

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

## CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **“Uso interno”**.

El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.

No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

## LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

**TABLA DE CONTENIDO**

**1. OBJETIVO.....3**

**2. ALCANCE.....3**

**3. CONTENIDO. ....3**

3.1. CUANDO SE CONSIDERA UN INCIDENTE MAYOR ..... 3

3.2. POLITICAS GENERALES PARA LA GESTIÓN DE LOS INCIDENTES MAYORES..... 4

3.3. RESPONSABILIDADES ..... 5

**4. FLUJO DEL PROCEDIMIENTO .....6**

**5. DETALLE DEL PROCEDIMIENTO .....7**

**6. CONTROL DE CAMBIOS.....18**

**7. FLUJO DE APROBACIÓN.....19**

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

## 1. OBJETIVO.

Describir el manejo de los incidentes mayores que se presenten con base en el proceso de gestión de incidentes establecido.

## 2. ALCANCE.

Detección, registro y solución de incidente mayores de forma oportuna y eficiente que permitan controlar y abordar los impactos que pueden llegar a afectar la correcta operación de los servicios de la organización.

El proceso de gestión de incidentes mayores cubre las actividades mínimas que deben ejecutar durante la atención de un incidente mayor; estableciendo las funciones y responsabilidades de cada uno de los roles que intervienen en la resolución del incidente.

Este procedimiento aplica para:

- Priorizar y agilizar la atención de incidentes con un impacto Crítico a la operación.
- Priorizar y agilizar la atención de incidentes que derivado de los criterios de impacto y urgencia la combinación da como resultado una prioridad Crítica.
- Realizar investigación y diagnóstico.
- Trabajar con otros procesos y/o áreas de la organización para implementar la solución o resolución del incidente.
- Tener bases de conocimiento que sirvan como fuente de información para futuros incidentes y proceso de Gestión de Problemas.

## 3. CONTENIDO.

### 3.1. CUANDO SE CONSIDERA UN INCIDENTE MAYOR

Este procedimiento establece las siguientes características para la declaración de un incidente mayor:

- % alto de usuarios afectados del cliente.
- Afectación crítica de la continuidad operativa del servicio de la organización.
- El nivel de indisponibilidad sea total para los servicios de la organización.
- Interrupción severa del servicio de impacto crítico para la organización.

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

### **3.2. POLITICAS GENERALES PARA LA GESTIÓN DE LOS INCIDENTES MAYORES.**

1. El proceso de Gestión de Incidentes Mayores estará basado bajo el marco de referencia ITIL 4.
2. Toda persona involucrada en la gestión de incidentes mayores debe referirse al presente documento, conocer las actividades asociadas a la solución de las fallas reportadas, y registrar toda la información y los datos del incidente, incluyendo la respectiva documentación y evidencia de la solución en la herramienta de gestión determinada para tal fin.
3. La gestión de incidentes es responsable en el seguimiento del esquema de escalamiento y comunicación oficial hacia la organización:
  - Aviso de apertura incidente mayor
  - Aviso de actualización de incidente mayor
  - Aviso de cierre de incidente mayor
  - Asegurar que los incidentes sean atendidos oportunamente.
4. El orden de atención y resolución de incidentes mayores se realizara de acuerdo al modelo de priorización establecido.
5. Todo incidente mayor debe tener documentación completa con los avances socializados y el informe de causa raíz asociada a la causa del incidente.
6. Cada incidente mayor debe ser priorizado con urgencia e impacto Critico de acuerdo con la matriz de priorización de la herramienta.
7. Ante la declaración de un incidente mayor se debe parametrizar en la planta telefónica un mensaje de IVR comunicando a los usuarios la novedad con el siguiente mensaje genérico:

Gracias por llamar al MAS, les informamos que en este momento se presentan inconvenientes con (especificar las aplicaciones, ubicaciones o problemas que represente el incidente), estamos generando el diagnóstico por el momento no tenemos tiempo estimado de solución, agradecemos su comprensión, si este inconveniente no afecta su operación por favor espere en la línea para ser atendido.

