**TABLA DE CONTENIDO**

[1. OBJETIVO 2](#_Toc22788711)

[2. FECHA DE CREACIÓN 2](#_Toc22788712)

[3. EQUIPO INVESTIGADOR 2](#_Toc22788713)

[4. METODOLOGÍA DE LA INVESTIGACIÓN 2](#_Toc22788714)

[5. ANÁLISIS DEL EVENTO 3](#_Toc22788715)

[5.1. IDENTIFICACIÓN DEL EVENTO 3](#_Toc22788716)

[5.2. servicios, PLATAFORMAS, infraestructura y/o activos AFECTADos 3](#_Toc22788717)

[5.3. NÚmero de Caso reportado: 3](#_Toc22788718)

[6. HIPÓTESIS PLANTEADAS 3](#_Toc22788719)

[7. DESARROLLO DE LAS HIPÓTESIS 3](#_Toc22788720)

[7.1. HIPÓTESIS 1: 3](#_Toc22788721)

[8. LECCIONES APRENDIDAS 3](#_Toc22788722)

[9. CONCLUSIONES 3](#_Toc22788723)

[10. LISTADO DE EVIDENCIAS 3](#_Toc22788724)

[11. ANEXOS 3](#_Toc22788725)

[12. POSTULACIONES 4](#_Toc22788726)

**INFORMACIÓN DEL REPORTE**

# OBJETIVO

# FECHA DE CREACIÓN

# EQUIPO INVESTIGADOR

# METODOLOGÍA DE LA INVESTIGACIÓN

La presente investigación seguirá la siguiente metodología para determinar la causa raíz del evento de interés:

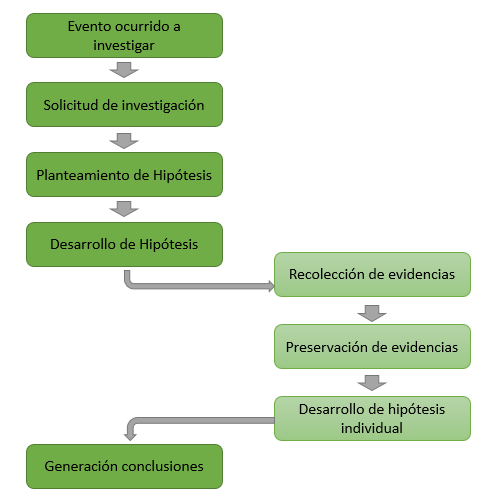


Imagen 1: Metodología desarrollada durante la investigación de causa raíz

1. **Evento ocurrido a investigar:** Evento que es de interés para la operación de TI y que puede ser objeto de investigación.
2. **Solicitud de investigación:** En este paso se realiza la solicitud por parte de los responsables de TI de la entidad para realizar investigación del evento de interés ocurrido en la infraestructura de TI de la entidad.
3. **Planteamiento de hipótesis:** Basado en el evento ocurrido, el equipo investigador plantea diferentes hipótesis para identificar la posible o posibles causas raíces que generaron el evento de interés.
4. **Desarrollo de la hipótesis:** En esta etapa se desarrolla cada una de las hipótesis planteadas a través de los siguientes pasos:

* **Recolección de evidencias:** En esta actividad se recolectan las evidencias correspondientes que sustentarán la hipótesis individual planteada.
* **Preservación de las evidencias:** En esta actividad se preservan las evidencias correspondientes a los hechos y datos asociados a las mismas, garantizando así la cadena de custodia correspondiente.
* **Desarrollo de hipótesis individual:** En esta actividad con las evidencias recolectadas se desarrolla la hipótesis individual a través de un enfoque sistémico que permite llegar a futuras conclusiones. Las hipótesis son desarrolladas por personal ajeno al evento ocurrido, este puede ser interno o externo.

1. **Generación de conclusiones:** En esta etapa se genera las conclusiones correspondientes que soporten cada una de las hipótesis planteadas, siempre evitando dar juicios de valor.

# ANÁLISIS DEL EVENTO

## IDENTIFICACIÓN DEL EVENTO

## servicios, PLATAFORMAS, infraestructura y/o activos AFECTADos

## NÚmero de Caso reportado:

# HIPÓTESIS PLANTEADAS

# DESARROLLO DE LAS HIPÓTESIS

## HIPÓTESIS 1:

# LECCIONES APRENDIDAS

# CONCLUSIONES

# LISTADO DE EVIDENCIAS

| **EVIDENCIAS** | **DESCRIPCIÓN** | **LINK** | **SUMA DE VERIFICACIÓN** |
| --- | --- | --- | --- |
|  |  |  |  |

# [ANEXOS](#_Toc412468392)

|  |  |
| --- | --- |
| **Nombre del Documento** | **Ubicación** |
|  |  |

# 

# POSTULACIONES

* 1. ¿Se debe postular a la Gestión de Conocimiento la solución de este Incidente de seguridad de la información?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Si |  |  |  | |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |
| No |  | ¿Por qué? | |  |  |  |  |  |  |

