1. OBJETIVO

Desarrollar las actividades para la atención y manejo de incidentes de seguridad que impactan los activos de información del Ministerio de Comercio, Industria y Turismo en cuanto a su disponibilidad, integridad, confidencialidad y privacidad, a través de la aplicación de mecanismos de contención, erradicación y recuperación de la infraestructura y servicios de TI.

2. ALCANCE

La gestión de incidentes de seguridad inicia con el reporte en la Mesa de Ayuda del incidente, continua con la implementación de las acciones de tratamiento, y finaliza con la documentación y cierre del caso. Aplica a todos los procesos del Ministerio.

3. DEFINICIONES Y SIGLAS

- **ACTIVO:** Cualquier elemento que tiene valor para la organización y que para Gestión de riesgos de seguridad de la información se consideran los siguientes: redes, hardware, información, ubicación, personal, procesos y actividades del negocio, software y estructura organizacional. [Fuente: ISO 27005] Cualquier cosa que tenga valor para la organización. [NTC 5411-1:2006]
- **ALCANCE:** Es el límite o grado en que se aplica un proceso, procedimiento, certificación, contrato, etc. Por ejemplo, el alcance de la gestión de incidentes puede cubrir activos como plataforma tecnológica e información del Ministerio de Comercio, Industria y Turismo.
- **CIERRE:** Es el acto público mediante el cual se da por finalizada la recepción de ofertas, en el lugar, fecha y hora señaladas en el pliego de condiciones; se procede a la apertura de la urna en donde se depositaron las ofertas.
- **CONFIDENCIALIDAD:** Propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos. Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **CONTENCIÓN:** Actividad(es) que busca(n) la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.
- **DISPONIBILIDAD:** Característica de seguridad de la información que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran asegurando su conservación durante el tiempo exigido por ley.
- **ERRADICACIÓN:** La erradicación de vulnerabilidades y amenazas consiste en la mitigación, reducción o eliminación de los eventos que puedan afectar los activos críticos de la organización, mediante una evaluación de los riesgos que puedan afectar activos, estableciendo unas acciones de mitigación para la protección de los activos y aplicando una serie de procedimientos y técnicas que permitan afrontar el riesgo de una manera eficaz.
- **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 la Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.
- **INCIDENTE DE SEGURIDAD:** Violación de lineamientos de seguridad de la información implícita o explícita.

- **INTEGRIDAD:** Característica técnica de seguridad de la información con la cual se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento asociados a la misma. Propiedad de salvaguardar la exactitud y estado completo de los activos. Propiedad de precisión y completitud. [Fuente: ISO 27000].
- **IMPACTO:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **MESA DE AYUDA:** Herramienta virtual que permite el registro, asignación y cierre de solicitudes de soporte técnico mediante el uso de tickets asignados a cada requerimiento. CENTRO DE ATENCIÓN AL USUARIO - HELP DESK ITIL V3 (Operación del Servicio). Punto de contacto para Usuarios para registrar Incidentes, está normalmente más técnicamente focalizado que un Centro de Servicio al Usuario y no proporciona un Punto Único de Contacto. El término Centro de Atención al Usuario es a menudo usado como sinónimo del Centro de Servicio al Usuario.
- **MITIGACIÓN:** El propósito de la mitigación de vulnerabilidades, es aplicar o ejecutar un conjunto de medidas para contrarrestar, minimizar, reducir o atenuar los daños o impactos potenciales sobre la infraestructura informática, sistemas de información o bienes causados por un evento.
- **PRIVACIDAD:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **RECUPERACIÓN:** La recuperación de datos e información, es el conjunto de técnicas y procedimientos utilizados para acceder y extraer la información almacenada en medios de almacenamiento digital que por daño o avería física o lógica no pueden ser accesibles de manera usual.

4. GENERALIDADES

4.1 Gestión de Incidentes de Información

La gestión de incidentes de seguridad y privacidad de la información es realizada a fin de contrarrestar de manera oportuna las amenazas que afecten los activos de información y contar con los registros de las acciones implementadas.

4.2 Normograma Proceso de Gestión de Información y Comunicación

Normas consideradas en la ejecución del procedimiento:

• Resolución 387 de 2012. Modifica la Resolución No. 3892 de 2011.
• Resolución 3892 de 2011. Modifica la Resolución No. 990 de 2008.
• Resolución 990 de 2008. Reglamenta el Manejo, Uso y Registro de los elementos informáticos del Ministerio.
• Resolución 2071 de 2016. Política de Tratamiento de Datos Personales MinCIT
• Conpes 3854 del 11 de abril de 2016. Política Nacional de Seguridad Digital.
• Conpes 3995 del 17 de julio de 2020, Política Nacional de Confianza y Seguridad Digital.
• ISO / IEC 27001: 2013. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos.

