CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Yeison Latorre Ruiz Cargo: Coordinador Grupo de Trabajo de Servicios Tecnológicos	Nombre: Francisco Rodríguez Eraso Cargo: Jefe de la Oficina de Tecnología e Informática	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2020 –12- 03

1 OBJETIVO

Establecer los lineamientos, para restaurar el normal funcionamiento de los servicios tecnológicos, definiendo las etapas requeridas en la implementación de una solución temporal o definitiva a cualquier incidente que produzca una interrupción o degradación de los servicios de TI, minimizando algún impacto negativo para la Superintendencia de Industria y Comercio.

2 DESTINATARIOS

Este documento aplica a todos aquellos funcionarios o contratistas de la Superintendencia de Industria y Comercio, en adelante SIC, que participen directa o indirectamente en la gestión de incidentes de tecnología que ingresan al Centro de Servicios Integrados de Tecnología.

3 GLOSARIO

ANALISTA DE MONITOREO: persona que en forma proactiva identifica alarmas que afecten la infraestructura informática.

ANALISTA DEL CENTRO DE SERVICIOS INTEGRADOS DE TECNOLOGÍA: persona encarga de registrar, canalizar, categorizar y solucionar los incidentes de servicio de primer nivel, o en su defecto, escalar a los equipos de soporte para dar la solución final.

ANALISTA SEGUNDO NIVEL: persona encargada de dar solución en sitio a los incidentes que surjan de la infraestructura tecnológica.

ANALISTA TERCER NIVEL: especialista OTI y/o Outsourcing, rol encargado de dar solución a los servicios tecnológicos que tengan que ver con su competencia.

BASE DE DATOS DE ERRORES CONOCIDOS (KEDB – Known Error Database): base de datos que contiene los registros de errores conocidos, presentados en los incidentes y entregados a la gestión de problemas como referencias futuras.

CATEGORIZACIÓN: es el listado de los servicios establecidos que se configuran en la herramienta de gestión, una vez ingresa un caso al centro de servicios integrados de tecnología, asigna una categoría dependiendo del tipo de incidente y del grupo de trabajo responsable de su resolución.

CSIT: Centro Integrado de Servicios de Tecnología.

ERROR CONOCIDO: problema que tiene una causa raíz documentada y una solución temporal.

EVENTO: alarma que impacta o puede impactar un servicio de tecnología.

GESTIÓN DE CAMBIO: procedimiento responsable de controlar el ciclo de vida de todas las solicitudes de cambios desde su registro hasta el cierre, evaluando impactos, minimizando la interrupción de servicios de TI.

GESTIÓN DE CONOCIMIENTO: es el proceso por el cual se facilita la trasmisión de conocimiento al usuario de manera sistemática y eficiente.

GESTIÓN DE PROBLEMAS: es la prevención de Incidentes y la minimización del impacto de aquellos Incidentes que no pueden prevenirse.

INCIDENTE: evento que no forma parte de la operación normal de un servicio y que causa, o puede causar, una interrupción o una reducción de la calidad de dicho servicio.

INCIDENTE MASIVO: falla en el servicio que causa alto impacto en la operación, afectando directamente la infraestructura de TI, y debe ser atendido con mayor grado de urgencia que un incidente normal. El tratamiento de este tipo de incidentes requiere un procedimiento separado con tiempos más cortos.

MATRIZ DE CATEGORÍAS CSIT: Listado de servicios tecnológicos ofrecidos por la OTI, bajo la cual se categorizan los servicios en la Herramienta de Gestión, es de uso exclusivo del CSIT.

RFC: formato requerido para cualquier solicitud de cambio, debe contener toda la información de las actividades, responsables, fechas y horarios que se llevarán a cabo para la ejecución del cambio.

TICKET, CASO o SOLICITUD: número consecutivo suministrado por la herramienta de gestión durante el reporte de un incidente, con el fin de facilitar seguimiento y control.

SOLICITANTE: persona o área de la SIC que reporta una falla, intermitencia o degradación en uno o más servicios tecnológicos a los que accede.

SOLICITUD: es una declaración formal de lo que se necesita, es también llamada Requerimiento.

