METODOLOGIA PARA LA GESTION Y CLASIFICACION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

CONTENIDO

METODOLOGIA PARA LA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

1. OBJETIVO

Establecer una metodología que permita Gestionar incidentes de seguridad y privacidad de la información, mediante la ejecución de actividades, responsabilidades y organización del flujo de trabajo, teniendo en cuenta los lineamientos y estándares en la identificación, atención y respuesta oportuna para mitigar el impacto asociado a la perdida de la integridad, confidencialidad y disponibilidad de la información.

2. ALCANCE

La gestión de incidentes inicia desde su notificación e identificación de un posible incidente, detección, contención y solución de este, finalizando con la documentación y lecciones aprendidas y aplica en desde el nivel directivo hasta el nivel más bajo de servicios que este estructurado en la Gobernación de Casanare.

3. POLÍTICAS DE OPERACIÓN

3.1.1. Notificación del Incidente

Los posibles incidentes de seguridad se reportarán a la Dirección de tecnologías de la información y las comunicaciones TIC a través de los siguientes canales:

Enviando un mensaje de correo electrónico con la solicitud al buzón seguridaddigital@casanare.gov.co.

Llamando a la Dirección de tecnologías de la información y las comunicaciones TIC extensión IP - 1451.

Informando de manera presencial a la Dirección de tecnologías de la información y las comunicaciones TIC de la Gobernación de Casanare ubicada en Centro Administrativo Departamental
Carrera 20 No. 8 - 02 - Piso 4 - Torre A- Yopal - Casanare - Colombia

El colaborador que identifique el posible incidente de seguridad debe reunir la información que llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención del mismo, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos, archivos, personas implicadas entre otros, y diligenciar el formato que para este procedimiento de establezca (Formato XX-XXX-000)

Si el incidente corresponde a la perdida de datos personales, este deberá ser reportado al Oficial de Protección de Datos Personales, quien lo reportara a la Superintendencia de Industria y Comercio.

3.1.2. Registro y Categorización de incidente

Una vez se reciba la notificación de un posible incidente de seguridad, la Dirección de tecnologías de la información y las comunicaciones TIC debe realizar el registro y clasificación en un sistema de requerimientos o en un documento electrónico que permita control y seguimiento para iniciar con la atención del mismo, allí se generará un número de seguimiento y categorización de acuerdo a los siguientes criterios básicos:

• Hubo daño o pérdida de información.
• Hubo fuga y/o robo de información.
• Hubo robo de credencias o información mediante Phishing.
• Se presentó modificación no autorizada de la información.
• Se presenta un comportamiento anormal del computador y/o sistema de información.
• Se presentó suplantación de identidad.
• Se presentó un acceso no autorizado.
• Se presentó pérdida o alteración de registros de base de datos.
• Se presentó una pérdida de un activo de información.
• Hubo presencia de código malicioso “malware, Ransomware”.
• Se presentó una denegación del servicio.
• Se presentó algún ciberataque.

3.1.3. Clasificación y Valoración del incidente

Todos los incidentes de seguridad deberán estar clasificados y valorados para su atención en la herramienta de gestión con la que cuente la Gobernación de Casanare y acorde a la Política Administración del Riesgo PT-SGI-01 27-02-2019 V. 04 adoptada por la entidad y acorde a la siguiente tabla:

Descriptor	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO	Valor del Impacto
Catastrófico	• Afectación ≥50% de la población, atendida por la entidad. • Afectación ≥50% del presupuesto anual de la entidad. • Afectación muy grave al medio ambiente que requiere de ≥1 años de recuperación.	• Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la disponibilidad de la información debido al interés particular de los	5 EXTREMO