4.3 Uso y Apropiación.

• Aplicación y apropiación

El presente procedimiento y su documentación asociada son de aplicación y apropiación por parte de los Equipos de Seguridad Perimetral, Infraestructura Tecnológica, Grupo de Desarrollo y Mantenimiento de Aplicaciones, Grupo de Ingenierita y Soporte técnico, y Equipo de Seguridad y Privacidad de la Información de la Oficina de Sistemas de Información, encargados de la ciberseguridad, seguridad informática y seguridad y privacidad de la información de la infraestructura tecnológica, servicios tecnológicos y servicios de aplicación.

• Cambios y Actualización

Los cambios en el procedimiento y sus documentos asociados se realizan atendiendo los requerimientos de la gestión de incidentes; y su documentación se realizará en el Sistema Integrado de Gestión- SIG.

• Divulgación y Socialización

La divulgación del procedimiento y su documentación asociada se realiza en el Sistema Integrado de Gestión- SIG.
La interiorización de su aplicación se realiza a nivel de los equipos de trabajo de la Oficina de Sistemas de Información.

4.4 Roles y Responsabilidades de la Gestión de Incidentes

RESPONSABILIDADES				
R	Responsible	Responsable / Encargado	Quien efectivamente realiza la actividad
A	Accountable	Aprobador	Quien es responsable de que la actividad se realice y rende cuentas sobre su ejecución.
C	Consulted	Consultado	Quien posee la información o capacidad para realizar la actividad.
I	Informed	Informado	Quien debe ser informado sobre el avance y los resultados de la ejecución de la actividad.

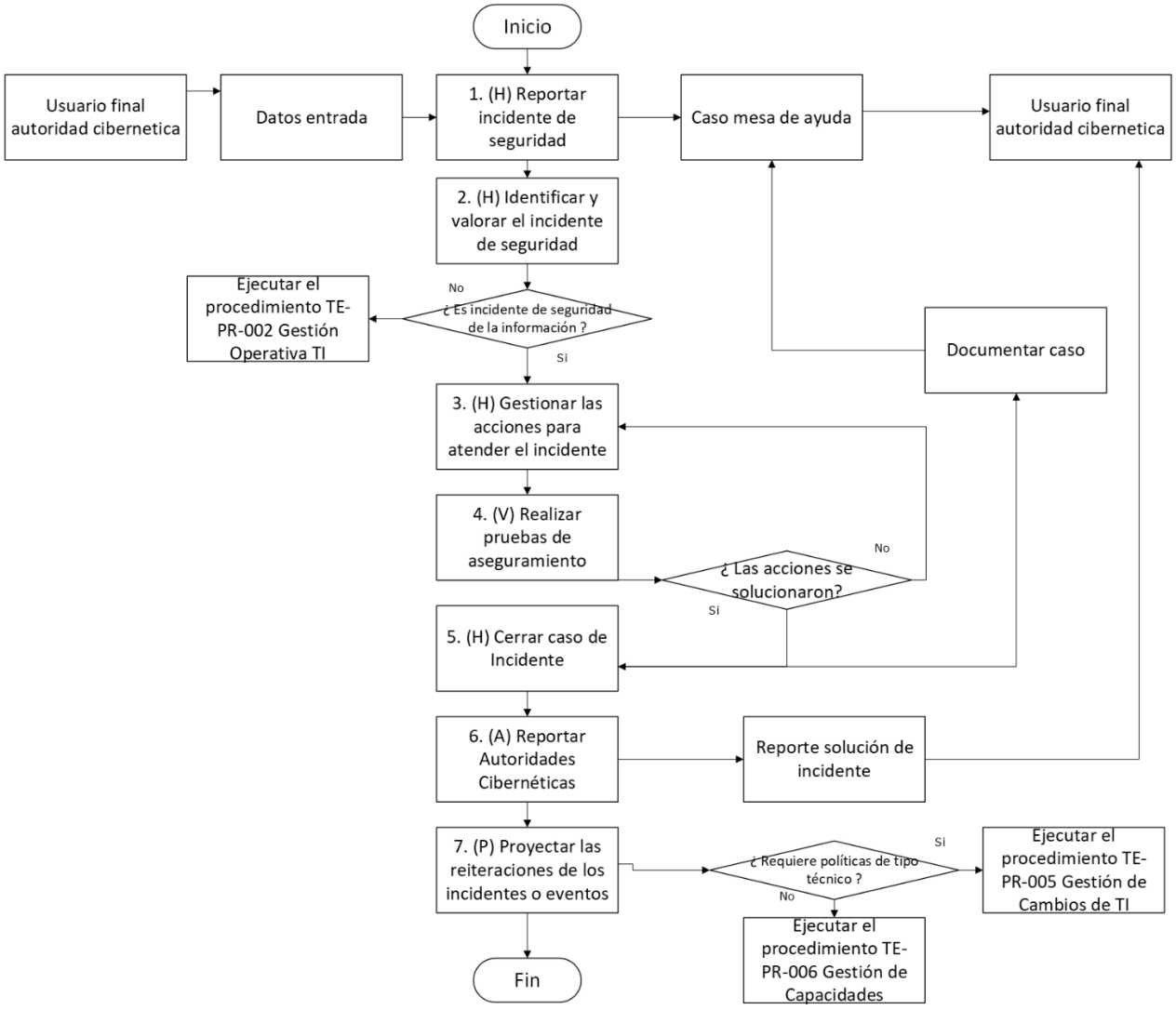
ROLES		Actividades													
		1	2	3	4	5	6	7							
		(H) Reportar incidente de seguridad	(H) Identificar y valorar el incidente de seguridad	(H) Gestionar las acciones para atender el incidente	(V) Realizar pruebas de aseguramiento	(H) Cierre del Incidente	(A) Reporte a Autoridades Cibernéticas	(P) Proyectar reiteraciones de incidentes							
Funcionario		R										I			
Contratista(s)		R										I			
Profesional TI (Gestor Sistema Información o Aplicativo)		R	C	I	R	C	I	R	C	I	C	I	C	I	C	I
Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones			R A	C	I	R A	C	I	R A	C	I	C	I	R A	I	R A	I
Coordinador Grupo Ingeniería y Soporte Técnico			R A	C	I	R A	I	R A	C	I	R A	C	I	R A	I	R A	I
Jefe Oficina Sistemas de Información			C	I	A	I	A	C	I	C	I	A	I	A	I	A	I
Personal Tercerizado	Soporte Técnico - Mesa de Ayuda	R	R A		R	I	R	C	C	R	C	I	C	C			
	SOC/NOC	R	C		R	I	R	C	C	R A	C	I	C	C			
	Infraestructura Tecnológica	R	C		R	I	R	C	C	R A	C	I	C	C			
Proveedor	Desarrollo de Software				R	I	R	C	C		C	I	C	C			
	Servicios Tecnológicos				R	I	R	C	C		C	I	C	C			
Oficial de Seguridad de la Información				I								I			