4 REFERENCIAS NORMATIVAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
Decreto Nacional	1008 del 14 de junio de 2018	Política de Gobierno Digital	Artículo 2.2.9.1.1.1 al 2.2.9.1.4.2	Aplicación total

5 GENERALIDADES

La gestión de incidentes es responsable de restaurar el normal funcionamiento de los servicios tecnológicos, generando interacción con otros procedimientos para identificar y atender oportunamente los servicios, minimizando el impacto negativo a los usuarios y asegurando que el procedimiento sea aplicado por las partes involucradas, generando la entrega de servicios tecnológicos operativos y confiables cumpliendo con las expectativas y especificaciones requeridas por la SIC.

La gestión de incidentes es responsable de restaurar el normal funcionamiento de los servicios tecnológicos, generando interacción con otros procedimientos para identificar y atender oportunamente los servicios, minimizando el impacto negativo hacia los usuarios y asegurando que el procedimiento sea aplicado por las partes involucradas, generando la entrega de servicios tecnológicos operativos y confiables cumpliendo con las expectativas y especificaciones requeridas por la SIC.

Nota 1: Los roles y responsabilidades se encuentran detallados en el Anexo 2 “Roles y Responsabilidades - Gestión de Incidentes TI.”

5.1 ALCANCE

Inicia con la revisión del incidente registrado en la herramienta de gestión de servicios, implementando una solución temporal o definitiva y termina con su posible postulación y actualización dentro de la base de datos de conocimientos para referencias futuras.

5.2 POLÍTICAS DE LA GESTIÓN DE INCIDENTES DE TECNOLOGÍA.

5.2.1 Identificar al Centro de Servicios Integrados de Tecnología - CSIT, como único punto de contacto para el registro de los incidentes, aplicando el esquema de categorización de prioridad, urgencia e impacto, los cuales se pueden realizar a través de los siguientes medios de comunicación:

- Correo electrónico: mesadeservicios@sic.gov.co
- Extensión: 10502
- Autoservicio: Intrasic – Aranda-sic/usdkv8

5.2.2 Se declarará un incidente masivo a partir de diez (10) o más casos reportados sobre una misma falla, o la afectación general sobre un servicio; comunicar la afectación al interior de las áreas de la SIC, descritas en este procedimiento.

5.2.3 Si un Incidente es catalogado como masivo, su apertura, seguimiento y cierre debe ser notificado al siguiente personal:

- Jefe de la Oficina de Tecnología e Informática - OTI.
- Profesional OTI que apoya la supervisión de la gestión de incidentes.
- Profesional OTI que apoya la supervisión del servicio asociado a la falla.
- Profesional de la OTI que apoya la supervisión de la mesa de servicios.
- Líder de Servicio y Técnico del Proveedor de TI.
- Líder Mesa de Servicio y Soporte en Sitio del Proveedor de TI.
- Especialista del Proveedor de servicios de TI.
- Personal de TI que se encuentre involucrado en el servicio afectado.

5.2.4 La postulación de un Incidente masivo o estándar a problema se realizará a través del procedimiento de gestión de problemas cuando:

- Exista uno o más incidentes de los cuales se desconozca su causa raíz.
- Se haya otorgado una solución temporal.
- Al no tener resolución del incidente en un lapso de 2 días hábiles.
- Cuando se haya otorgado solución definitiva, y se presente recurrencia del incidente.

5.2.5 Para la solución del incidente masivo, el resolutor debe realizar un informe de cierre con las actividades aplicadas (causa raíz, solución), el cual será adjuntado a la documentación de la herramienta de gestión. Este documento será postulado a gestión de problemas y gestión de la base del conocimiento tecnológico, para su posible creación de ID de error conocido y documentación de la base de conocimiento.

5.2.6 Los incidentes que dan origen a cambios en los ítems de configuración del servicio de tecnología deben atenderse por medio de un RFC (solicitud de cambio) del procedimiento |de control de cambios DE04-P04.

