

NORMA: NTC-ISO/IEC 27001: 2022 – ANEXO A. Control
A.8.8 Gestión de las vulnerabilidades técnicas.

AÑO: 2025

Los requisitos de planificación del programa de auditoría se desarrollan dando cumplimiento al procedimiento código SIG-PRO-007 Auditorías internas y externas para la revisión de procesos y OEC y al registro de este programa. La elaboración y presentación del informe de auditoría se hará una vez finalizada la auditoría.

La frecuencia de este programa es: Anual

Proceso/Unidad organizacional responsable de la auditoría: Sistema Integral de Gestión.

1. OBJETIVO DEL PROGRAMA:

Evaluar la capacidad de los controles de seguridad establecidos con el fin de proteger los activos de información de la Universidad Tecnológica de Pereira.

2. ALCANCE DEL PROGRAMA:

- Diferentes bases de datos de la infraestructura tecnológica del CRIE y GTISI.
- Aplicación de inscripciones.
- Sistema de votaciones
- Servidores de aplicaciones

3. CRITERIOS DE AUDITORÍA:

- Estándar OSSTMM (Open Source Security Testing Methodology Manual)
- Guías de Pruebas de OWASP.

4. MÉTODO DE AUDITORÍA:

Metodologías automatizadas y manuales para pruebas de seguridad ofensiva/Hacking Ético.

5. RECURSOS DE AUDITORÍA:

Humano: el equipo auditor lo integran expertos externos en seguridad informática. Tecnológicas: Herramientas OpenSource y Herramientas de pago según lo estimen los expertos.

6. SELECCIÓN DE LOS MIEMBROS DEL EQUIPO AUDITOR:

Servicio subcontratado con expertos en seguridad informática.



**SISTEMA INTEGRAL DE GESTIÓN
 FORMATO
 PROGRAMA DE AUDITORÍA INTERNA**

Código	1313-SIG-F15
Versión	1
Fecha	2025-07-14
Página	2 de 3

7. REQUISITOS DE PLANIFICACIÓN

Importancia de los procesos/ actividades involucradas.	Se auditará el proceso de Administración Institucional, específicamente al Centro de Recursos Informáticos y Educativos (CRIE) y Gestión de Tecnologías Informáticas y Sistemas de Información (GTIySI).
Resultados de auditorías previas.	Los hallazgos se han trabajado a través del formato del plan de mejoramiento derivado de las pruebas anteriores y retest a aplicaciones afectadas.
Cambios que afectan el proceso/ laboratorio.	Se tendrán en cuenta todas las acciones llevadas a cabo en el plan de mejoramiento relacionadas con las pruebas de vulnerabilidad.
Otro(s)	No aplica.

8. CRONOGRAMA DE AUDITORÍA

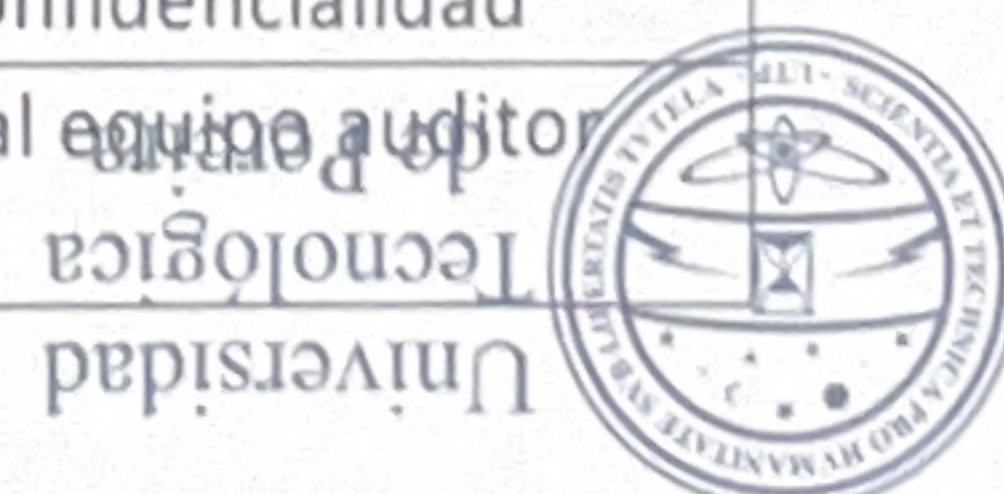
PROCESO	UNIDAD ORGANIZACIONAL/ FACULTAD/OEC	FECHA AUDITORÍA
Administración institucional	Gestión de Tecnologías Informáticas y Sistemas de Información	
Administración institucional	Recursos Informáticos y Educativos	

