Contenido

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

1.INTRODUCCIÓN

Una respuesta inmediata a los incidentes que podrían poner en riesgo la seguridad, integridad, confidencialidad y disponibilidad de los datos, activos, programas, redes y demás recursos de tecnología de información es indispensable para garantizar la operación continua de la Entidad. Sin una política y procedimiento para resolver incidentes, los recursos de tecnologías de información podrían estar comprometidos, violando políticas, estatutos o la confianza otorgada por los miembros de la entidad.

2.OBJETIVO DE LA POLITICA

La gestión de incidentes es un área de procesos perteneciente a la Gestión de Servicio TI. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual del funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la Entidad de forma que la calidad del servicio y la disponibilidad se mantengan**.**

3.ALCANCE

El presente proceso de gestión de incidentes aplica para toda la gestión de incidentes de servicio sobre la infraestructura de tecnologías de información.

4.Responsables:

- Jefe de Oficina de Informática y Sistemas – Funcionario
- Funcionarios de soporte técnico
- Contratistas de apoyo de soporte técnico
- Proveedor de servicios de soporte técnico

5.DEFINICIONES

Incidencia: Conocido como interrupción de los servicios TI, puede coincidir con un “Problema conocido” (fallo sin un origen conocido) o con un “Error conocido” (fallo con origen conocido) bajo el control de la gestión de problemas y registrado en el sistema de soporte técnico. Estas incidencias pueden ser reportadas:

- Comunicada por el usuario
- Generada automáticamente por aplicaciones

Servicio de ayuda (Service Desk): Responsable directo de la gestión de las incidencias

- Administrador Centro de Computo de la Entidad TI
- Primera línea de incidentes

Elementos TIC: Elementos de hardware o software que pertenecen a la Tecnología de la Informática y Comunicaciones.

TIC: Tecnología de Informática y Comunicaciones.

Registro y Clasificación: Creación de un registro de incidente

- Prioridad, impacto, urgencia.
- Categorización: Asignación de tipo y personal de soporte

Resuelto?:
Si se conoce el método de solución:

- Se asigna los recursos necesarios

Si NO se conoce el método de solución:

- Se escala la incidencia a un nivel superior de Soporte.

Escalamiento: Traspaso de un caso para ser atendido por un grupo de atención (proveedor) con mayores privilegios, conocimientos y posibilidades de dar solución a un incidente que no pudo ser resuelto en un grupo de atención dado (funcionario o contratista de apoyo). Existen dos tipos de escalamiento en el proceso de solución de una incidencia.

- Escalado funcional: se recurre a técnicos responsables y/o expertos en el tema.
- Escalado Proveedor: entran en juego los proveedores de servicios de soporte técnico de TI que tenga contratado en el momento la Entidad.

Resolución y Cierre: Cuando se ha resuelto el incidente satisfactoriamente.
Registro del proceso en el sistema de soporte técnico.

Monitorización y Seguimiento: El proceso debe ser controlado mediante:

- Revisión de los incidentes en el sistema de soporte técnico.
- Indicador del servicio de soporte

Interrelaciones: Debe existir una estrecha relación entre la gestión de incidentes y otros procesos TI con el objetivo:

- Mejorar el servicio y cumplir adecuadamente los Acuerdos de Niveles de Servicios
- Conocer la capacidad y disponibilidad de la infraestructura TI
- Planificar y realizar los cambios necesarios para la optimización y desarrollo del servicio TI

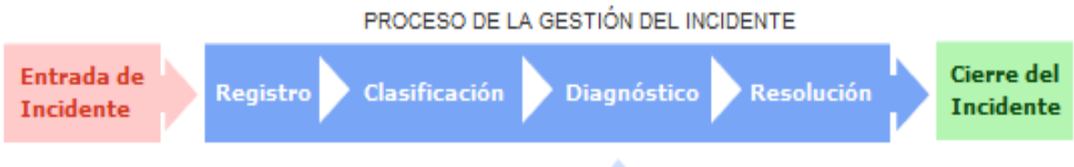
Los objetivos principales de la Gestión de Incidentes son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en los Acuerdos de Niveles de Servicio correspondiente.

Horas de Servicio: Periodo de tiempo acordado durante el que un determinado servicio de TI debe estar disponible.

Horas de Soporte: Tiempo u horas cuando el soporte debe estar disponible para los usuarios.

6.PROCESO DE GESTION DE INCIDENTES



6.1Clasificación

La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser de utilizada para la resolución del mismo.

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

6.1.1Categorización: Se asigna una categoría dependiendo del tipo de incidente o del técnico responsable de su resolución. Se identifican los servicios afectados por el incidente.

6.1.2 Establecimiento del nivel de prioridad: Dependiendo del impacto y la urgencia se determina, según criterios preestablecidos, un nivel de prioridad.

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

6.1.3 Asignación de recursos: El funcionario o contratista responsable del servicio de soporte técnico si no puede resolver el incidente en primera instancia designará al personal de soporte técnico responsable de su resolución (segundo nivel).

6.1.4 Monitorización del estado: Se asocia un estado al incidente que puede ser: abierto, vencido y cerrado y el nivel de prioridad. El tiempo para su solución está dato de acuerdo con el impacto, como se observa en la gráfica de Impacto y Urgencia de una Incidencia Técnica y su cuadro adjunto.

