mesa de Servicio (se cuenta con él) y el Administrador del Proceso de Incidentes
- Documentar las soluciones de los incidentes atendidos.

El **Usuario (puede ser un especialista técnico)**, quien es el solicitante al levantar el Incidente, funciones:

- Detectar los incidentes de la infraestructura que utiliza para sus actividades de su día a día
- Llamar para reportar los incidentes detectados
- Proporcionar la información que le requiera el Especialista, para el registro y atención del Incidente

9. Método de Trabajo

El siguiente diagrama ilustra las macro actividades del proceso de Administración de Incidentes:



Identificar y registrar incidente	El usuario reporta el incidente, el Agente de 1er Nivel de Soporte recibe registro del incidente, solicita datos generales del Servidor Público y registra la descripción a detalle del incidente.
Categorizar incidente	El Agente del 1er. Nivel de Soporte selecciona la clasificación del tipo de incidente que está siendo registrado, para que en el futuro pueda agruparse con otros incidentes similares y proporcionar información a otros procesos, tal como Administración de Problemas.
Priorizar incidente.	El Agente del 1er. Nivel de Soporte realiza una evaluación del impacto y la urgencia del incidente para definir la prioridad y dar soporte inicial.
Diagnóstico inicial	El 1er. Nivel de Soporte revisa los registros de incidentes similares, la base de datos de errores conocidos y/o la base de datos de conocimiento, para proporcionar una solución al incidente. Si no puede proporcionar una solución, entonces deberá realizar una escalación a los grupos de soporte especializados.
Escalar incidente	El 1er Nivel de Soporte recurrirá al 2º o 3er. Nivel de Soporte, para diagnosticar e investigar el incidente y proporcionar una solución.
Investigación y diagnóstico	El especialista de 2º o 3er. Nivel de Soporte evalúa los detalles del incidente, recolecta y analiza la información relacionada con el

	incidente, con el propósito de encontrar una solución permanente y si no es posible, encontrar una solución temporal. Se comunica vía telefónica o correo electrónico con el usuario, e informa si existe la posibilidad de contar con los medios para continuar con sus actividades, aunque exista una degradación en el servicio, es decir que no esté operando al 100%.
Resolver y recuperar	Las acciones a realizar son establecidas dependiendo del incidente reportado y de los recursos disponibles para poder atenderlo y dar solución, la cual es registrada. De ser necesario, se realizan pruebas de restauración del servicio.
Cierre del incidente	Una vez que el incidente ha sido resuelto y se ha documentado el seguimiento se realiza el cierre del incidente y se confirma con los usuarios la solución satisfactoria del mismo, verificando si el servicio ha sido evaluado, de lo contrario solicita al usuario su evaluación. Una vez concluido este paso, el incidente es cerrado.
Monitoreo y seguimiento	Durante la vida del incidente, se mantiene la posesión del mismo, aun cuando otros grupos de soporte hayan sido involucrados. Deberá contarse con un responsable del monitoreo y seguimiento del estado del incidente, vigilando el cumplimiento con los objetivos de Niveles de Servicio; así mismo dará seguimiento a las escalaciones verificando que se realicen apropiadamente.

10. Matriz RACI

Una tarea muy importante es realizar un mapeo de los roles y las responsabilidades las cuales recaen en sus funciones, así como su intervención en cada una de las actividades del proceso, para conocer quién toma parte en cada actividad y con qué nivel de participación. Este mapeo se lleva a cabo con una matriz llamada RACI, donde cada letra que forma su nombre es el nivel de responsabilidad específico en la actividad.

A continuación se muestra la nomenclatura a utilizar dentro de la tabla RACI definida para el proceso de Administración de Incidentes.

	RESPONSABILIDAD	DESCRIPCIÓN
R	Responsible	Responsable de ejecutar la actividad.
A	Accountable	Encargado del verificar el cumplimiento y la calidad en la ejecución de la actividad.
C	Consulted	Aporta conocimiento y/o información para que el responsable ejecute la actividad.
I	Informed	Rol que debe ser informado una vez que la actividad ha finalizado.

A continuación se muestra la tabla RACI definida para el proceso y está conformada por los siguientes rubros:

- **No:** Número correspondiente a la secuencia de actividades del diagrama de flujo del proceso de Administración de Incidentes.
- **Actividad:** Nombre de la actividad del diagrama de flujo del proceso de Administración de Incidentes que se haya establecido en la organización.
- **Roles:** Nombre de los roles participantes en el proceso de Administración de Incidentes.

La siguiente tabla contempla las figuras propuestas en el presente proceso, a manera de guía.

No.	Actividad	Administrador de Incidentes	1er. Nivel de Soporte/Especialista Mesa de Servicios	2º y 3er Nivel de Soporte	Usuario/Especialista Técnico
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

11. Medición

Los indicadores tienen como objetivo proveer datos estadísticos sobre el comportamiento del proceso o calidad del servicio/producto generado por la Administración de Catálogo de Servicios; a través de dichas mediciones se busca la optimización y mejora continua del proceso.

A continuación se muestra una tabla (como propuesta de uso) que deberá contener los indicadores definidos, los cuales deberán reflejar los rubros de medición de información importante para la organización y para el proceso. Dicha tabla está conformada por los siguientes rubros:

- **Código:** Identificador asignado al indicador, para hacer referencia a este en reportes.
- **Indicador:** Nombre de la métrica
- **Descripción:** Propósito del indicador
- **Fórmula:** Ecuación o regla que relaciona objetos matemáticos o cantidades.
- **Unidad:** Unidad de medición que se obtiene al generar el indicador
- **Frecuencia:** Lapso de tiempo específico para generar el indicador (mensual, bimestral, etc.)
- **Responsable:** Rol responsable de generar el indicador

Código	Indicador	Descripción	Fórmula	Unidad	Frecuencia	Responsable