## 1. OBJETIVO

Definir las actividades que permiten cumplir con una adecuada identificación, recolección, adquisición y preservación de las evidencias digitales de la Escuela Tecnológica Instituto Técnico Central (ETITC), cuando se reporte un incidente de seguridad que afecte la preservación de la confidencialidad, integridad y disponibilidad de los activos de información de la institución.

## 2. ALCANCE

Inicia con el reporte del incidente de seguridad de la información por parte de los servidores públicos y partes interesadas de la ETITC y finaliza con la entrega del informe final de la autoridad respectiva.

## 3. RESPONSABILIDADES

**SERVIDORES PÚBLICOS Y PARTES INTERESADAS:**

Deben reportar por correo electrónico al equipo de Mesa de Servicios (mesadeayuda@itc.edu.co), tomando captura de pantalla o marcando la opción en el menú indicado en el instructivo para reportar mensajes sospechosos de Microsoft 365, el posible incidente de seguridad de la información.

**GESTOR DE MESA DE SERVICIOS:**

Debe generar el respectivo ticket en el aplicativo de mesa de servicios (GLPI), haciendo uso de la categoría Gestión de Seguridad.

**PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN:**

Debe identificar la evidencia digital respectiva producto de la materialización del incidente de seguridad de la información reportado bajo el formato GSI-FO-06 Reporte de eventos e incidentes de seguridad de la información.

**PROFESIONAL DE GESTIÓN DE INFORMÁTICA Y TELECOMUNICACIONES:**

Debe identificar y recolectar la evidencia digital respectiva, producto de la materialización del incidente de seguridad de la información reportado bajo el formato GSI-SI-FO-06 Reporte de eventos e incidentes de seguridad de la información.

**ALTA DIRECCIÓN:**

Decide de acuerdo con la gravedad de los hechos, contactar con las autoridades externas bajo el procedimiento " GSI-SI -PC-06 Contacto con las autoridades"

**AUTORIDAD RESPECTIVA:**

Debe elaborar un informe final, donde se incluya los resultados de la investigación forense, dictando además las posibles soluciones del caso.

## 4. DEFINICIÓN DE TÉRMINOS

**EVENTO DE SEGURIDAD:** Es cualquier ocurrencia observable que sea relevante para la seguridad de la información. Esto puede incluir intentos de ataques cibernéticos o fallas que expongan vulnerabilidades de seguridad.

**INCIDENTE DE SEGURIDAD:** Es un evento de seguridad que resulta en daño o riesgo para los activos y operaciones de seguridad de la información.

**ADQUISICIÓN:** Proceso de realizar imágenes forenses para obtener copias binarias exactas del contenido de los objetos originales involucrados en la investigación.

**IDENTIFICACIÓN:** Reconocimiento de donde se haya la evidencia digital, sea física o lógica.

**IMAGEN FORENSE:** Copia binaria de la evidencia digital original.

**PRESERVACIÓN:** Aseguramiento de la integridad de la evidencia digital durante todo el proceso, ya sea la original o la copia.

**RECOLECCIÓN:** Acción de adquirir toda la información necesaria, que sirva de evidencia digital para su posterior análisis y tratamiento.

## 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. REPORTAR INCIDENTE.**<br><br>Los servidores públicos y partes interesadas reportan por correo electrónico al equipo de Mesa de Servicios (mesadeayuda@itc.edu.co), tomando captura de pantalla o marcando la opción en el menú indicado en el instructivo para reportar mensajes sospechosos de Microsoft 365, el posible incidente de seguridad de la información. | Servidores públicos y partes interesadas.<br><br>Gestor de Mesa de Servicios. | N/A | GSI-SI-FO-06 Reporte de eventos e incidentes de seguridad de la información. | Correo electrónico.<br><br>Aplicativo de Mesa de Servicios (GLPI). |
| **2. IDENTIFICAR EVIDENCIA**<br><br>Las áreas de Seguridad de la información y/o Informática y Telecomunicaciones, identifican la evidencia digital respectiva, producto de la materialización del incidente de seguridad de la información reportada. | Profesional de Seguridad de la Información.<br><br>Profesional de Gestión de Informática y Telecomunicaciones. | N/A | N/A | Evidencia digital identificada |
| **3. RECOLECTAR EVIDENCIA.**<br><br>Las áreas de Seguridad de la Información y/o Informática y Telecomunicaciones, recolectan la evidencia digital identificada a través de | Profesional de Seguridad de la Información. | N/A | N/A | Medio en el cual se recolecta la evidencia digital. |