4.5 Riesgos

- Los riesgos del proceso se encuentran documentados en la matriz de riesgos institucionales.
- Los controles aplicables a cada riesgo se relacionan en las actividades descritas en los documentos y se identifican por medio del código del control.

5. DIAGRAMA DE FLUJO

(A continuación se visualiza de manera gráfica y secuencial las actividades descritas en el numeral 6)



6. DESCRIPCIÓN DE ACTIVIDADES

(A continuación se detallan las actividades graficadas en el numeral 5)

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
1	(H) Reportar incidente de seguridad	Funcionario, Contratista(s), Personal Tercerizado., Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones, Coordinador Grupo Ingeniería y Soporte Técnico	Realizar reportes a la Mesa de Ayuda por medio de: Mintranet> Servicios> Soporte Técnico (http://helpdesk.mincit.gov.co/USDK/Login.aspx/") Correo electrónico soportetecnico@mincit.gov.co Comunicándose a la extensión número 2291 La herramienta Mesa de Ayuda genera automáticamente para el incidente reportado un número de CASO. **Tiempo:** Permanente	Registro de Caso en la Herramienta de Mesa de Ayuda
2	(H) Identificar y valorar el incidente de seguridad	Coordinador Grupo Ingeniería y Soporte Técnico	Identificar y valorar el incidente de seguridad de la siguiente manera: 1. Determinar las características del incidente o evento reportado. 2. Valorar el incidente por Tipo de Servicio, determinar el Nivel de Criticidad y priorizar su tratamiento de acuerdo con la guía "TE-DR-008 Guía para el Análisis de Eventos e Incidentes de Seguridad y Privacidad de la Información". 3. Realizar el escalamiento al Rol Responsable según corresponda. Si el Evento es considerado "evento o incidente" continuar con la Actividad 3. De lo contrario ejecutar el procedimiento "TE-PR-002 Gestión Operativa TI" **Tiempo:** Permanente **Control 1 GTI-R4** **Control 2 RC-12**	Caso valorado en la Herramienta Mesa de Ayuda
3	(H) Gestionar las acciones para atender el incidente	Coordinador Grupo Ingeniería y Soporte Técnico, Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Personal Tercerizado.	Gestionar las acciones para atender el incidente de la siguiente manera: 1. Identificar las actividades previas o posteriores a realizar de acuerdo con la valoración efectuada. 2. Ejecutar las acciones de contención, erradicación, aislamiento o recuperación a implementar, atendiendo las indicaciones de la guía de Gestión de Incidentes. 4. Verificar la implementación de las acciones, continuar con la Actividad 4. 5. Reportar la efectividad de las acciones conforme se define en la "TE-DR-008 Guía para el Análisis de Eventos e Incidentes de Seguridad y Privacidad de la Información". **Tiempo:** Permanente	Caso Documentado Herramienta Mesa de Ayuda
4	(V) Realizar pruebas de aseguramiento	Personal Tercerizado., Coordinador Grupo Ingeniería y Soporte Técnico, Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones.	Confirmar que las acciones implementadas hayan dado solución al Incidente. Si se presentan elementos remanentes, o artefactos con resiliencia o amenazas persistentes después de haber aplicado las acciones de contención, volver a la Actividad 3.	Caso Documentado Herramienta Mesa de Ayuda