5.2.7 La suspensión de los casos se debe realizar de acuerdo con el anexo 1 – Manejo de casos suspendidos.

5.2.8 Los Incidentes de Seguridad de la Información serán gestionados mediante el ***Procedimiento de gestión de incidentes de seguridad de la información SC05-P01***, publicado en el Sistema Integrado de Gestión Institucional – SIGI[1]

[1] https://sigi.sic.gov.co/SIGI/scriptsportal/mapa_procesos/document_tab.php?id_doc=1129&version=2&back=1

5.2.9 Todos los incidentes relacionados con seguridad de la información deberán ser informados al correo seguridaddigital@sic.gov.co del grupo de trabajo de informática forense y seguridad digital, con la periodicidad que el coordinador del grupo estipule.

5.3 COMUNICACIÓN DE INCIDENTES MASIVOS.

La Oficina de Tecnología e Informática – OTI, aplicará los siguientes niveles de escalamiento para comunicar a las diferentes áreas de la Superintendencia de Industria y Comercio las posibles afectaciones masivas que se puedan presentar sobre la infraestructura tecnológica, con el objetivo que los diferentes grupos: atención al ciudadano, contratistas y funcionarios, mantenga informada a la ciudadanía y a las partes interesadas sobre la afectación presentada y puedan activar sus planes de contingencia.

NIVEL DE ESCALAMIENTO	TIEMPO DE ATENCIÓN	ACCIONES	ÁREAS A INFORMAR	OBJETIVO
Nivel 0	Tiempo: De 0 a 45 minutos de transcurrido el incidente.	El coordinador del grupo de trabajo de servicios tecnológicos o a quién se delegue, informará directamente y mediante comunicación telefónica, el resumen del incidente y el posible tiempo de atención. El apoyo a la actividad se realiza con mesa de servicios.	OSCAE, dirección administrativa, RNPC, y áreas de atención al ciudadano.	Que las áreas de atención al ciudadano sepan cómo actuar ante posible falla y exista una comunicación unificada hacia los terceros.
Nivel 1	Tiempo: De 45 minutos hasta 1 hora de transcurrido el incidente.	El coordinador del grupo de trabajo de servicios tecnológicos o a quién se delegue, enviará un correo electrónico con el resumen de la falla y el tiempo probable de solución, el cual depende de la validación técnica realizada con proveedores.	OSCAE, dirección administrativa, RNPC, y áreas de atención al ciudadano.	Que las áreas de atención al ciudadano sepan cómo actuar ante un posible problema de tecnología.
Nivel 2	Tiempo: De 1 hora hasta 2 horas de transcurrido el incidente.	El jefe de la oficina de tecnología e informática enviará comunicación escrita a los jefes y directivos de la entidad, con el resumen de la falla y tiempo probable de la solución, corroborado con el proveedor de servicios.	Nivel directivo de las áreas de atención inmediata y directa al ciudadano.	Prepararse para tomar acciones de contingencia en la operación de la SIC.

NIVEL DE ESCALAMIENTO	TIEMPO DE ATENCIÓN	ACCIONES	ÁREAS A INFORMAR	OBJETIVO
Nivel 3	Tiempo: De 2 horas en delante de transcurrido el problema.	Luego de 2 horas de detención de la operación, el incidente se convierte en problema y se efectúan las actividades del Procedimiento de Gestión de Problemas, el jefe de la OTI, enviará comunicación a nivel directivo de toda la entidad, informando la situación y posibles tiempos de atención al problema, y se comunica a secretaría general la activación de los planes de contingencia.	Nivel directivo de todas las áreas de la entidad, todas las áreas y comunicación al ciudadano.	Gestionar el plan de recuperación de desastres y/o plan de contingencia ante la operación, en el momento se incluyen las siguientes opciones: proyectar resolución de detención de vencimiento de términos, comunicación en la página web de la entidad, comunicación con proveedores alternos de operación.