Número de caso: \_\_\_\_\_\_\_\_\_\_\_\_

* 1. ¿Se debe postular a la Gestión de Problemas con el fin de iniciar proceso para verificación de análisis de causa raíz o creación de Error conocido?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Si |  | Error Conocido |  |  |  | Análisis Causa Raíz | |  |
| No |  | ¿Por qué? |  |  |  |  |  |  |

|  |  |
| --- | --- |
| Elaborado por: | Revisado por: |
| Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Nombre:  Rol: | Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Nombre:  Rol:  Servicio afectado: |
| Fecha: DD/MM/AAAA | Fecha: DD/MM/AAAA |
| Correo electrónico: | Correo electrónico: |

**INSTRUCCIONES PARA DILIGENCIAR EL FORMATO**

**(NO ANEXAR AL FORMATO ENVIADO)**

# OBJETIVO: (Obligatorio) Plantee los objetivos que se desarrollaran durante la elaboración del presente informe de incidente de seguridad.

# FECHA DE CREACIÓN: (Obligatorio) Indique la fecha de creación del informe (DD/MM/AAAA).

# EQUIPO INVESTIGADOR: (Obligatorio) Relacione el equipo que realizó la investigación y el presente reporte.

# METODOLOGÍA DE LA INVESTIGACIÓN: (Obligatorio) No modifique este apartado

# ANÁLISIS DEL EVENTO

## IDENTIFICACIÓN DEL EVENTO: (Obligatorio) Haga una descripción del evento y/o incidente de seguridad ocurrido que es motivo de investigación. Cité hechos relevantes que puedan ayudar al lector a entender la situación que se quiere evidenciar, teniendo en cuenta los siguientes interrogantes: Quién, Cómo, Cuándo, Dónde, Por qué y Para qué.

## servicios, PLATAFORMAS, infraestructura y/o activos AFECTADos: (Obligatorio) Enumere los servicios, plataformas, infraestructura y/o activos de información afectados por el evento y/o incidente de seguridad.

## NÚmero de Caso reportado: (Obligatorio) Escriba el número del caso que se abrió el incidente.

# HIPÓTESIS PLANTEADAS: (Obligatorio) Enumere las diferentes hipótesis que se desarrollaran para encontrar la causa raíz que generó el evento y/o incidente de seguridad.

# DESARROLLO DE LAS HIPÓTESIS (Obligatorio) Desarrolle cada una de las hipótesis planteadas que se utilizarán para encontrar la causa raíz que generó el evento y/o incidente de seguridad.

## HIPÓTESIS 1: (Obligatorio) Desarrolle la hipótesis planteada.

# Lecciones aprendidas: (Obligatorio) Identifique las lecciones aprendidas que se identificaron durante la gestión del incidente.

# CONCLUSIONES: (Obligatorio) Indique cada una de las conclusiones generadas con el desarrollo de las diferentes hipótesis planteadas.

# LISTADO DE EVIDENCIAS: (Obligatorio) a continuación se detallan los datos a diligenciar en cada campo:

| **EVIDENCIAS** | **DESCRIPCIÓN** | **LINK** | **SUMA DE VERIFICACIÓN** |
| --- | --- | --- | --- |
| Coloque el nombre de la evidencia. Registre una evidencia por fila. Adicione cuantas filas necesite. | Describa brevemente la evidencia. | Si la evidencia es digital coloque la ruta donde se encuentra almacenada. | Si la evidencia es digital calcule la suma de verificación de la misma e ingréselo acá. |

# [ANEXOS](#_Toc412468392): (Obligatorio) a continuación se detallan los datos a diligenciar en cada campo:

|  |  |
| --- | --- |
| **Nombre del Documento** | **Ubicación** |
| Registre el nombre del documento identificado como anexo.  Registre un anexo por fila. Adicione cuantas filas necesite. | Registre la ruta donde se encuentra ubicado. |

# POSTULACIONES: Diligencie seleccionando la opción que corresponda tanto para la Gestión de Conocimiento como en Gestión de Problemas. En caso de seleccionar No, debe tener en cuenta que se debe justificar.

**Elaborado por:** Nombre del profesional de la Subdirección de Recursos Tecnológicos que apoya la gestión de incidentes de seguridad de la información o del Especialista del proveedor de servicios de TI a cargo de la solución del incidente.

**Revisado por:** Nombre del Profesional de la Subdirección de Recursos Tecnológicos que apoya la supervisión del servicio asociado al Incidente, o del Profesional responsable de los sistemas misionales y apoyo de la Subdirección de Sistemas Integrados de información.

**Fecha:** registrar la fecha en la que firma, en el orden día, mes y año.