1. Objetivo

Gestionar cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz, minimizando el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantenga.

Objetivos Específicos:

- Minimizar el impacto del negocio ante la materialización de un incidente de seguridad de la información.
- Definir los roles y responsabilidades asociados a la gestión de incidentes de seguridad.
- Establecer una metodología para la gestión de incidentes de seguridad usando como base las mejores prácticas de la industria

2. Alcance

Este documento establece las directrices para gestionar y definir las normas de tratamiento de incidentes de seguridad, tanto tecnológico como no tecnológico, con el objetivo de minimizar el riesgo, el impacto y prevenir futuras ocurrencias. También se especifican las áreas que deben ser notificadas sobre estos incidentes y los registros que deben mantenerse para respaldo y seguimiento. Aplica a todos los funcionarios, contratistas, proveedores y demás partes interesadas que accedan a la información o tengan vínculos laborales o contractuales con el Ideam.

3. Definiciones

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000)
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Autenticidad**: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Cadena de Custodia:** Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
- **Contención:** Evitar que el incidente siga ocasionando daños.
- **Erradicación:** Eliminar la causa del incidente y todo rastro de los daños.
- **Evento de seguridad:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2009].
- **Gestión de Incidentes:** Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.
- **Hash:** Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Impacto:** Consecuencias que produce un incidente de seguridad sobre la organización.

- **Incidente:** Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y/o prácticas de seguridad básicas.
- **Incidente de seguridad digital - Ciber incidente:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.
- **Infraestructura crítica cibernética:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.
- **Libros de estrategias:** Procedimientos documentados que tienen como objetivo trazar la ruta de acción ante un tipo de incidente específico.
- **Logs:** Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Recuperación:** Volver el entorno afectado a su estado natural.
- **Validación:** Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. Siglas

- **COLCERT:** Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia, que está a cargo del Viceministerio de Transformación Digital, para continuar articulando y coordinando a nivel nacional los aspectos de ciberseguridad a todos los sectores públicos y privados del país.
- **CSIRT:** (Computer Security lncident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés.
- **DRP:** Sigla en inglés (Disaster Recovery Plan) Plan de Recuperación ante Desastres de Tecnología:
- **IoCs:** son indicadores que se utilizan en la detección y respuesta a incidentes de seguridad informática.
- **MSPI:** Modelo de seguridad y privacidad de la información
- **NTC-ISO-IEC 27001:** Norma Técnica Colombiana ISO - Tecnología de la información. Técnicas de seguridad. Modelo de seguridad y privacidad de la información.

5. Normatividad

- **Constitución Política de Colombia**, artículos 15, 209 y 269.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- **Decreto 767 de 2022.** "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único

Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

- **Norma ISO/IEC 27001:2022:** Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
- **Guía Técnica Colombiana GTC-ISO/IEC 27035:** Esta norma proporciona un enfoque estructurado para detectar, reportar, evaluar y gestionar incidentes de seguridad de la información.

6. Responsables

- **Usuario Final / Mesa de Ayuda**: Son los disparadores del proceso, un usuario final puede ser un usuario técnico o no técnico que genere el reporte a la mesa de ayuda y/o al gestor de plataformas de seguridad.
- **Gestor de plataforma de Seguridad**: Responsable de gestionar y/o administrar plataformas de seguridad o procesos, como el administrador de la consola de antivirus, firewall o el CISO.
- **Canal de Respuesta del Incidente**: Medio por el cual se entablará una comunicación abierta y continua entre los diferentes responsables técnicos y no técnicos para dar solución ágil y oportuna al incidente.
- **Jefe Oficina de Informática**: Dueño de los diferentes procesos técnicos en caso de requerir activación de DRP para algún sistema critico afectado.
- **Especialista**: responsable técnico de alguna tecnología y/o plataforma para dar gestión a los requerimientos que se soliciten sobre la misma.
- **Tercero**: Empresa externa que brinda soporte de segundo o tercer nivel sobre la plataforma o aplicación afectada

Nota Importante: En caso de tener un evento o incidente de seguridad se debe diligenciar el registro **Reporte de Incidentes de Seguridad de la Información.** Para la gestión y atención por parte del encargado de gestión de incidentes en Ideam.