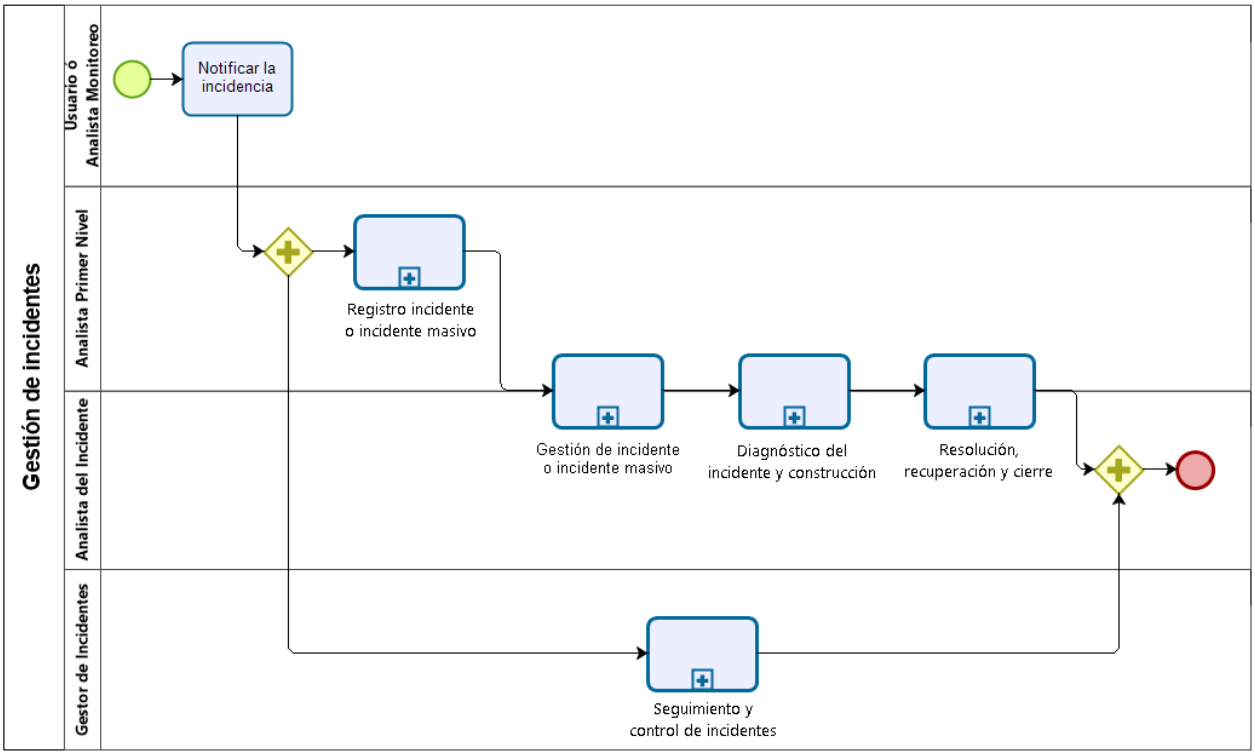
5.4 ESTADO DE UN INCIDENTE

- Registrado: Estado de un incidente al momento de ser creado y que genera el ID de identificación del incidente.
- En proceso: El responsable comienza con la atención del incidente.
- Anulado: Estado al cual se pasan los Incidentes que son registrados por error o el Incidente se encuentra duplicado.
- Solucionado: Ya se dio y se documentó una solución definitiva o temporal al incidente. Se inicia etapa de aseguramiento de la calidad, donde se valida la calidad de atención y solución del incidente con el usuario y se hace la revisión de la priorización, categorización y documentación de acuerdo con la solución documentada del incidente.
- Suspendido: Por una causa justificada no se puede avanzar en la solución, lo anterior bajo los criterios del documento Manejo de Suspendidos.
- Cerrado: El incidente pasa a este estado después de que ha finalizado el aseguramiento de calidad, lo anterior al ser calificada positivamente la encuesta o si en 3 días hábiles no es contestada, el sistema la cierra automáticamente. En caso de ser calificada negativamente la encuesta de satisfacción, el incidente se reabre y pasa a estado En Proceso para su atención y solución.