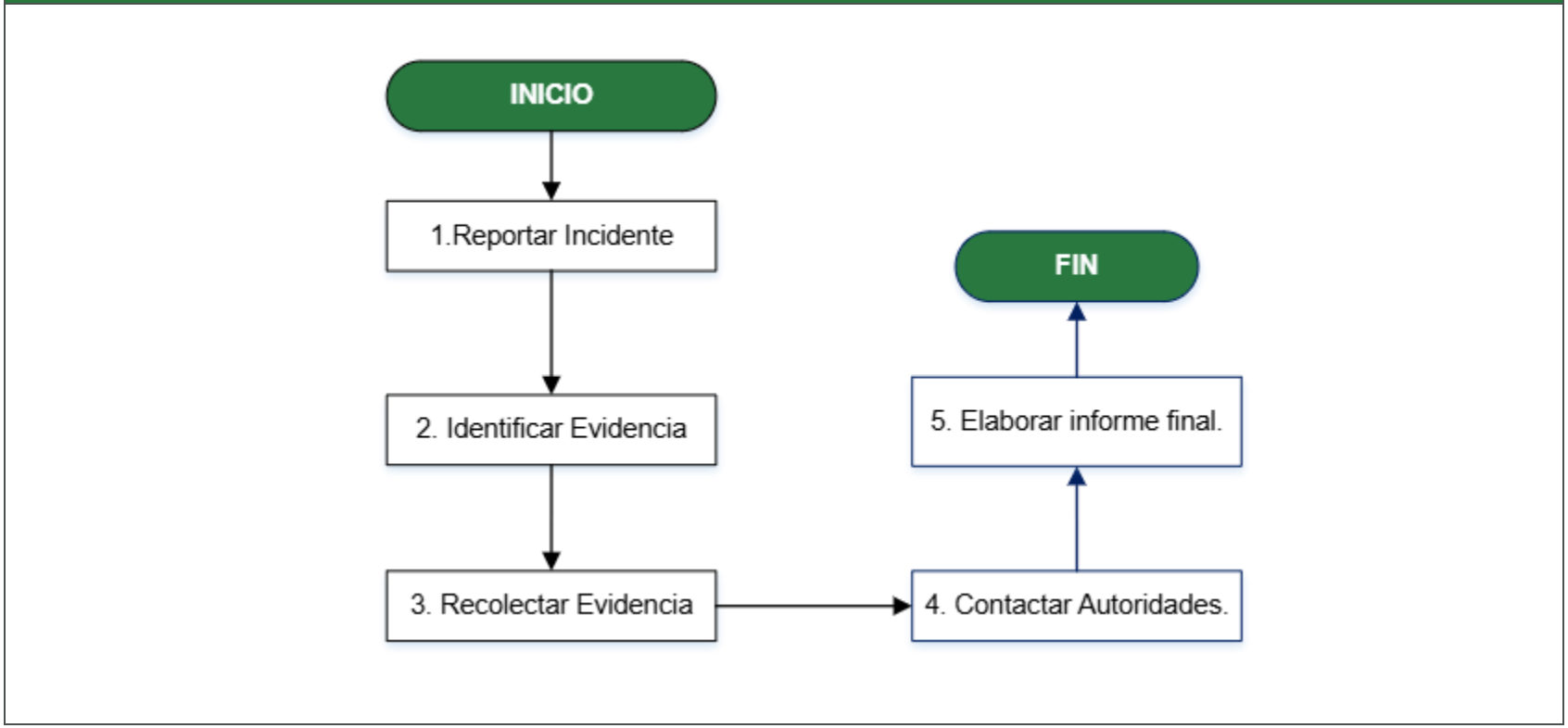
| DESCRIPCIÓN DE LA ACTIVIDAD | RESPONSABLE | CONTROL | DOCUMENTO DE REFERENCIA | REGISTRO RESULTANTE |
|---|---|---|---|---|
| GSI-FO-06 Reporte de eventos e incidentes de seguridad de la información. | Profesional de Gestión de Informática y Telecomunicaciones. | | | |
| **4. CONTACTAR AUTORIDADES.**<br><br>De acuerdo con el reporte de las áreas de Seguridad de la Información e Informática y Telecomunicaciones, la Alta Dirección pone en práctica el procedimiento GSI-PC-06 Contacto con las autoridades, con el fin de que la autoridad respectiva (ejemplo, Centro Cibernético Policial y/o Grupo CSIRT Gobierno, etc.) garantice la actividad de adquisición de la imagen forense (copia binaria de la evidencia digital original), para de esta forma hacer ISP de personal técnico especializado.<br><br>La autoridad respectiva debe garantizar la preservación de la integridad de la evidencia digital suministrada por la ETITC durante todo el proceso de investigación. | Alta Dirección. | N/A | GSI-SI -PC-06 Contacto con las autoridades | Imagen forense tomada por la autoridad respectiva. |

| DESCRIPCIÓN DE LA ACTIVIDAD | RESPONSABLE | CONTROL | DOCUMENTO DE REFERENCIA | REGISTRO RESULTANTE |
|---|---|---|---|---|
| **5. ELABORAR INFORME FINAL.**<br><br>La autoridad respectiva elabora un informe final, donde se incluye los resultados de la investigación forense, dictando además las posibles soluciones del caso. | Autoridad respectiva. | N/A | N/A | Informe final |

**7.ANEXOS:**

GSI-SI-FO-06 Reporte de eventos e incidentes de seguridad de la información.
GSI-SI -PC-06 Contacto con las autoridades

## 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 | Migrado de la versión 3 del procedimiento **GSI-PC-01** PROCEDIMIENTO PARA LA IDENTIFICACIÓN, RECOLECCIÓN, ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIAS DIGITALES. en la transición de proceso de seguridad de la información a sistema qué compone el sistema de gestión de aseguramiento. Se actualizaros los anexos: GSI-SI-FO-06 Reporte de eventos e incidentes de seguridad de la información. GSI-SI -PC-06 Contacto con las autoridades |

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