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

8. El Gestor de incidentes debe hacer retroalimentación cada 30 minutos indicando el avance hasta la solución del Incidente Mayor.
9. Todo incidente mayor identificado debe tener documentación completa en ticket con los avances hasta encontrar la solución por parte de los líderes técnicos.
10. Los incidentes mayores que en la organización sean declarados pero que no sigan las actividades del este procedimiento no harán parte de la data oficial de la gestión de incidentes.

### **3.3. RESPONSABILIDADES**

#### **3.3.1.1. Responsable del proceso**

El responsable del cumplimiento, actualización y mejoramiento de este procedimiento es el líder de gestión de servicio, de la Gerencia Corporativa de Tecnología.

#### **3.3.1.2. Responsables de las actividades del procedimiento**

Cada una de las actividades dentro del proceso están identificadas con su responsable(s), que deben asegurar la correcta ejecución de las actividades.

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

## 4. FLUJO DEL PROCEDIMIENTO

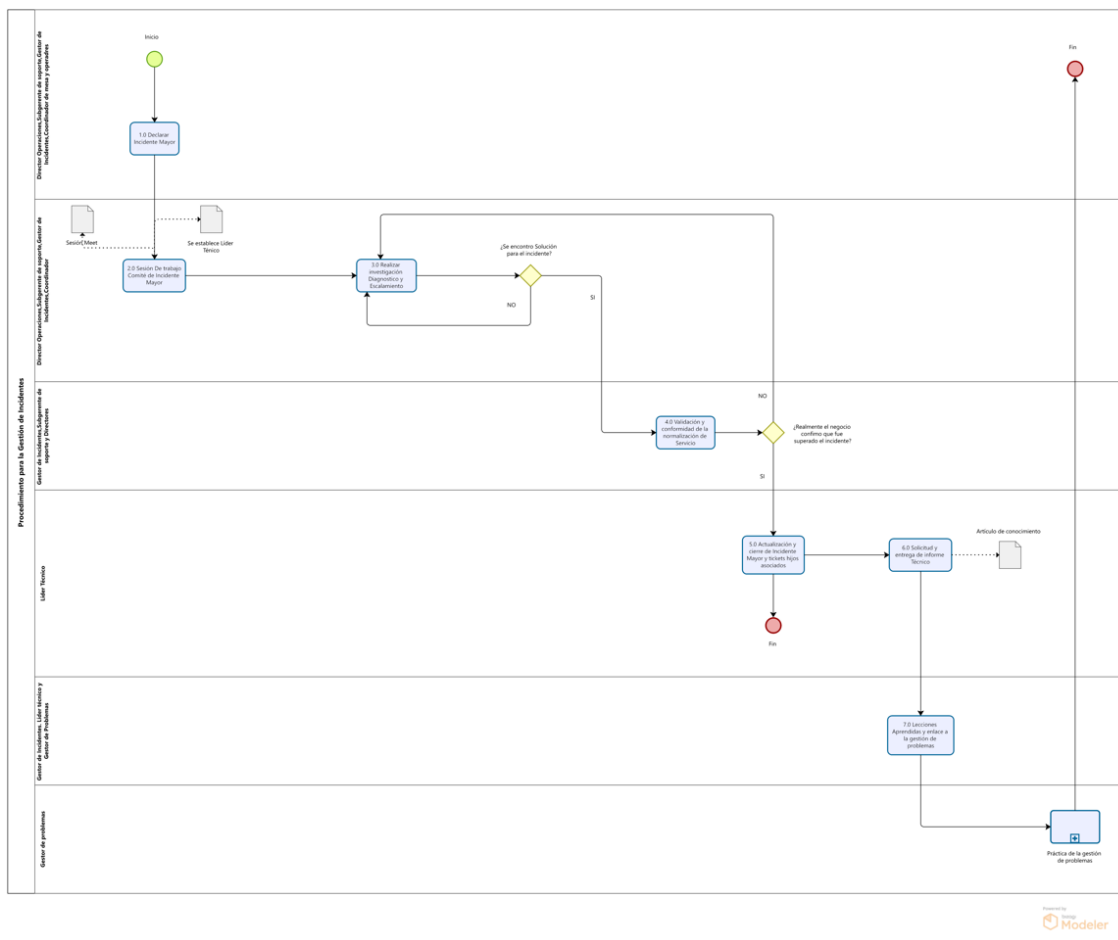


Ilustración 1 Flujo del procedimiento

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

## 5. DETALLE DEL PROCEDIMIENTO

A continuación, se relacionan las actividades del procedimiento:

### Declarar Incidente Mayor

<b>Responsable</b>	<ul style="list-style-type: none"> <li>✓ Director(a) de Operaciones de TI.</li> <li>✓ Director(a) de Redes y Comunicaciones</li> <li>✓ Director(a) de Bases de Datos</li> <li>✓ Subgerente de Soporte</li> <li>✓ Gestor de Incidentes</li> <li>✓ Coordinador Mesa de Servicios</li> <li>✓ Operadores</li> </ul>
<b>Objetivo</b>	Definir un Incidente como Mayor para dar prioridad a su solución dado que compromete gravemente los servicios de la organización.