5.5 INTEGRACION CON OTRAS PRACTICAS DE GESTIÓN ITIL

- Mesa de Servicios: punto único de contacto con los usuarios para los servicios de TI contratados.
- Gestión de catálogo de servicios: Relación de los servicios y los tipos de incidentes.
- Gestión de niveles de servicios: Tiempos de atención y solución de los incidentes, esquema de priorización de incidentes, definición de reportes e informes de seguimiento de niveles de servicio.
- Gestión de activos del servicio y configuración: Relación entre los CI´s y los tipos de incidentes.
- Gestión de cambios: Cambios implementados para dar solución a incidentes, y asegurar que se pueda tener una trazabilidad con los posibles incidentes que puedan ocurrir posterior a la aplicación de un cambio.
- Gestión de solicitudes: Solicitudes que generan incidentes.
- Gestión de problemas: Soluciones temporales y definitivas para incidentes escalados como problemas.
- Gestión de eventos: Eventos de advertencia o críticos que se detecten durante el monitoreo del servicio pueden convertirse en incidentes que serán gestionados a través de este procedimiento.
- Gestión de accesos: Accesos no autorizados que generan incidentes.
- Gestión de disponibilidad: Asegurar el menor impacto en la disponibilidad de los servicios, por la presencia de incidentes en la operación de este.
- Gestión de la base del conocimiento tecnológico: Las soluciones de incidentes pueden ser postuladas a la gestión de la base del conocimiento tecnológico para ser parte de la KMDB y errores conocidos.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO



No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	**REGISTRAR INCIDENTE O INCIDENTE MASIVO**	Notificación de la afectación por parte del usuario o analista de monitoreo	Realizar el registro de los incidentes que sean notificados a través del único punto de contacto y por los canales de comunicación establecidos, y presenta las siguientes actividades: - Realizar la notificación a través de los canales de comunicación. - Identificar datos del usuario. - Realizar el registro y categorización. - Analizar información para dar solución en primer nivel. - Validar la existencia de otras notificaciones asociadas a la falla reportada en caso de presentarse masivo. - Clasificar y escalar si es necesario la intervención de atención en segundo o tercer nivel.	Analista de primer nivel	Registro del incidente en la herramienta de gestión

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
2	**GESTIONAR INCIDENTE O INCIDENTE MASIVO**	Incidente y/o masivo registrado y documentado en la herramienta de gestión	Identificar la falla o fallas presentadas en caso de afectación masiva, de ser así, realizar la notificación a las personas interesadas, presenta las siguientes actividades: - Notificar el registro de incidente o incidente masivo. - Reportar a las partes interesadas. - Entregar solución.	Dueño del servicio Dueño de proceso Gestor incidente Analistas; segundo, tercer nivel Proveedor	Notificación de incidente masivo, e inicio del diagnóstico de la afectación
3	**DIAGNOSTICAR EL INCIDENTE Y CONSTRUIR LA SOLUCIÓN**	Tipificación y categorización del incidente. Base de conocimiento.	Identificar tipo de incidente (seguridad), y grupo resolutor a diagnosticar y proponer solución, realiza las siguientes actividades: - Identificar tipo de incidente. - Escalar incidente a especialista del servicio afectado. - Proponer solución y evaluar y realizar pruebas.	Dueño de proceso Gestor incidente Analistas; segundo, tercer nivel (outsourcing, OTI, seguridad forense) Proveedor	Solución Temporal o Definitiva Postular a gestión de problemas
4	**RESOLVER Y CERRAR EL INCIDENTE**	Solución temporal o definitiva	Implementar la solución temporal o definitiva, validada en la etapa de diagnóstico y construcción de la solución, se presentan las siguientes actividades: - Implantar solución propuesta. - Validar la restauración del servicio. - Documentar y solucionar el incidente en la herramienta de gestión. - Aplicar encuesta de satisfacción. - Cerrar el incidente. - Postular a gestión de la base del conocimiento tecnológico	Dueño de proceso Gestor incidente Analistas; segundo, tercer nivel (outsourcing, OTI, seguridad forense) Proveedor	Incidente solucionado y servicio restablecido
5	**REALIZAR SEGUIMIENTO Y CONTROL**	Registro de incidentes en el periodo de evaluación. Definición de procedimiento y actualización. Orientación del procedimiento Oportunidades de mejora	Describir las actividades que realiza el gestor de incidentes de manera transversal a las etapas de registro, gestión de incidente o incidente masivo, diagnóstico y construcción de la solución, resolución y cierre del incidente, aplicando las siguientes actividades: - Realizar seguimiento al cumplimiento de los ANS. - Proponer mejoras. - Producir y analizar mediciones del procedimiento.	Gestor de Incidentes	Acciones de Mejora. Posible actualización del catálogo de servicios. Capacitaciones

