1. OBJETIVO

Definir acciones para identificar, analizar, clasificar, valorar y dar respuestas pertinentes en busca de la solución de los incidentes de Seguridad de la Información que se presenten.

2. ALCANCE

Inicia desde la detección de un incidente de Seguridad de la Información hasta que se da cierre en la herramienta de gestión de servicios de TI (Aplicativo Mesa de Ayuda).

3. RESPONSABILIDADES

PROFESIONAL DE GESTIÓN INFORMÁTICA Y COMUNICACIONES: encargado de gestionar los servicios de TI.
GESTOR DE MESA DE AYUDA: responsable de administrar la aplicación de la mesa de ayuda.
EQUIPO TÉCNICO DE SOPORTE: responsable de dar el soporte a los incidentes reportados en el primer nivel según lo escale la mesa de ayuda.
PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN: responsable de dar respuesta a los incidentes de Seguridad de la Información según lo escale la mesa de ayuda.

4. DEFINICIÓN DE TÉRMINOS

ACTIVO DE INFORMACIÓN: son todos los datos, sistemas o servicios que generan valor a la ETITC.

ATAQUE INFORMÁTICO: es un procedimiento técnico que tiene como objetivo tener acceso a un sistema de información de forma no autorizada o ejecutar malware en el mismo.

AMENAZA CIBERNÉTICA: aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854, pág. 87).

ATAQUE CIBERNÉTICO: acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (CONPES 3854, pág. 87).

BASE DE DATOS: es un conjunto de datos almacenados sistemáticamente y que son consultados mediante un sistema de información.

CERT (Computer Emergency Response Team): equipo de respuesta a emergencias cibernéticas.

CCOC: el comando conjunto cibernético se desempeña como unidad élite en aspectos relacionados con la ciberseguridad y ciberdefensa, incluida la protección de las Infraestructuras Críticas Cibernéticas Nacionales, desarrollando operaciones militares en el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional, contribuyendo a generar un ambiente de paz, seguridad y defensa nacional.

CIBERATAQUE: es cualquier tipo de actividad ofensiva realizada por personal malintencionado que comprometen los sistemas de información como la infraestructura, redes de datos y bases de datos que están alojadas en servidores institucionales. Generalmente estas actividades maliciosas son originadas desde fuentes anónimas y direcciones que no pueden ser rastreadas.

CIBERCRÍMEN (DELITO CIBERNÉTICO): conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).
Ciberespacio: red independiente de infraestructuras de tecnología de información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias. (Decreto 338 de 2022, pág. 5).

CIBERSEGURIDAD: es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (CONPES 3854, pág. 87).

CÓDIGO MALICIOSO: es un script o código que fue escrito para generar vulnerabilidades en un sistema de información.

COLCERT (COMPUTER EMERGENCY RESPONSE TEAM): grupo de respuesta a emergencias cibernéticas de Colombia.

CSIRT PONAL: equipo de respuesta a incidentes de seguridad informática de la Policía Nacional CSIRT-PONAL.

CSIRT DEFENSA: equipo de respuesta a incidentes de seguridad digital – Sector Defensa.

CSIRT EDUCACIÓN - equipo de respuesta ante incidentes de seguridad informática y ciberseguridad – Sector Educación

DATOS PERSONALES: son los datos o información que se relacionan con las personas y que los hace identificables.

DENEGACIÓN DEL SERVICIO: es una técnica que tiene como objetivo detener la operación de algún sistema de información.

ENTORNO DIGITAL: ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

ENTORNO DIGITAL ABIERTO: entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

INCIDENTE DIGITAL: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

INCIDENTE: interrupción no planificada de un servicio de TI o reducción de la calidad de un servicio de TI (ITIL v3).

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: cualquier evento que se presente y que afecte la confidencialidad, integridad o disponibilidad de los activos de información de la ETITC. (accesos a los sistemas de información, intrusiones, uso no autorizado, divulgación no autorizada, falsificación o destrucción no autorizada de la información).

MALWARE: software malicioso que tiene como objetivo infiltrarse en algún sistema de información sin autorización y de esta forma dañar o perjudicar al propietario de la misma.

MESA DE AYUDA: aplicación institucional en donde se registran todos los incidentes y servicios.
Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).

RIESGO DE SEGURIDAD DIGITAL: es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que pueden afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la autenticidad, confidencialidad, integridad y disponibilidad de la información, en cualquier medio de almacenamiento: impreso o digital, y la aplicación de procesos de resiliencia operativa.

VULNERABILIDAD: es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

5. REQUISITOS Y CONDICIONES GENERALES

Lineamientos de Seguridad de la Información:

9.5 Política de contacto con las autoridades y grupos de interés especial

9.7 Política de seguridad de la información en la gestión de proyectos.

9.15 Política para la planificación y preparación de la gestión de incidentes de seguridad de la información

9.16 Política de seguridad de la información durante una interrupción y preparación de las TIC para continuidad del servicio.