9. REQUISITOS DE LA NORMA A EVALUAR

NTC-ISO/IEC 27001: 2022. ANEXO A. Control A.8.8 Gestión de las vulnerabilidades técnicas.
--

10. OTROS ASPECTOS DE LA AUDITORÍA

Confidencialidad del equipo auditor:	Clausula presente en el contrato de prestación de servicios correspondiente al manejo de los derechos de autor y confidencialidad
Seguridad de la información por parte del equipo auditor:	La información suministrada por parte de los auditados al equipo auditor no se copia ni se transfiere a personal no autorizado.



SISTEMA INTEGRAL DE GESTIÓN
FORMATO
PROGRAMA DE AUDITORÍA INTERNA

Código	1313-SIG-F15
Versión	1
Fecha	2025-07-14
Página	3 de 3

Seguridad equipo auditor:	Cumplimiento de los protocolos de bioseguridad de la universidad.
Riesgos del programa de auditoría	Ver mapa de riesgos GSIC: Riesgo: "No ejecutar los programas de auditorías internas parcial o totalmente".

11. TESTIFICACIÓN ENSAYOS/CALIBRACIONES

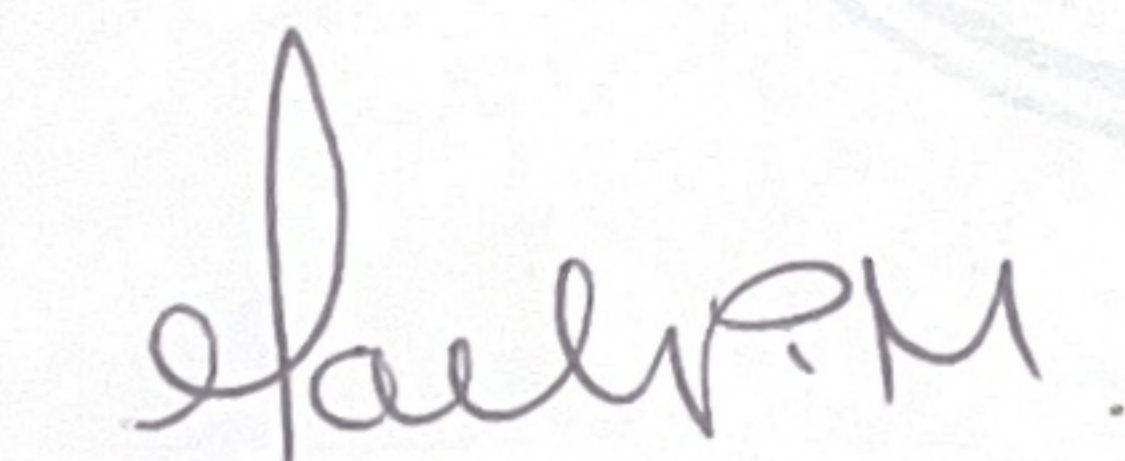
OEC	ENSAYO/CALIBRACIÓN	PRODUCTO O MATERIAL A ENSAYAR / INSTRUMENTO A CALIBRAR	OBSERVACIÓN
N/A	N/A	N/A	N/A