	• Recuperación y normalización de la continuidad de la operación ≥72 h	empleados y terceros. • Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	
Mayor	• Afectación ≥40% y <50% de la población, atendida por la entidad. • Afectación ≥40% y <50% del presupuesto anual de la entidad. • Afectación importante del medio ambiente que requiere de ≥3 meses de recuperación. • Recuperación y normalización de la continuidad de la operación ≥48 h	• Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4 ALTO
Moderado	• Afectación ≥25% y <40% de la población, atendida por la entidad. • Afectación ≥25% y <40% del presupuesto anual de la entidad. • No hay afectación al medio ambiente. • Recuperación y normalización de la continuidad de la operación ≥48 h	• Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros	3 MODERADO
Menor	• Afectación ≥5% y <15% de la población, atendida por la entidad.	• Afectación leve de la integridad. • Afectación leve de la disponibilidad.	1, 2 BAJO

	• Afectación ≥5% y <15% del presupuesto anual de la entidad. • No hay afectación al medio ambiente. • Recuperación y normalización de la continuidad de la operación ≥ 24 h	• Afectación leve de la confidencialidad..	
Insignificante	• Afectación <0.5% de la población, atendida por la entidad. • Afectación <0.5% del presupuesto anual de la entidad. • No hay afectación medioambiental. • Recuperación y normalización de la continuidad de la operación < 8 h	• Sin afectación de la integridad. • Sin afectación de la disponibilidad. • Sin afectación de la confidencialidad	

Tabla 1: Valoración del Incidente (Fuente Política Administración del Riesgo PT-SGI-01 27-02-2019 V. 04**).**

3.1.4. Prioridad de Atención

Acorde con la clasificación o valoración del incidente, deberá brindarse atención acorde al nivel.

URGENCIA	Descripción
Extremo, Alto	El incidente de seguridad de la información debe atenderse de forma inmediata (0 - 120) minutos
moderado	El incidente de seguridad de la información debe atenderse de forma inmediata (0 - 240) minutos
Bajo	El incidente de seguridad de la información debe atenderse de forma inmediata (0 - 1440) minutos

Tabla 2: Nivel de Atención (Fuente Autor del documento**).**

3.1.5. Actuación frente al incidente

Una vez identificado y evaluado el incidente y definida la urgencia, las acciones a ejecutar**.**

TIPO	ZONA DE RIESGO	NIVEL DE ACEPTACION

Riesgos de Seguridad Digital (Proceso, Producto y Proyecto)	**Líder de Proceso**	• Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documental en el Plan de mejoramiento. • Iniciar el análisis de causas y determinar acciones • preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. • Analizar y actualizar el mapa de riesgos. • Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.

Tabla 3: Actuación frente al Incidente (Fuente Política Administración del Riesgo PT-SGI-01 27-02-2019 V. 04**).**

3.1.6. Equipos de Respuesta

Los equipos de respuesta que atiendan incidentes de seguridad que NO se consideren catastróficos, estarán conformados como mínimo por el propietario y/o custodio del activo, el Director de Tecnologías de la Información y las comunicaciones y su equipo que apoya la gestión de incidentes de seguridad de la información de la Gobernación y demás profesionales de los procesos de Recursos Tecnológicos o Sistemas Integrados de Información que tengan a cargo activos o servicios que se vean afectados por el mismo, además del Oficial de Datos Personales de la Dirección de Planeación y Control de Gestión que participará si se ve afectada una base de datos con datos personales. Para el caso de los incidentes de seguridad informática, el equipo de respuesta estará conformado por el propietario y/o custodio del activo, el profesional asignado por la Dirección de las Tecnologías de la Información y las Comunicaciones TIC que apoya la supervisión del servicio de seguridad informática, el profesional de la Dirección de las Tecnologías de la Información y las Comunicaciones TIC que apoya la supervisión del servicio afectado, el Especialista de TI del proveedor de servicios de TI del servicio afectado, el Gestor Seguridad Informática del proveedor de servicios de TI y el Oficial de Seguridad de la Información del proveedor de servicios de TI.
Los equipos que se conformen podrán solicitar información o la participación de otros colaboradores, procesos, especialistas y/o operadores estratégicos requeridos para la atención del incidente de seguridad.