10.2 Política de proceso disciplinario

6. DESCRIPCIÓN DEL PROCEDIMIENTO

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
1.REGISTRAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN El usuario (propietario y/o custodio de la información) reporta el incidente de seguridad que identifique o reconozca a la mesa de ayuda de acuerdo al manual de políticas de SGSI de la ETITC, numeral 19.1 “Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información”.	Usuario (propietario y/o custodio de la información) Gestor de Mesa de Ayuda	N/A	Políticas aplicables de seguridad de la Información	Solicitud de ticket/caso en aplicativa mesa de ayuda
2.IDENTIFICAR Y CATEGORIZACIÓN DEL INCIDENTE El gestor de la mesa de ayuda se encarga de analizar e identificar el incidente con el fin de priorizar, categorizar como seguridad de la información de la información y asignarlo al Profesional de Seguridad de la Información	Gestor de Mesa de Ayuda	N/A	N/A	Ticket/caso en aplicativo mesa de ayuda
3. INFORMAR AL USUARIO Se informa al propietario y/o custodio de la información asociado al incidente para que no sea	Profesional de Seguridad de la Información	N/A	N/A	Correo electrónico.

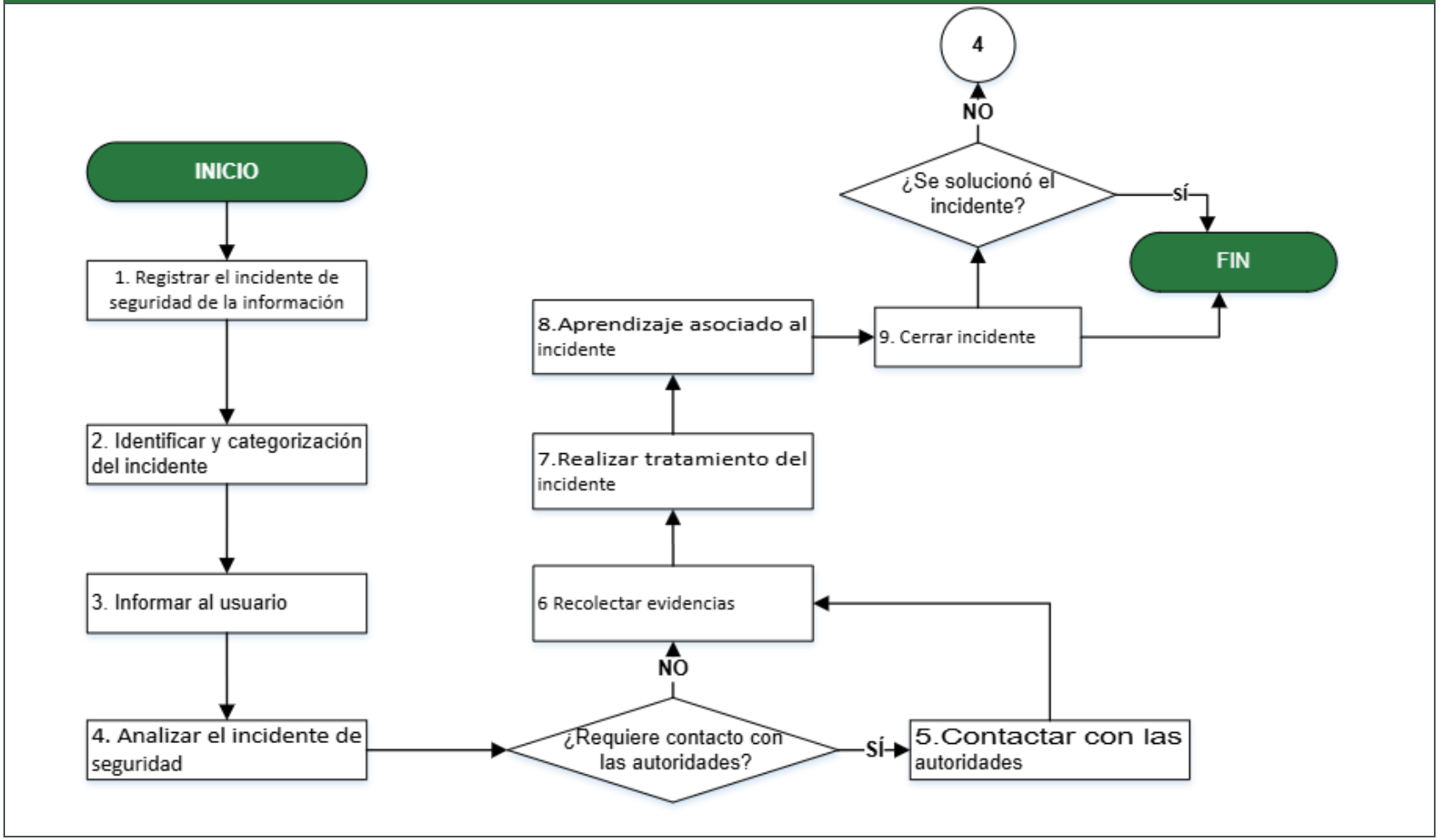
DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
manipulado el activo de información relacionado por él o por más personas de su área y otras recomendaciones.				
4. analizar el incidente de seguridad Ejecutar las actividades de análisis pertinentes en busca de la solución del incidente de seguridad. **NOTA** En caso de que el análisis determine que requiere contacto con las autoridades se continua con el paso 5, de lo contrario continúe con el paso 6.	Profesional de Seguridad de la Información	N/A	N/A	Histórico en la aplicativa mesa de ayuda
5. CONTACTAR CON LAS AUTORIDADES Contactar a las entidades externas oficiales que dan soporte a incidentes de seguridad de la información tales como la COLCERT, CSIRT de Gobierno, Fiscalía y DIJIN de acuerdo al procedimiento **GSI-SI -PC-06** Contacto con las autoridades.	Profesional de Gestión informática y Comunicaciones Profesional de Seguridad de la Información	N/A	**GSI-SI -PC-06**	Correo electrónico
6 RECOLECTAR EVIDENCIAS Se identifica, recolecta y documenta todas las evidencias asociadas al incidente de seguridad según el procedimiento: **GSI-SI-PC-01** Identificación, Recolección, Adquisición y Preservación de Evidencias	Profesional de Gestión informática y Comunicaciones Profesional de Seguridad de la Información	N/A	**GSI-SI -PC-01**	Evidencia física o digital identificada y recolectada
7.REALIZAR TRATAMIENTO DEL INCIDENTE El profesional de seguridad de la información en conjunto con el área de informática y	Equipo Técnico de Soporte	N/A	N/A	Histórico en el aplicativa mesa de ayuda