<b>Acciones</b>	<p>Cualquiera de los roles autorizados para declarar el incidente mayor tiene la responsabilidad de notificar vía: Correo electrónico, mensaje de WhatsApp, llamada telefónica al gestor de incidentes quien deberá realizar las siguientes actividades:</p> <ol style="list-style-type: none"> <li>1. Escribir al grupo de WhatsApp “Inc.Mayores Keralty” consultando si se presenta la novedad de incidente mayor. <p><b>SI :</b> Cuando por este grupo confirman y dan respuesta confirmar el incidente padre y verificar si existe o si se debe crear una sala de crisis.</p> <p><b>NO:</b> Cuando no confirman y la mesa continúa colapsada se realiza la habilitación del ticket padre y se notifica operadores.</p> <p><b>Nota 1:</b> Si en grupo de WhatsApp “Inc.Mayores Keralty” no hay respuesta se escribe al grupo.</p> </li> <li>2. Escribir al grupo de WhatsApp “Operación infraestructura” consultando si se presenta la novedad de incidente mayor. <p>Cuando por este grupo confirman y da respuesta confirmar el incidente padre y verificar si existe o si se debe crear una sala de crisis.</p> <p><b>Nota 2:</b> Una vez se declare el ticket de Incidente Mayor el gestor de incidentes deberá en la herramienta de gestión BMC marcar el ticket como “Incidente Mayor” y notificar a la mesa de servicio que todos los incidentes relacionados a la falla principal se deben asociar al ticket padre.</p> </li> </ol>

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

**Conocemos que WhatsApp no es un canal oficial de la mesa de servicios, pero este mensaje es de carácter informativo.**

#### **Formato de Aviso de apertura de Incidente Mayor por WhatsApp**

Tener en cuenta que el canal de WhatsApp solo será para informar de una manera más rápida y solo podrán enviar mensajes los administradores, solamente se informará lo siguiente a través de el:

Contenido el mensaje:

Buenos días/tardes, Se informa que se ha abierto el incidente mayor No. #####

Problema reportado: <Resumen breve del problema registrado>

Asunto del correo: Apertura incidente mayor No. #####

Contenido del correo:

#### **AVISO DE APERTURA DE INCIDENTE MAYOR**

**Horario Inicio Incidente:** <hh>:<mm>

**Fecha:** <día> de <mes> del <año>

**Numero de Ticket de referencia al incidente Mayor abierta:** # XXXXX

#### **Situación Actual:**

Describir de manera clara y concisa la situación actualmente identificada con base a los reportes de los usuarios.