En caso que un incidente de seguridad de la información se considere **CATASTRÓFICO**, se deberá informar al Líder del Eje (Director(a) de Información y Tecnología) la ocurrencia de dicho evento, quien deberá informar a la alta gerencia (Dirección y Secretaría General) para la instalación de la mesa de crisis, en donde se analizará los recursos financieros, humanos y tecnológicos correspondientes a

la atención de la emergencia, al igual evaluar las alternativas para la contención, erradicación y solución del incidente.

3.1.7. Marco normativo

- Modelo de seguridad y privacidad de la información – Ministerio de las TIC
- ISO/IEC 27001:2013.
- Política Administración del Riesgo PT-SGI-01 27-02-2019 V. 04
- Política Nacional de Seguridad Digital Compes 3854 de 2016

4.1.1. Formato para reporte formal de incidentes de seguridad de la información

Fecha y Hora del Reporte			
Nombre del Quien Reporta			
Cargo		Dependencia	
Correo Electrónico		Teléfono	

INFORMACION GENERAL DEL INCIDENTE	
Fecha y hora del Incidente	
Afectación a la Información	[ ]pérdida, [ ]daño, [ ] acceso no autorizado, [ ]alteración
Lugar donde se presentó el Incidente	
Descripción del Incidente	
En este campo se deben detallar los sucesos asociados al incidente como: • Situación que generó la sospecha de incidente. • Persona o personas que se vieron afectados en el incidente. • Acciones tomadas después de identificada la sospecha de incidente. Características que puedan ayudar al análisis de incidentes como: ventanas emergentes, bloqueos de pantalla, comportamientos extraños en los equipos de cómputo, personal sospechoso, etc.	
Relación de Evidencias(Describa el tipo de evidencia que adjunta o relaciona)	
Evidencia No. 1:	
Evidencia No. 2:	
Evidencia No. 3:	
Evidencia No. 4:	
Evidencia No. n:	
Nota: conserve este formato y las evidencias como acervo probatorio en una posterior investigación	

4.1.2. Metodología para el Informe Incidente de Seguridad de la Información

El presente informe deberá ser generado una vez concluida la investigación del incidente de seguridad de la información, por el Oficial de Seguridad de la Información de la Gobernación de Casanare o quien haga sus veces en colaboración con el equipo investigador.