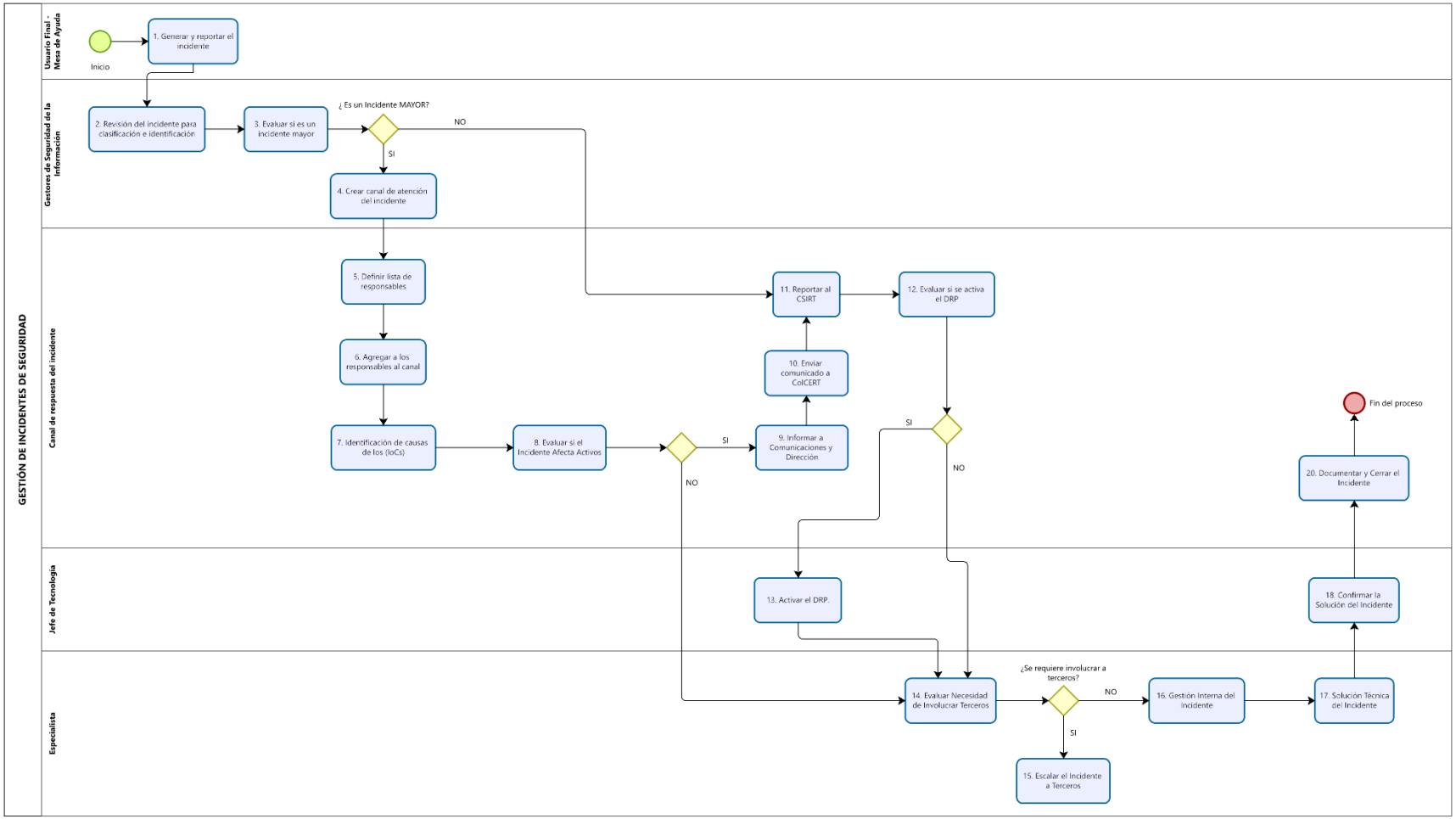
7. Documentos relacionados en el SGI

Política de seguridad y privacidad de la información

Manual de políticas complementarias de seguridad de la información

Formato para reporte de incidentes Ideam

DIAGRAMA DE FLUJO DEL PROCESO DE GESTION DE INCIDENTES DE SEGURIDAD



8. DESCRIPCION DE ACTIVIDADES DEL PROCESO

Tabla 1 Desarrollo de actividades Ciclo PHVA

No.	ACTIVIDAD	Ciclo PHVA	RESPONSABLE	DESCRIPCIÓN	PUNTOS DE CONTROL	TIEMPOS
1	Generar y Reportar el Incidente	P	Usuario Final o Mesa de Ayuda	Reporte mediante la mesa de servicio o correo electrónico.		N/A
2	Revisión del incidente para clasificación e identificación	P	Gestores de Seguridad de la Información	Clasificación del incidente según su naturaleza y gravedad.	Registro en sistema de seguimiento seguridadoti@ideam.gov.co mesadeservicio@ideam.gov.co	30 min
3	Evaluar si es un Incidente Mayor	P	Gestores de Seguridad de la Información	Se evalúa el impacto del incidente para determinar qué tipo de escenario del evento o incidente es. Es un incidente mayor: continuar con actividad 4.		30 min