**Nivel de Afectación identificado al momento:** Administrativo / Clínicas/ Etc

#### **Servicio(s) Afectados:**

<Descripción del Servicio 1>

<Descripción del Servicio 2>

Fecha y hora del reporte inicial:

Líder asignado al caso:

Grupos de especialistas:

Dueños de los servicios afectados:

Diagnóstico y acciones actuales:



<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

	<p>Impacto:</p> <p><b>Nota 2:</b> Se realiza la notificación a los grupos de WhatsApp: Soporte sitio Bogotá, microinformática regional, clínica sitio y mesa de servicio Keralty informando el número de ticket padre.</p> <p>3. Ante la declaración de un incidente mayor se debe parametrizar en la planta telefónica un mensaje de IVR comunicando a los usuarios la novedad con el siguiente mensaje genérico:</p> <p>➤ Gracias por llamar al MAS, les informamos que en este momento se presentan inconvenientes con (especificar las aplicaciones, ubicaciones o problemas que represente el incidente), estamos generando el diagnóstico por el momento no tenemos tiempo estimado de solución, agradecemos su comprensión, si este inconveniente no afecta su operación por favor espere en la línea para ser atendido.</p> <p>Esta actividad es responsabilidad del Coordinador de la mesa de servicio.</p>
<b>Entregable</b>	Declaración incidente mayor Ticket padre. Habilitación del IVR en la planta telefónica.
<b>Plazo</b>	Durante la declaración
<b>Trazabilidad</b>	Herramienta de gestión – Tickets Grupos de WhatsApp

*Tabla 1 Declarar incidente mayor*

### Sesión De Trabajo Comité De Incidente Mayor

<b>Responsable</b>	<ul style="list-style-type: none"> <li>✓ Gestor de Incidentes</li> <li>✓ Director(a) de Operaciones de TI.</li> <li>✓ Director(a) de Redes y Comunicaciones</li> <li>✓ Director(a) de Bases de Datos</li> <li>✓ Subgerente de Soporte</li> <li>✓ Gerente Corporativo de Tecnología</li> <li>✓ Operadores</li> <li>✓ Líderes de servicios</li> </ul>
<b>Objetivo</b>	Convocar a cada una de las personas responsables de la resolución del incidente para que en esta sesión de trabajo puedan identificar las posibles soluciones temporales para mitigar el impacto del incidente mayor.
<b>Acciones</b>	<p>1. Es responsabilidad del gestor de incidentes habilitar la sala de reunión mediante herramienta de Google meet convocando a:</p> <ul style="list-style-type: none"> <li>➤ Líderes y coordinadores</li> <li>➤ Director(a) de Operaciones de TI.</li> </ul>

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

- Director(a)de Redes y Comunicaciones
- Director(a)de Bases de Datos
- Subgerente de Soporte
- Gerente Corporativo de Tecnología

Quedará bajo responsabilidad de los participantes de la meet determinar que otros roles , especialistas y proveedores deberán participar en la sesión y delegar las actividades necesarias para trabajar en la solución.

1. Durante la sesión de trabajo la dirección determinara quien es el líder técnico del incidente el cual se hará cargo de guiar la restauración del Incidente Mayor, interactuar con las distintas áreas resolutoras en caso de requerir información y/o apoyo, y será el responsable de proveer información a la mesa de servicio.
2. Con la información de quien es el líder técnico que tiene la responsabilidad del incidente mayor el gestor de incidentes junto al equipo de dirección y subgerencia deberá definir la versión oficial y los detalles que se proporcionarán a los interesados en relación con el Incidente Mayor.
3. Notificación de avance o recuento del incidente mayor:

#### **Formato de Aviso de actualización de Incidente Mayor por WhatsApp**

Contenido el mensaje:

Buenos días/tardes, Se informa estatus del incidente mayor No. #####

Actualización: <Resumen breve de las actividades realizadas y el estado actual del incidente>

**Asunto del correo:** Actualización incidente mayor No. #####

**Contenido del correo:**

#### **Actualización del caso – Situación actual:**

Describir de manera clara y concisa la situación actualmente identificada. ¿Existe algún avance o solución temporal a comunicar a los usuarios?