METDOLOGIA Y CONTENIDO DEL INFORME

1. METODOLOGÍA DE LA INVESTIGACIÓN

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

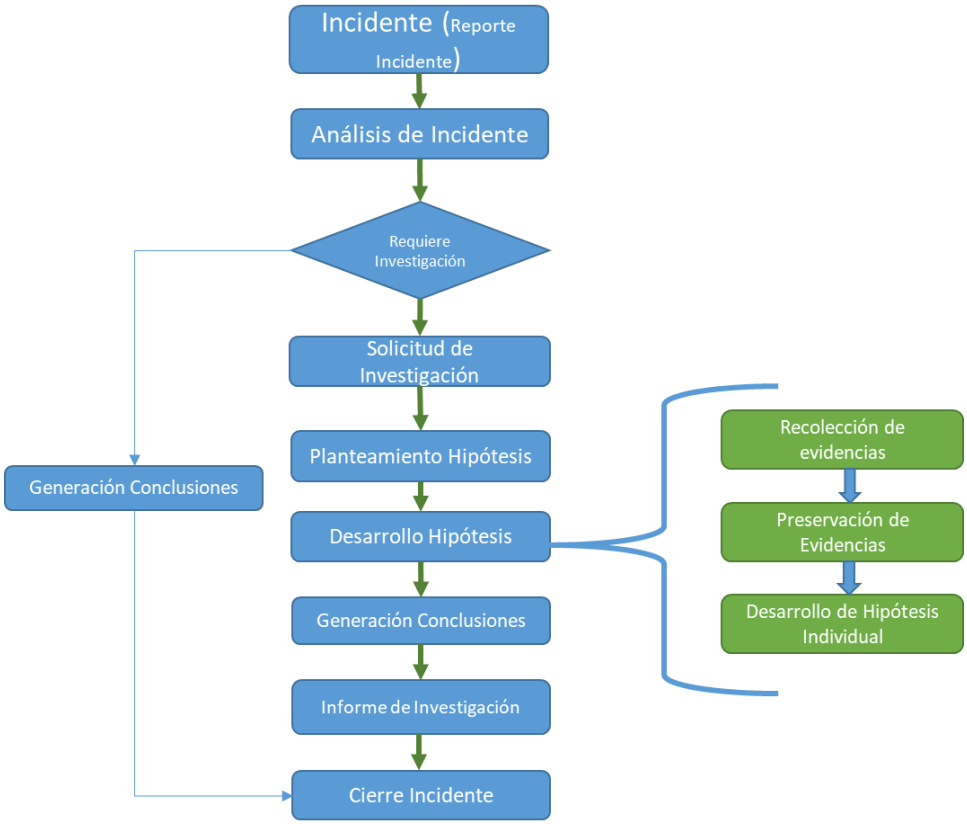

Imagen 1: Metodología desarrollada durante la investigación de causa raíz

a. **Incidente o Evento ocurrido a investigar:** Basado en el reporte del incidente, se identificara y procede a su evaluación.
b. **Análisis de Incidente:** Se identifica el tipo de incidente, acorde a la categorización, la clasificación e impacto y se determina si se requiere realizar investigación al incidente.
c. **Generar Conclusiones:** Cuando el resultado del análisis arroje que no se requiere investigación, se procederá a generar conclusiones y se realiza cierre del incidente.
d. **Solicitud de investigación:** Si el análisis del incidente arroja que se requiere realizar una investigación, la Dirección de tecnologías de la información y las comunicaciones TIC formalizara una solicitud para la entidad para que se autorice las acciones necesarias para realizar investigación del evento de interés ocurrido, la entidad deberá conformar un equipo interdisciplinario acorde al evento ocurrido y proceder a la generación de hipótesis.
e. **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.

f. **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.

g. **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.
h. **Informe de Investigación:** Se formula el presente informe, resultado de la investigación para su proceso de cierre con respecto a la investigación.
i. **Cierre del Incidente:**

2. INFORME DEL INCIDENTE

2.1. OBJETIVO
2.2. FECHA DE CREACIÓN
2.3. EQUIPO INVESTIGADOR
2.4. ANÁLISIS DEL EVENTO
2.4.1. Identificación del evento
2.5. HIPÓTESIS PLANTEADAS
2.6. DESARROLLO DE LAS HIPÓTESIS
2.6.1. Hipótesis 1:
2.6.2. Hipótesis 2:
3.1.1. HIPÓTESIS 3:
2.7. CONCLUSIONES
2.8. LISTADO DE EVIDENCIAS

EVIDENCIAS	DESCRIPCIÓN	LINK	SUMA DE VERIFICACIÓN

2.9. ANEXOS

Nombre del Documento	Ubicación

2.10. POSTULACIONES

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

Si ☐

No ☐ ¿Por qué? _____

¿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.

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.

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: Desarrolle la hipótesis planteada.

HIPÓTESIS 2: Desarrolle la hipótesis planteada.

HIPÓTESIS 3: Desarrolle la hipótesis planteada.

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: (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 la ruta donde se encuentra ubicado.

Registre un anexo por fila. Adicione cuantas filas necesite.	

POSTULACIONES: (Obligatorio), 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 Dirección de tecnologías de la información y las comunicaciones TIC 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 Dirección de tecnologías de la información y las comunicaciones TIC que apoya la supervisión del servicio asociado al Incidente, o del Profesional responsable de los sistemas misionales y apoyo de la Oficina de Sistemas de Información.

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