7 DESCRIPCIÓN DE ETAPAS Y ACTIVIDADES

7.1 REGISTRAR INCIDENTE O INCIDENTE MASIVO

7.1.1 Realizar la notificación a través de los canales de comunicación

Esta etapa inicia con la notificación de una falla, interrupción o degradación de un servicio que reporta el usuario o el analista de monitoreo, a través de los canales de comunicación establecidos por el Centro de Servicios Integrados de Tecnología - CSIT.

El analista de primer nivel debe indagar sobre los detalles del error presentado, bien sea por medios de imágenes de la falla o el error presentado, notificaciones ya reportadas por otros usuarios, y sintomatología presentada para tener bases suficientes para iniciar la gestión sobre el servicio de tecnología afectado.

7.1.2 Identificar datos de usuario

El analista de primer nivel realiza la validación de los datos e información básica del usuario, de necesitar más información para el registro del caso, ésta será solicitada a través del medio de comunicación por el cual este atendiendo el caso, con el fin de tener la información consolidada en la herramienta de gestión de servicios tecnológicos de la SIC, y tener consolidada la información de todos los funcionaros y contratistas quienes hacen uso de los servicios tecnológicos administrados por la OTI.

7.1.3 Realizar el registro y categorización

El analista de primer nivel realiza un análisis para identificar la necesidad reportada por el usuario, realizando su categorización de acuerdo con el servicio de tecnología que se encuentra afectado, identifica el grupo que resolverá el incidente de acuerdo con la matriz de categorías del CSIT y registra el caso como incidente en la herramienta de gestión de servicio.

7.1.4 Analizar información para dar solución en primer nivel

De acuerdo con el análisis realizado a la información reportada por el usuario o el analista de monitoreo, se debe consultar en la base de conocimiento si ya se cuenta con una solución aprobada que se pueda implementar para restaurar la falla o el servicio afectado, siempre y cuando la solución a implementar sea del alcance del analista de primer nivel, de lo contrario, debe ser escalada al grupo resolutor encargado de dar solución al incidente.

7.1.5 Validar la existencia de otras notificaciones asociadas a la falla reportada en caso de presentarse masivo

Identificar si existen más notificaciones asociadas a la falla reportada, y realizar el análisis de la presencia de incidente masivo, para declarar un masivo, deben existir 10 casos que presenten la misma sintomatología o que un servicio tecnológico afecte la operación de una o varias áreas de trabajo de la SIC.

El analista de primer nivel debe realizar la notificación al gestor de incidente, quien realizará la comunicación de la afectación del incidente masivo, lo más pronto posible al personal involucrado en la solución y personal de la OTI que debe estar informado, de acuerdo con la política de la gestión de incidentes de tecnología 5.2.3, de este documento.

7.1.6 Clasificar y escalar si es necesario la intervención de atención en segundo o tercer nivel

Si el analista de primer nivel identifica la presencia de un incidente masivo o no encuentra la solución en este nivel, debe clasificar el incidente de acuerdo con servicio afectado y la matriz de categorías del CSIT, escalando al grupo correspondiente quien iniciará la etapa de la gestión del incidente o incidente masivo, y así entregar la información recopilada en esta etapa al especialista con el fin de recuperar el servicio en el menor tiempo posible y minimizar impactos negativos en las áreas de la SIC.

7.2 GESTIONAR INCIDENTE O INCIDENTE MASIVO.

7.2.1 Notificar incidente o incidente masivo

Al tener el registro y asignación del incidente o incidente masivo al grupo encargado de la solución, debe iniciar con el análisis de la causa raíz de la afectación, validar en la base de conocimiento si existen registros de una solución temporal o definitiva que se pueda implementar, de lo contrario, debe empezar a construir una nueva solución.

