1. PROPÓSITO

Fortalecer la capacidad institucional para atender incidentes graves o muy graves de seguridad de la información (GSI-SI-PC-05), que requieran la recolección y gestión especializada de evidencia digital (por ejemplo, que conlleven investigaciones disciplinarias, administrativas o penales), garantizando que los procesos de identificación, preservación, adquisición, análisis, custodia, transporte y presentación de dicha evidencia se ejecuten de manera íntegra, trazable y legalmente admisible, en cumplimiento de la normativa vigente y en coordinación con las autoridades competentes (Ente de control, Fiscalía/Policía Judicial).

2. ALCANCE

Aplica a todos los activos de información y su entorno (en sitio, nube, computadores, móviles, correo, SaaS, respaldos, redes telemáticas y TO cuando aplique), a todo el personal (funcionarios, directivos, docentes, estudiantes y contratistas) y a terceros que en cumplimiento a objeto contractual hagan tratamiento de información de la ETITC.

3. MARCO NORMATIVO Y REFERENCIAS

- MSPI 2025 (Res. MinTIC 02277 del 3 de junio de 2025): adopta lineamientos acordes a la NTC ISO/IEC 27001:2022.
- Ley 1273 de 2009: base penal de los delitos informáticos (269A–269G, etc.).

4. GLOSARIO

- **Activo de Información:** Conocimiento o información que tiene valor para la ETITC.
- **Cadena de Custodia:** La cadena de custodia es el conjunto de procedimientos documentados que garantizan el control, la integridad, la autenticidad y la trazabilidad de la evidencia digital desde su recolección hasta su análisis, almacenamiento y disposición final, asegurando que no sea alterada ni manipulada de forma indebida.
- **Confidencialidad:** Asegurar que la información institucional, independientemente de su formato o medio, y en aquellos casos exceptuados por la Ley 1712 de 2014 sobre transparencia y acceso a la información pública, sea accesible únicamente por

personas, procesos o sistemas autorizados. Este principio se extiende tanto a datos administrativos como académicos, investigativos y de terceros.

- **Evidencia Digital:** Cualquier información almacenada o transmitida en formato digital que puede demostrar, respaldar o esclarecer hechos relacionados con un evento o incidente de seguridad de la información, y que debe conservarse de manera íntegra, auténtica y trazable para su análisis o uso posterior.
- **Hash:** Resultado de aplicar funciones matemáticas de cifrado (“Cryptography”) a un conjunto de datos, generando una cadena de longitud fija que sirve para verificar la integridad de la información, ya que cualquier modificación en los datos originales produce un valor de hash diferente.
- **Incidente de Seguridad de la Información:** Cualquier evento real o potencial que compromete o amenaza la confidencialidad, integridad y disponibilidad de la información de la ETITC, y que requiere atención y respuesta para mitigar sus efectos.

5. PRINCIPIOS

- Legalidad y admisibilidad (coordinación con Jurídica, Fiscalía y Policía judicial).
- Integridad y autenticidad (hash SHA-256/512; verificación previa y posterior a cada traslado/uso).
- Trazabilidad completa (registro cronológico y bitácora forense/cadena de custodia).
- Mínima manipulación (trabajo sobre imágenes forenses bit a bit, no sobre originales).
- Confidencialidad y no repudio (control de acceso, MFA, segregación de funciones, cifrado de repositorios).

6. RECOLECCIÓN Y GESTIÓN DE LA EVIDENCIA DIGITAL

Para aquellos incidentes de seguridad de la información que, debido a su naturaleza, requieran la adquisición y gestión especializada de evidencia digital, la ETITC deberá garantizar la atención por parte de personal idóneo y certificado, activando los servicios forenses amparados en póliza de ciberseguridad previamente contratada, con el fin de asegurar la integridad, trazabilidad y validez legal de la evidencia recopilada.

En caso de no contar con el amparo de una póliza se deberá hacer la inmediata contratación de una empresa especializada bajo la premisa de urgencia manifiesta. A manera de ejemplo y guía se sugiere la siguiente justificación para la debida gestión de la contratación:

"La contratación de un equipo forense especializado se justifica plenamente debido a que la ETITC actualmente no cuenta con las herramientas técnicas, los recursos operativos ni el personal certificado e idóneo necesarios para realizar adquisiciones forenses confiables, preservar la integridad de la evidencia digital y garantizar una cadena de custodia válida. La ausencia de capacidades internas representa un riesgo significativo para la admisibilidad legal, la trazabilidad, la confidencialidad y la veracidad de la evidencia en investigaciones disciplinarias, administrativas o penales. Un equipo forense externo aporta la experticia certificada, la infraestructura especializada y las metodologías reconocidas internacionalmente que aseguran que toda evidencia digital sea tratada con rigor técnico y jurídico, protegiendo así a la ETITC frente a fallos procesales, sanciones o responsabilidades derivadas de una gestión inadecuada."

7. REQUISITOS PARA LA GESTIÓN DE LA EVIDENCIA DIGITAL

Para asegurar una correcta gestión de la evidencia digital bajo controles formales, consistentes y alineados con la legislación vigente y estándares como el MSPI 2025 y la NTC ISO/IEC 27001:2022, el equipo forense externo podrá hacer uso de su propio procedimiento para el desempeño de sus labores. En todo caso se deberá respetar las siguientes fases del ciclo de vida de la evidencia:

Identificación y preservación inicial: Puede contener entre otras tareas como aislar cuando proceda (criterio de continuidad vs. preservación); capturar volátil (RAM, conexiones, procesos) antes de apagar/reiniciar; rotular y documentar lugar, fecha, responsable, condiciones; calcular el hash inicial del artefacto.

Adquisición forense: Por ejemplo, realizar imágenes bit a bit con herramientas autorizadas; registrar parámetros, versiones, hash de origen e imagen; para nube/correo/SaaS, usar exportaciones "forensic-friendly" conservando metadatos.

Custodia, almacenamiento y transporte: Ejemplo usar contenedores/embalajes que eviten alteración y daños ambientales; control de acceso con MFA; mantener bodega de evidencias con inventario, estantería segura, y registro de préstamos/transferencias; Cifrar repositorios de evidencia (p. ej., AES-256).

Análisis e informe: Laboratorio controlado; líneas de tiempo, correlación con tipos penales (Ley 1273 de 2009); informe pericial: objetivos, metodología, herramientas, resultados, hash, límites y anexos (cadena y capturas).

Entrega a autoridad: Acta formal de transferencia de custodia a ente autorizado, conservando copia forense cuando sea permitido y registro de hash.

8. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
31/03/2026	1	Emisión de la guía

ELABORÓ	REVISÓ	APROBÓ
JORGE A. TAMAYO REINEL Profesional de Seguridad de la Información	**JAVIER DIAZ MORALES** Profesional del Sistema de Gestión de Calidad	**YANETH JIMENA PIMIENTO CORTÉS** Líder del Proceso