-----  
**Horario Inicio Incidente:** <hh>:<mm>

**Fecha:** <día> de <mes> del <año>

**Numero de Ticket de referencia al incidente Mayor abierta:** # XXXXX

**Fecha y hora actualización:** día> de <mes> del <año> <hh>:<mm>

**Situación Actual:**

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

	<p><b>Nivel de Afectación identificado al momento:</b> Administrativo / Regional / Ciudad.</p> <p><b>Servicio(s) Afectados:</b></p> <p>&lt;Descripción del Servicio 1&gt;</p> <p>&lt;Descripción del Servicio 2&gt;</p> <p>Fecha y hora del reporte inicial:  Líder asignado al caso:  Grupos de especialistas:  Dueños de los servicios afectados:  Diagnóstico y acciones actuales:  Impacto:</p> <p>4. El gestor de incidentes durante la sesión de meet en promedio cada 30 minutos y dependiendo de duración de la meet preguntara a los participantes de la sesión cual es avance para notificarlo en los grupos de WhatsApp.</p> <p>5. Esta información deberá entregarse a la coordinación del MAS para su difusión interna y notificación en el momento en que los usuarios registren ausencia del servicio asociado al IM.</p> <p><b>Nota 1:</b> El gestor de incidentes será un articulador durante la meet pero la responsabilidad de encontrar las soluciones a implementar es de los roles especializados de la organización.</p> <p><b>Nota 2:</b> Si debido al Incidente Mayor se presentan vulnerabilidades de la Confidencialidad, Disponibilidad y/o Integridad de la información, convocar al Área de Seguridad de la Información.</p>
	<b>Entregable</b> Declaración incidente mayor Ticket padre
	<b>Plazo</b> Máximo 10 minutos después de ser declarado el IM.
	<b>Trazabilidad</b> Herramienta de gestión – Tickets Grupos de WhatsApp

*Tabla 2 Sesión de trabajo comité de incidente mayor*

### Realizar Investigación, Diagnostico y Escalamiento

<b>Responsable</b>	<ul style="list-style-type: none"> <li>✓ Gestor de Incidentes</li> <li>✓ Director(a) de Operaciones de TI.</li> <li>✓ Director(a) de Redes y Comunicaciones</li> <li>✓ Director(a) de Bases de Datos</li> </ul>
--------------------	---

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

	<ul style="list-style-type: none"> <li>✓ Subgerente de Soporte</li> <li>✓ Gerente Corporativo de Tecnología</li> <li>✓ Operadores</li> </ul>
<b>Objetivo</b>	Investigar y diagnosticar el incidente mayor y de ser necesario realizar escalamiento niveles 3, fabricantes, etc., con el objetivo de resolver el IM.
<b>Acciones</b>	<p>Se deben realizar las siguientes acciones:</p> <ol style="list-style-type: none"> <li>1. Identificar sintomatología de la falla.</li> <li>2. Entender el orden cronológico de los hechos.</li> <li>3. Confirmar el impacto completo del Incidente.</li> <li>4. Identificar cualquier evento que pudiera haber provocado el Incidente. (Calendario de cambios)</li> <li>5. Búsqueda de información (Base de conocimientos, etc.)</li> <li>6. Confirmar si el líder técnico asignado en el punto 2.0 continua o si deber cambiar a otro líder.</li> <li>7. Involucrar grupos especialistas que contribuyan a la solución temporal o definitiva del IM.</li> </ol> <p><b>¿Se encontró solución para el incidente?</b></p> <p><b>SI:</b> Durante la sesión se encontró la posible solución para el incidente temporal o definitiva y para implementarla requiere realizar alguna acción sobre componentes, infraestructura, servicios etc. en producción debe quedar legalizado con un ticket de cambio de "EMERGENCIA".</p> <p><b>Nota :</b> Después de la ejecución del cambio de emergencia el líder técnico deberá notificar que el incidente fue solucionado para que en la actividad 4.0 Validación y conformidad de la normalización del servicio el gestor de incidentes y directores puedan validar con el negocio si esta confirmación es cierta.</p> <p>En el escenario donde aún <b>NO</b> se tenga solución temporal o definitiva al incidente mayor se debe realizar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>➤ Evaluar si el grupo de solución requiere hacer escalamientos de tercer nivel o cualquier otro.</li> <li>➤ Esta acción debe ser evaluada de manera constante durante la atención del incidente mayor.</li> </ul>