Todas las notificaciones recibidas a través del CSIT y registradas en la herramienta de gestión, que contengan los mismos síntomas deben ser relacionados al masivo, con el fin de dar una solución general y realizar el cierre unificado de todos los casos identificados y asociados a la misma falla.

7.2.2 Reportar a las partes interesadas

El gestor de incidentes con el apoyo del especialista a cargo de incidente masivo debe informar por correo electrónico en el menor tiempo posible, a las partes involucradas, la presencia del incidente masivo, detallando el servicio afectado, fecha y hora del incidente, tiempo estimado de la solución, y observaciones generales de la falla presentada.

En esta actividad se debe realizar seguimiento y notificación del incidente hasta su solución de acuerdo con los niveles de tiempo definido en el numeral ***5.3 COMUNICACIÓN DE MASIVO***, establecido en esté procedimiento, con esta información, el grupo de tecnología de la OTI, informará a las áreas de atención al ciudadano la falla presentada y tiempos de solución, con el fin de mantener informados al personal directivos de la SIC en caso de que deban iniciar con planes de contingencia.

7.2.3 Entregar solución

Paralelamente a las actividades anteriores definidas en esta etapa, el grupo de especialistas asignado realiza el análisis causa raíz para la entregar una posible solución y recuperación del servicio afectado.

Si al transcurrir dos horas de no tener solución al incidente masivo, se debe involucrar a la gestión de problemas quién apoyará a identificar la causa raíz, de acuerdo con el procedimiento de problemas establecido hasta encontrar su solución.

7.3 DIAGNOSTICAR EL INCIDENTE Y CONSTRUIR LA SOLUCIÓN

7.3.1 Identificar tipo de Incidentes

Si en la etapa del registro del incidente, el analista de primer nivel identifica que el reporte realizado por el usuario es un incidente de seguridad, y no es solucionable en este nivel, el analista de primer nivel identifica el grupo a dar solución, de acuerdo con la matriz de categorías del CSIT, puede ser el especialista OTI o especialista del proveedor de tecnología.

7.3.2 Escalar incidente a especialista del servicio afectado

De acuerdo con las actividades realizadas, el analista de primer nivel debe documentar el caso, adjuntar la evidencia detalladas y enviadas por el usuario, direccionar la solicitud al grupo que corresponda en el nivel necesario para gestionar el incidente. Se debe tener en cuenta los grupos de solución asignados en la matriz de categorías del CSIT.

Si el incidente es asignado al Grupo de Trabajo de Informática Forense y Seguridad Digital, debe guiarse por el ***Procedimiento de gestión de incidentes de seguridad de la información SC05-P01***, y dar solución al incidente, de requerir apoyo del especialista del proveedor de TI, escalar caso con la documentación necesaria para continuar con la gestión del incidente de seguridad, al grupo de especialistas del proveedor de tecnología.

7.3.3 Proponer Solución y evaluar y realizar pruebas

El grupo de especialistas del proveedor de tecnología, evaluar la información y recomendaciones entregadas por el Grupo de Trabajo de Informática Forense y Seguridad Digital, realiza pruebas necesarias, proporciona solución a implementar, de ser necesario, involucra especialistas externos (proveedores de TI) para entregar una solución temporal o definitiva.

En esta actividad, la gestión de la base del conocimiento tecnológico y la gestión de problemas estarán alineados con la gestión de incidentes para encontrar la mejor solución que permita la restauración de los servicios de tecnología afectados, minimizando impactos negativos a la operación.

7.4 RESOLVER Y CERRAR EL INCIDENTE

7.4.1 Implantar solución propuesta

El especialista que tenga a cargo el incidente debe ejecutar la solución entregada de la etapa de diagnóstico, validar si se requiere implementar un cambio en la infraestructura tecnológica, de ser así, se debe solicitar una ventana de mantenimiento al gestor de cambios de acuerdo con el procedimiento de control de cambios DE04-P04, con el fin de no generar una mayor afectación a los servicios tecnológicos.

