NORMA:	NTC-ISO/IEC 27001: 2013 – ANEXO A. Control A.12.6.1 Gestión de las vulnerabilidades técnicas.	AÑO:	2021

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

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:

Auditoria de seguridad a Centro de Recursos Informáticos y Educativos (CRIE): Red de gestión - Servicios Web - Bases de datos - Servicios DSN- RADIUS.

Auditoria de seguridad a Gestión de Tecnologías Informáticas y Sistemas de Información (GTIySI): - Nuevo software de pagos o Nuevo software de votaciones - Software de Contratación - Software Solicitudes de Compra - Software de salud o Software de extensiones.

El tiempo de duración es: 15 días

3. CRITERIOS DE AUDITORÍA:

- Procedimientos de las áreas de alcance.
- 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.

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.	Se realizará revisión al 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	DEPENDENCIA /ÁREA/ OEC	FECHA AUDITORÍA
Administración institucional	Gestión de Tecnologías Informáticas y Sistemas de Información	9 al 24 de noviembre.
Administración institucional	Recursos Informáticos y Educativos	

9. REQUISITOS DE LA NORMA A EVALUAR

NTC-ISO/IEC 27001: 2013. ANEXO A. Control A.12.6.1 Gestión de las vulnerabilidades técnicas.

10. OTROS ASPECTOS DE LA AUDITORÍA

Confidencialidad del equipo auditor:	Clausula Vigésima tercera. Derechos de autor y confidencialidad del contrato de prestación de servicios No.8823
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.
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

APROBADO POR:

Profesional IV

ELABORADO POR:

Profesional