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

- Validar si se requiere en la sesión de crisis la participación de proveedores o consultores especializados
- Continuar con las actividades hasta encontrar la solución temporal o definitiva al IM.

Se debe realizar la actualización del avance o recuento del incidente mayor:

**Formato de Aviso de cierre de Incidente Mayor por WhatsApp**

Contenido el mensaje:

Buenos días/tardes, Se informa que el incidente mayor No. ##### ha sido cerrado

Detalle cierre: <Resumen breve del cierre>

Asunto del correo: Cierre incidente mayor No. #####

Contenido del correo:

**AVISO DE CIERRE DE INCIDENTE MAYOR**

**Acciones Correctivas / Siguietes pasos:**

¿Qué pasos faltan llevarse a cabo? Rol, responsabilidad, fecha. Agregar el número de ticket del registro de Problema para búsqueda de causa raíz y solución definitiva.

**Información del cierre - Solución:**

Ya cerrado el incidente, describir de manera clara y concisa la situación actualmente identificada con base a la retroalimentación de los usuarios.  
¿Existe una solución temporal a comunicar a los usuarios?

**Causa:**

Describir de manera general la causa identificada con base al diagnóstico realizado.

**Fecha:** <día> de <mes> del <año>

**Numero de Ticket de referencia al incidente Mayor Cerrada:** # XXXXX

**Horario Inicio Incidente:** <hh>:<mm>

**Horario Fin Incidente:** <hh>:<mm>

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

	<p><b>Tiempo de Solución:</b> &lt;hh&gt;:&lt;mm&gt;</p> <p><b>Tiempo Total de Negocio Impactado:</b> &lt;hh&gt;:&lt;mm&gt;</p> <p><b>Fecha y hora de restauración a la operación normal:</b></p> <p>&lt;día&gt; de &lt;mes&gt; del &lt;año&gt;</p> <p>&lt;hh&gt;:&lt;mm&gt;</p> <p><b>Nivel de Afectación identificado al momento:</b> Administrativo /Regional / Ciudad.</p> <p>Fecha y hora del reporte inicial:</p> <p>Líder asignado al caso:</p> <p>Grupos de especialistas:</p> <p>Dueños de los servicios afectados:</p> <p>Diagnóstico y acciones actuales:</p> <p>Impacto:</p>
<b>Entregable</b>	Incidente diagnosticado
<b>Plazo</b>	Máximo 30 minutos después de ser declarado el IM.
<b>Trazabilidad</b>	Actualización Ticket de Incidente Mayor por parte del líder técnico

*Tabla 3 Realizar investigación, diagnóstico y escalamiento*

### Validación y Conformidad De La Normalización del Servicio

<b>Responsable</b>	<ul style="list-style-type: none"> <li>✓ Gestor de Incidentes</li> <li>✓ Subgerente de Soporte</li> <li>✓ Directores</li> </ul>
<b>Objetivo</b>	Obtener la validación y conformidad de parte del negocio para dar por superado el incidente mayor
<b>Acciones</b>	<ul style="list-style-type: none"> <li>➤ Una vez confirmado por el equipo de IM, se debe solicitar al negocio la ejecución de pruebas de los servicios que se encontraban afectados.</li> <li>➤ Actualizar el ticket de Incidente Mayor.</li> <li>➤ Notificar a los agentes de mesa la solución del IM, para que a su vez le sea informado a aquellos usuarios que se comuniquen con el MAS.</li> </ul> <p><b>¿Realmente el negocio confirmo que fue superado el incidente?</b></p> <p><b>SI</b> Ir la actividad N° 5.0 Actualización y Cierre De Incidente Mayor y Tickets Hijos Asociados</p>