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
comunicaciones, desarrollaran las actividades necesarias para dar tratamiento al incidente de seguridad, documentando en la mesa de ayuda las actividades realizadas.	Profesional de Gestión informática y Comunicaciones Profesional de Seguridad de la Información			
8.APRENDIZAJE ASOCIADO AL INCIDENTE Se documenta todo el conocimiento adquirido asociado a la identificación, análisis y respuesta del incidente de seguridad con el fin de reducir la posibilidad y el impacto en futuros incidentes.	Profesional de Gestión informática y Comunicaciones Profesional de Seguridad de la Información	N/A	N/A	Histórico en el aplicativo mesa de ayuda por parte del responsable a dar gestión
9. CERRAR INCIDENTE **NOTA:** Si el incidente se solucionó finaliza el procedimiento y se procede a cerrarlo de acuerdo con el procedimiento GIT-PC-08 Gestión de Servicios TI. Ne se solucionó el incidente se devuelve a la actividad 4.	Gestor de Mesa de Ayuda	N/A	GIT-PC-08	Histórico en la aplicativa mesa de ayuda por parte del responsable a dar gestión

7.ANEXOS:

GSI-SI -PC-01 Procedimiento para la Identificación, Recolección, Adquisición y Preservación de Evidencias Digitales
GSI-SI -PC-06 Procedimiento contacto con las autoridades
GIT-PC-08 Gestión de Servicios de TI

8. DIAGRAMA DE FLUJO



9.SISTEMAS DE INFORMACIÓN			
SISTEMA DE INFORMACIÓN	**DESCRIPCIÓN**	**FRECUENCIA**	**UBICACIÓN**
Aplicativo de Mesa de Servicios (GLPI).	Aplicativo destinado para la solicitud, documentación y seguimiento de los requerimientos y solicitudes de tecnología.	Cuando se requiera.	https://mesadeayuda.etitc.edu.co/

10. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
2025-03-19	1	Se elimino el anexo GIC-PC-13 y se actualizo el código del procedimiento GIC-PC-08, también se incluyó el procedimiento GSI-SI -PC-06 PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES Migrado de la versión 2 del procedimiento GSI-PC-05 PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. en la transición de proceso de seguridad de la información a sistema qué compone el sistema de gestión de aseguramiento.

ELABORÓ	REVISÓ	APROBÓ
SANDRA GUERRERO G. Líder del Proceso de Seguridad de la Información	**ANAY PINTO VALENCIA** Administrador de la Documentación	**JORGE HERRERA ORTIZ** Jefe de oficina de planeación Institucional