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
			En caso contrario continuar con la Actividad 5. **Tiempo:** Permanente **Control GTI-R4**	
5	(H) Cerrar caso de Incidente	Personal Tercerizado., Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico	Cerrar el caso en la Herramienta Mesa de Ayuda donde debe documentarse las acciones implementadas para dar solución al incidente. A través de la Herramienta Mesa de Ayuda se notifica el cierre del caso. **Tiempo:** Permanente	Cierre de Caso en la Herramienta Mesa de Ayuda, Correo electrónico
6	(A) Reportar Autoridades Cibernéticas	Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico	Reportar a Autoridades Cibernéticas - CSRIT Policía Nacional, ColCERT, CCOCI – Comando Conjunto Cibernético y CSIRT Gobierno – MinTIC -, la respuesta se debe realizar en el formato o sitio web dispuesto por estas entidades y de acuerdo con lo indicado en la "TE-DR-008 Guía para el Análisis de Eventos e Incidentes de Seguridad y Privacidad de la Información". Para respuesta de reportes de eventos o incidentes recibidos a través de Gestión Documental – PQRS, la respuesta o cierre de este tipo de comunicaciones deberá realizarse por el Jefe de la Oficina Sistemas de Información. **Tiempo:** Permanente	Registro de Reporte
7	(P) Proyectar las reiteraciones de los incidentes o eventos	Personal Tercerizado., Contratista(s), Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico	Realizar el seguimiento a las reiteraciones de incidentes con similar causa raíz para categorizarlos como problema y adelantar las acciones pertinentes a: 1. Definir, crear o ajustar políticas de tipo técnico, ejecutar el procedimiento "TE-PR-005 Gestión de Cambios de Tecnologías de la Información". 2. Adquirir, incorporar o actualizar tecnología, ejecutar el procedimiento "TE-PR-006 Gestión de la Capacidad de TI.". **Tiempo:** Permanente	TE-FM-013 Gestión de Cambios TE-FM-014 Gestión de Capacidad de TI Requerimientos

7. FORMATOS DEL PROCEDIMIENTO

No.	CODIGO	NOMBRE DEL FORMATO
1	TE-FM-013	Gestión de Cambios
2	TE-FM-014	Gestión de la capacidad TI- Requerimientos

8. HISTORIAL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
12/06/2026	0	Primera versión del documento para el nuevo Mapa de procesos. Código anterior: GTI-PR-004. V01. Para efectos de trazabilidad y soporte de la migración al nuevo aplicativo de administración de la documentación del Modelo Institucional de Operación (MIO), los siguientes fueron los responsables de la revisión y aprobación del documento migrado: REVISÓ: MARIA DEL ROSARIO CHACON HERRERA – Cargo: Profesional especializado OSI; IXEL RODRIGUEZ CORREA – Cargo: Profesional especializado OSI APROBÓ: EDGAR GREGORIO CARRILLO MONCADA – Cargo: Jefe OSI Desde la OAPS se asegura que el contenido corresponde a la última versión vigente en ISOlución al momento de la migración a MIOsoft.

9. FLUJO DE APROBACIÓN

ELABORÓ		APOYO OAPS		REVISÓ		APROBÓ	
Nombre:		Nombre:	Jefferson López Saavedra	Nombre:		Nombre:	
Cargo:		Cargo:	Profesional Especializado	Cargo:		Cargo:	