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

	<b>NO</b> regresar a la actividad N° 3.0 Realizar investigación, diagnóstico y escalamiento.
<b>Entregable</b>	Incidente Mayor resuelto
<b>Plazo</b>	Dentro de los 10 minutos siguientes a la solución del Incidente
<b>Trazabilidad</b>	Notificación a los grupos de WhatsApp y cierre del Ticket de Incidente Mayor (se debe registrar el ticket en la generación del informe técnico).

*Tabla 4 Validación y conformidad de la normalización del servicio*

### Actualización y Cierre De Incidente Mayor y Tickets Hijos Asociados

<b>Responsable</b>	✓ Líder técnico
<b>Objetivo</b>	Actualizar y documentar el cierre del ticket del incidente Mayor y tickets asociados en la herramienta de gestión BMC
<b>Acciones</b>	<p>Es responsabilidad del líder técnico asignado en la solución del incidente mayor a realizar las siguientes actividades:</p> <ul style="list-style-type: none"> <li>➤ Actualizar y garantizar que la categoría del ticket padre corresponde a la falla del incidente mayor.</li> <li>➤ Actualizar grupo y especialista responsable de la solución del incidente mayor.</li> <li>➤ Documentar el campo “Nota de Resolución” las actividades y acciones que se ejecutaron para dar solución al incidente mayor.</li> <li>➤ Adjuntar documentos y evidencias de cierre.</li> </ul>
<b>Entregable</b>	Ticket de Incidente Mayor y tickets asociados documentados y en estado “Resuelto” en BMC.
<b>Plazo</b>	Inmediato una vez confirme la solución.
<b>Trazabilidad</b>	Ticket de incidente mayor y tickets asociados

*Tabla 5 Actualización y cierre de incidente mayor y tickets hijos asociados*

### Solicitud y Entrega De Informe Técnico

<b>Responsable</b>	<ul style="list-style-type: none"> <li>✓ Gestor de Incidentes</li> <li>✓ Líder técnico, director o gerente.</li> </ul>
<b>Objetivo</b>	Solicitar los antecedentes del Incidente Mayor, actividades realizadas, solución del incidente y acciones futuras para evitar que se presente un nuevo incidente y dar cuenta de los antecedentes del Incidente Mayor, su contexto, análisis de impacto y cronología, situación actual, riesgos del negocio, conclusiones y compromisos de mejora.

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

<b>Acciones</b>	<p>El gestor de incidentes de manera inmediata una vez se de resolución al incidente mayor debe realizar la solicitud del informe técnico</p> <ul style="list-style-type: none"> <li>➤ Identificar la persona responsable de la entrega del informe técnico.</li> <li>➤ El Gestor de incidentes solicitará en la Meet (sala de crisis) y a través de un correo electrónico en donde indique el número de ticket de la solicitud del informe técnico respectivo.</li> </ul> <p><b>El informe técnico debe tener las siguientes características:</b></p> <ul style="list-style-type: none"> <li>➤ La entrega del informe técnico es responsabilidad del Líder Técnico, el cual deberá ser bajo el formato definido por la Gerencia Corporativa de Tecnología.</li> <li>➤ En caso de aplicar, se debe identificar puntos de falla crítica, las cuales deber ser analizadas desde las áreas que puedan verse involucradas.</li> <li>➤ Si durante la fase de cierre de incidente de mayor no se tiene el informe técnico no se puede realizar la actividad de lecciones aprendidas y es por esto que será responsabilidad del gestor de problemas garantizar que el líder técnico lo entregue porque esto es insumo de análisis del ciclo de vida de la gestión de problemas.</li> </ul> <p><b>Nota:</b> Los informes técnicos contribuyen a la gestión de conocimiento es por esta razón el que gestor de conocimiento deberá garantizar que los informes técnicos son entregados y cargados en la base de conocimiento de la herramienta de gestión ITSM.</p>
<b>Entregable</b>	Informe técnico
<b>Plazo</b>	Máximo 5 días hábiles (luego de que el incidente haya sido restaurado).
<b>Trazabilidad</b>	Ticket de incidente mayor y repositorio