No.	ACTIVIDAD	Ciclo PHVA	RESPONSABLE	DESCRIPCIÓN	PUNTOS DE CONTROL	TIEMPOS
				No es un incidente mayor: continuar actividad 11.		
4	Crear Canal de Atención del Incidente	H	Gestores de Seguridad de la Información	Crear un canal de comunicación para gestionar el incidente.		30 min
5	Definir Lista de responsables	H	Canal de Respuesta del Incidente	Definir los responsables para la gestión y solución del incidente.		N/A
6	Agregar a los responsables al Canal	H	Canal de Respuesta del Incidente	Incluir a los responsables en el canal de atención para coordinar las acciones.		N/A
7	Identificación de Causas (IoCs)	H	Canal de Respuesta del Incidente	Investigación y clasificación de las causas del incidente.	Mesa de Servicio	N/A
8	Evaluar si el Incidente Afecta	H	Canal de Respuesta del Incidente	Determinar si el incidente afecta activos críticos.		N/A

No.	ACTIVIDAD	Ciclo PHVA	RESPONSABLE	DESCRIPCIÓN	PUNTOS DE CONTROL	TIEMPOS
	Activos y corregir			Hay afectación: Proceder a corregir y continuar con actividad 9. No hay afectación: continuar actividad 14.		
9	Informar a Comunicaciones y Dirección	H	Canal de Respuesta del Incidente	Notificación a Comunicaciones y Dirección General, dependiendo del nivel de afectación.	Registro de notificación	N/A
10	Enviar Comunicado a ColCERT	H	Canal de Respuesta del Incidente	Informar a ColCERT si el impacto lo requiere.	Registro de notificación	N/A
11	Reportar al CSIRT	H	Canal de Respuesta del Incidente	Determinar si es necesario escalar el incidente al CSIRT para asistencia. En caso de ser necesario se registra el incidente en el canal	Registro de notificación	N/A

No.	ACTIVIDAD	Ciclo PHVA	RESPONSABLE	DESCRIPCIÓN	PUNTOS DE CONTROL	TIEMPOS
				correspondiente, de lo contrario continua con la actividad 12		
12	Evaluar si se Activa el DRP	H	Jefe de Oficina de Informática y Canal de Respuesta del Incidente	Analizar si la afectación requiere la activación del Plan de Recuperación ante Desastres (DRP). Requiere activación: continuar con actividad 13. No requiere activación: continuar actividad 14.		N/A
13	Activar el DRP	H	Jefe de Oficina de Informática	Activar el Plan de Recuperación ante Desastres y coordinar las acciones con las áreas tecnológicas para la recuperación.	Comunicación	N/A
14	Evaluar Necesidad de	H	Especialistas	Determinar si es necesario involucrar a terceros para la solución del incidente.	N/A	N/A

No.	ACTIVIDAD	Ciclo PHVA	RESPONSABLE	DESCRIPCIÓN	PUNTOS DE CONTROL	TIEMPOS
	Involucrar Terceros			Se requiere involucrar terceros: continuar con actividad 15. No se requiere involucrar terceros: continuar actividad 16.		
15	Escalar el Incidente a Terceros	H	Terceros	Escalamiento del incidente a proveedores externos para revisión y gestión.	Mesa de Servicio	N/A
16	Gestión Interna del Incidente	H	Especialistas	Gestión del incidente internamente si no se requiere escalar a terceros	N/A	N/A
17	Solución Técnica del Incidente	V	Especialistas	Resolución del incidente y restauración de servicios afectados	Verificación de solución	N/A
18	Confirmar la Solución del Incidente	A	Jefe de Oficina de Informática y Especialistas	Validar que el incidente ha sido solucionado y el entorno opera normalmente	Mesa de Servicio	N/A

No.	ACTIVIDAD	Ciclo PHVA	RESPONSABLE	DESCRIPCIÓN	PUNTOS DE CONTROL	TIEMPOS
20	Documentar y Cerrar el Incidente	A	Gestores de Seguridad	Documentar todo el proceso del incidente y cerrar el caso	Mesa de Servicio y Formato para reporte de incidentes Ideam	N/A

Fuente: Propia

9. HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción
01	11/07/2024	Documento nuevo perteneciente al Modelo de seguridad y privacidad de la información (MSPI)