6.1.5Clasificación del Incidente: Es natural y frecuente que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas.

6.1.6 Nivel de Prioridad: El nivel de prioridad se basa esencialmente en dos parámetros:

7.Impacto: Determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados. Esto determina el nivel de atención de las solicitudes de soporte técnico con las siguientes especificaciones:

- **Urgente y Alto (Crítico):** Se define inhabilítate en la totalidad o en una parte de la funcionalidad del servicio TI.
- **Normal (Media):** Se define como aquel fallo que permite el funcionamiento del servicio TI o de parte de él, pero limita su buen uso.
- **Bajo (No Critico):** Se define como aquel fallo leve del servicio y que no afecta su uso.

Urgencia: Depende del tiempo máximo de respuesta que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en el Acuerdo de Nivel de Servicio correspondiente.

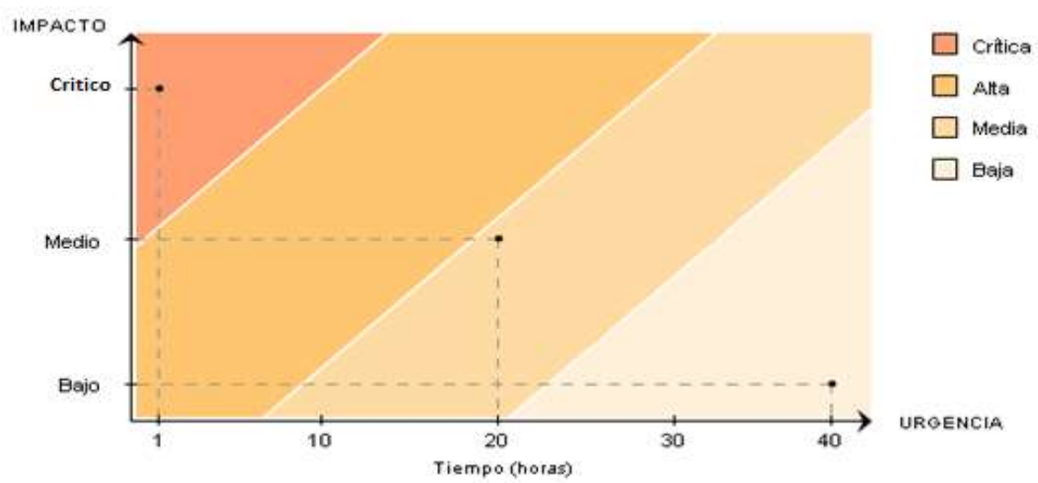
También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes “sencillos” se tramitarán cuanto antes.

Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente.

La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente. El siguiente diagrama nos muestra un “diagrama de prioridades” en función de la urgencia e impacto del incidente:

Grafica de Impacto y Urgencia de una Incidencia Técnica



Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

Nivel	Categoría	Tiempo de Respuesta	Tipo de Acción
1	Critico (Urgente o Alta)	Inmediata	Continuidad hasta su resolución dentro del mismo día.
2	Media (Normal)	Hasta dos días (20 horas)	Resolución dentro del horario regular de servicio.
3	Bajo (No critica)	Hasta cuatro días (40 horas)	Resolución dentro del horario regular de servicio.

- **Nivel 1.** Se denomina Nivel 1 cuando el sistema presenta bloqueo o caída total crítica, si se cuenta con proveedor éste debe atender el requerimiento personalmente en las instalaciones de la Entidad en horario 7x8, en un tiempo no mayor a tres (3) horas; si no se cuenta con proveedor se debe atender el requerimiento por el recurso humano de la Oficina de Informática y Sistemas (funcionario o contratista) en las instalaciones de la Entidad en horario 7x8, en un tiempo no mayor a tres (3) horas.
- **Nivel 2.** Se denomina Nivel 2 cuando el sistema presenta fallas parciales que no afectan el funcionamiento total del sistema, si se cuenta con proveedor éste debe atender el requerimiento personalmente o vía telefónica en un tiempo no mayor a setenta y dos (72) horas; si no se cuenta con proveedor se debe atender el requerimiento por el recurso humano de la Oficina de Informática y Sistemas (funcionario o contratista de apoyo) personalmente en un tiempo no mayor a setenta y dos (72) horas.
- **Nivel 3.** Se denomina Nivel 3 cuando el sistema presenta fallas leves del servicio. El impacto es un inconveniente que puede requerir una solución alternativa para restablecer la funcionalidad, si se cuenta con proveedor éste debe atender el requerimiento personalmente o vía telefónica en un tiempo no mayor a veinticuatro (24) horas; si no se cuenta con proveedor se debe atender el requerimiento por el recurso humano de la Oficina de Informática y Sistemas (funcionario o contratista de apoyo) personalmente en un tiempo no mayor a veinticuatro (24) horas.

Los incidentes deben clasificarse a medida que son reportados. Algunos ejemplos de incidentes según su clasificación son los siguientes:

Incidente a nivel de Aplicaciones

- Servicio no disponible
- Fallo de la aplicación
- Capacidad del disco duro excedida

Incidente a nivel de Hardware

- Caída del sistema
- Alerta automática
- Impresión

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co