12.OBSERVACIONES

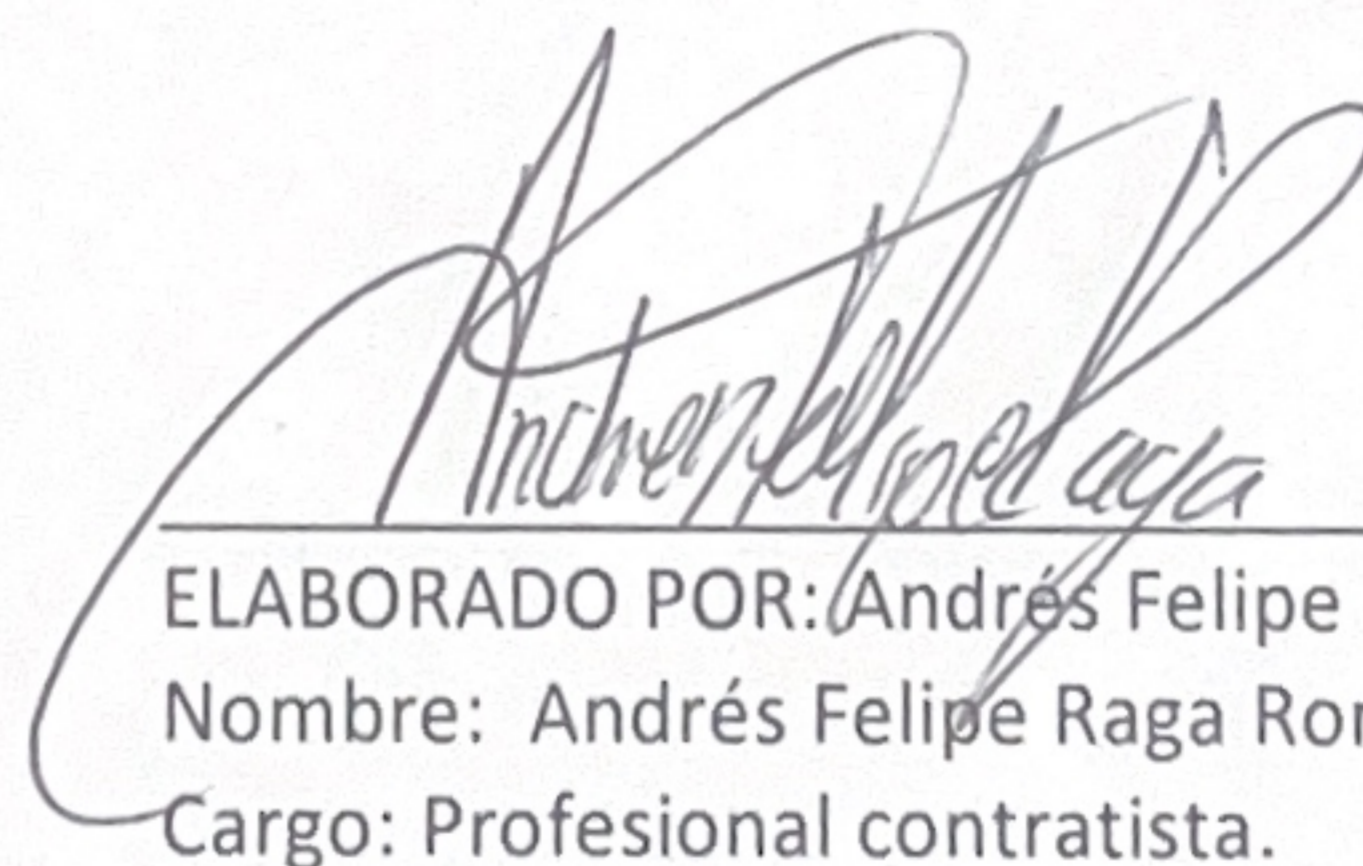
N.A.

Fecha elaboración: 15 octubre de 2025

Fecha actualización: 15 octubre de 2025



APROBADO POR: Gloria Yamile Parra Marín
Nombre: Gloria Yamile Parra Marín
Cargo: Profesional Especializado III



ELABORADO POR: Andrés Felipe Raga Romero
Nombre: Andrés Felipe Raga Romero
Cargo: Profesional contratista.