*Tabla 6 Solicitud y entrega de informe técnico*

### Lecciones Aprendidas y Enlace a la Gestión de Problemas

<b>Responsable</b>	<ul style="list-style-type: none"> <li>✓ Gestor de Incidentes</li> <li>✓ Líder Técnico</li> <li>✓ Gestor de problemas</li> </ul>
<b>Objetivo</b>	<ul style="list-style-type: none"> <li>➤ Evaluar la correcta ejecución del proceso de gestión de Incidente Mayor.</li> <li>➤ Analizar Impacto, Riesgo y Causa Raíz del Incidente Mayor de forma colaborativa y transversalmente con todas las áreas involucradas.</li> </ul>
<b>Acciones</b>	<p>Convocar a todos los involucrados en la gestión del Incidente Mayor, para socializar las lecciones aprendidas.</p> <p>Para el día hábil siguiente a la restauración del incidente mayor.</p>



<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

	<p><b>En esta sesión se revisará los siguientes aspectos:</b></p> <p>Realizar la sesión en donde se expongan las lecciones aprendidas.</p> <p>El gestor de incidentes debe realizar la minuta de la reunión, siendo el plazo máximo de envío 1 día hábil posterior a la reunión.</p> <p>La cronología de la sesión es:</p> <ol style="list-style-type: none"> <li>1. Análisis cumplimiento del proceso. Checklist de tareas del procedimiento. 15 minutos.</li> <li>2. Análisis cronología e impacto. 15 minutos</li> <li>3. Análisis causa raíz, bajo la metodología de los 5 porqués. 15 minutos</li> </ol> <p>Es responsabilidad del Líder Técnico completar el borrador de informe técnico que se trabaja en la reunión, enviarlo para la validación cruzada, corregir de ser necesario y, por último, adjuntarlo en el ticket mediante el cual se solicita.</p> <p><b>Nota:</b> Esto se revisará en detalle en la gestión de problemas ver documento anexo.</p>
	<p><b>Entregable</b></p> <p>Minuta Reunión Lecciones Aprendidas. Postulación de ticket de problema</p>
	<p><b>Plazo</b></p> <p>Máximo 3 días hábiles después de solucionado el Incidente Mayor con duración de 1 hora</p>
	<p><b>Trazabilidad</b></p> <p>Ticket de Problema</p>

*Tabla 7 Lecciones aprendidas y enlace a la gestión de problemas*

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

## 6. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
02/08/2022	Creación del documento	1.0
02/08/2023	Ajuste sobre el documento.	2.0
30/04/2024	El documento se revisa en el marco de la actualización del SGSI año 2024, se valida con el responsable del documento quien nos informa que a la fecha no existe ningún cambio en el contenido de este, se realiza inclusión de la sigla del país y la compañía en el código del documento.	2.1

*Tabla 8 Control de cambios*

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES MAYORES</b>	
<b>Fecha: 28-10-2024</b>		
<b>Código: SIG-SS-CKE-PR10</b>		

## 7. FLUJO DE APROBACIÓN.

<b>ELABORÓ</b>	<b>REVISÓ</b>	<b>APROBÓ</b>
Nombre: Javier Alonso Galván Castañeda Área/Proceso: Gerencia Corporativa de tecnología Fecha: 02/08/2022	Nombre: Fredy Arley Páez Valencia Área/Proceso: Microinformática Fecha: 28/10/2024	Nombre: Luisa Fernanda Trujillo Área/Proceso: vicepresidente de sistemas de información Fecha: 28/10/2024

*Tabla 9 Flujo de aprobación*

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.