Realizar pruebas de la solución sobre el servicio reestablecido, si la solución entregada no fue satisfactoria, retornar a la actividad 7.3 Diagnosticar y construir la solución del incidente.

7.4.2 Validar restauración del servicio

Si la solución aplicada por el especialista a cargo del incidente fue satisfactoria, realiza las pruebas necesarias para notificar el restablecimiento del servicio y la operación normal de las actividades.

Si el incidente surgió de un masivo, se debe recopilar las evidencias de la solución para diligenciar el Formato – ***Informe de cierre de incidente masivo***, y postularlo a gestión de la base del conocimiento tecnológico para que sea incluido en la base de conocimiento para referencias futuras.

7.4.3 Documentar y solucionar el incidente en la herramienta de gestión

El especialista a cargo del incidente, valida el resultado de la implementación de la solución, la cual debe ser registrada en la herramienta de gestión del servicio, adjuntar la documentación de las actividades ejecutadas y efectuadas para la restauración del servicio afectado, e incluir el Formato – ***Informe de cierre de incidente masivo***, como información adjunta al caso.

Al realizar la solución del incidente en la herramienta de gestión, de forma automática se envía una notificación al correo electrónico del usuario sobre la encuentra de satisfacción de la solución otorgada al incidente reportado.

7.4.4 Aplicar encuesta de satisfacción

Al obtener la solución del incidente, se genera una encuesta de forma automática desde la herramienta de gestión, la cual debe ser realizada por el solicitante del caso, y es opcional su diligenciamiento.

Si la encuesta es calificada de forma negativa, se reabre el caso automáticamente en la herramienta de gestión, para realizar nuevamente atención y gestión al caso en la etapa diagnóstico y construcción de la solución, con el fin de entregar una solución a satisfacción del usuario.

7.4.5 Cerrar el incidente

La herramienta de gestión de servicios tecnológicos automáticamente cambia de estado solucionado a estado cerrado, cuando la encuesta de satisfacción diligenciada obtuvo una puntuación positiva o luego de tres días hábiles si la encuesta de satisfacción no fue diligenciada y el usuario estuvo de acuerdo con la solución proporcionada.

7.4.6 Postular a la gestión de la base del conocimiento tecnológico

Si la solución implementada es temporal o definitiva, y no se encontraba registrada en la base de conocimiento, se postula a la gestión de la base del conocimiento tecnológico, enviando el Formato ***Informe de cierre de incidente masivo.***

Esta actividad debe ser realizada por el especialista que otorgo la solución, en conjunto con el gestor de incidentes quien realiza el seguimiento y control para la articulación con otras gestiones.

7.5 REALIZAR SEGUIMIENTO Y CONTROL

Las siguientes actividades propuestas, serán realizadas por el gestor de incidentes:

7.5.1 Realizar seguimiento al cumplimiento de los ANS

Realizar seguimiento sobre los casos registrados como incidentes o incidentes masivos, velando que se aplique adecuadamente el procedimiento establecido para la gestión de incidentes en la gestión realizada y solución aplicada a los casos.

Revisar el backlog para velar por la solución de los incidentes, identificando aquellos que requieren intervención de proveedores o especialistas de otras áreas para la solución requerida.

7.5.2 Proponer mejoras

Brindar orientación y ejecución del procedimiento de la gestión de incidentes, identificado opciones de mejora, además, vela porque el procedimiento se siga y

sea guía a la operación, para todos los involucrados directamente en la solución de los incidentes, aclarando inquietudes respecto al mismo.

7.5.3 Producir y analizar mediciones del procedimiento

Recolectar mediciones de desempeño que sirvan para el planteamiento de mejoras al servicio y al procedimiento en general.

8 DOCUMENTOS RELACIONADOS

- SC05-P01 Procedimiento de gestión de incidentes de seguridad de la información.
- DE04-P04 Procedimiento control de cambios
- Procedimiento gestión de problemas
- Formato – Informe Cierre de Incidente Masivo.
- Anexo 1 – Documento Manejo de Casos Suspendidos.
- Anexo 2 “Roles y Responsabilidades - Gestión de Incidentes TI.”
- Matriz de categorías del CSIT

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Creación del documento.

_____

Fin documento