



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código	SIG-FOR-007-01
Versión	12
Fecha	2023-06-08
Página	1 de 9

NORMA:

AÑO:

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:

Proceso/Unidad organizacional responsable de la auditoría:

1. OBJETIVO DEL PROGRAMA:

Contribuir a la mejora del Sistema Integral de Gestión de los laboratorios de ensayo y calibración de la Universidad Tecnológica de Pereira con base en los requisitos de la Norma ISO/IEC 27001:2022.

2. ALCANCE DEL PROGRAMA:

Se realizará auditoría interna con alcance a las áreas TIC, **Gestión de Tecnologías Informáticas y Sistemas de Información** (Arquitectura de Software, Administración de Servidores Especializados y Bases de Datos, Administración de Servicios Informáticos, Implementación del Sistema de Información Institucional, Renovación Tecnológica Institucional), **Recursos Informáticos y Educativos** (Administración de la red de datos y Administración del sitio Web Institucional), y **Gestión de Documentos** para verificar el cumplimiento de la Norma ISO/IEC 27001:2022.

3. CRITERIOS DE AUDITORÍA:

Se determina la conformidad frente:
-Norma ISO/IEC 27001:2022
-Procedimientos del Sistema Integral de Gestión.
-Requisitos legales.

4. MÉTODO DE AUDITORÍA:

-Realización de entrevistas.
-Completar lista de verificación con la participación del auditado.
- Verificación de Controles.
-Observación.

5. RECURSOS DE AUDITORÍA:



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código	SIG-FOR-007-01
Versión	12
Fecha	2023-06-08
Página	2 de 9

Humano: La Auditoría la llevará a cabo un Auditor líder externo.

Tecnológicos: Para la verificación de la aplicación de controles.

6. SELECCIÓN DE LOS MIEMBROS DEL EQUIPO AUDITOR:

Auditor líder con formación en:
ISO/IEC 27001:2022 – SGSI
ISO/IEC 27701:2019 – IIP

7. REQUISITOS DE PLANIFICACIÓN

Importancia de los procesos/ actividades involucradas.	Se auditarán los procesos de Administración Institucional y Aseguramiento de la Calidad Institucional
Resultados de auditorías previas.	Será la primera Auditoría que se le realiza al Sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27001.
Cambios que afectan el proceso/ laboratorio.	N.A.
Otro(s)	Ver ítem 10. Otros aspectos de la auditoría.

8. CRONOGRAMA DE AUDITORÍA

PROCESO	UNIDAD ORGANIZACIONAL/ FACULTAD/OEC	FECHA AUDITORÍA
Día 1		
Reunión apertura	Todos los procesos	2024/04/08 8:00 a 8:30 am
Aseguramiento de la Calidad Institucional.	Sistema Integral de Gestión. Estrategia	2024/04/08 8:30 a 9:10 am
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A.5 Controles organizacionales: Control Acceso / Identidad	2024/04/08 9:10 a 10:00 am
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos Gestión de Servicios Institucionales (Mantenimiento) A.7 Controles físicos	2024/04/08 10:00 a 11:00 am
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información.	2024/04/08 11:00 a 11:30 am



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código	SIG-FOR-007-01
Versión	12
Fecha	2023-06-08
Página	3 de 9

	Recursos Informáticos y Educativos Gestión de Servicios Institucionales (Mantenimiento) A.7 Controles físicos	
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A5 Controles organizacionales Activos	2024/04/08 11:30 am a 12:00 m
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos Gestión de Talento Humano Jurídica A6 Controles de personas Personas	2024/04/08 2:00 pm a 3:30 pm
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos Gestión de Talento Humano Jurídica A6 Controles de personas Personas	2024/04/08 2:00 pm a 3:30 pm
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos Sistema Integral de Gestión A5 Controles organizacionales: Gobierno	2024/04/08 3:30 pm a 5:45 pm
Día 2		
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A8 Controles Tecnológicos Protección Información	2024/04/09 8:00 a 9:10 am
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A8 Controles Tecnológicos Seguridad Sistemas	2024/04/09 9:10 a 10:30 am
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A.8 Controles tecnológicos Accesos	2024/04/09 10:30 a 11:00 am



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código	SIG-FOR-007-01
Versión	12
Fecha	2023-06-08
Página	4 de 9

Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A.5 controles organizaciones. Relación con Proveedores	2024/04/09 11:00 a 12:00 am
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A.8 Controles tecnológicos Seguridad Aplicación	2024/04/09 2:00 a 3:00 pm
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A.5 Controles organizacionales Gestión de eventos/Incidentes	2024/04/09 3:00 a 4:45 pm
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos A.8 Controles Tecnológicos Eventos / Vulnerabilidades técnicas	2024/04/09 4:45 a 5:00 pm
Administración Institucional	Gestión de Tecnologías Informáticas y Sistemas Información. Recursos Informáticos y Educativos Verificación de procesos de origen externo (out sourcing), cuyo resultado incide en el producto o servicio y que hacen parte del alcance de certificación.	2024/04/09 5:00 a 5:30 pm
Reunión de cierre	Todos los procesos	2024/04/09 5:30 a 6:00 pm

9. REQUISITOS DE LA NORMA A EVALUAR

Se van a Auditar los siguientes requisitos de la norma:



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código SIG-FOR-007-01

Versión 12

Fecha 2023-06-08

Página 6 de 9

PROCESOS	Administración Institucional											Aseguramiento de la calidad Ins.					
	Rectoría-Comunicación	Vice Adm Y Fin	Jardín Botánico	Facultades	Secretaría general	Gestión de documentos	Jurídica	Planeación	Gestión financiera (Compras)	Gestión TH	Gestión de servicios	Gestión TISI	Recursos Informáticos y edu	Vice Académica	Planeación	Sistema IG	Vice IIE
REQUISITOS NTC:ISO 27001:2022 UTP																	
CONTROLES ANEXO A ISO/IEC 27001:2022																	
A5 Controles Organizacionales												X	X				
5.1 Políticas de seguridad de la información												X	X				
5.2 Roles y responsabilidades en la Seguridad de la Información												X	X				
5.3 Segregación de deberes												X	X				
5.4 Responsabilidades de la dirección												X	X				
5.5 Contacto con las autoridades												X	X				
5.6 Contacto con grupos de interés especial												X	X				
5.7 Inteligencia de amenazas												X	X				
5.8 Seguridad de la Información en la gestión de proyectos												X	X				
5.9 Inventario de información y otros activos asociados												X	X				
5.10 Uso aceptable de la información y otros activos asociados												X	X				
5.11 Devolución de activos												X	X				
5.12 Clasificación de la información												X	X				
5.13 Etiquetado de la información												X	X				
5.14 Transferencia de información												X	X				
5.15 Control de acceso												X	X				
5.16 Gestión de identidades												X	X				
5.17 Información de autenticación												X	X				
5.18 Derechos de acceso												X	X				
5.19 Seguridad de la información en las relaciones con proveedores												X	X				
5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores												X	X				
5.21 Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información												X	X				
5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores												X	X				
5.23 Seguridad de la información para el uso de servicios en la nube												X	X				
5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información												X	X				
5.25 Evaluación y decisión sobre eventos de seguridad de la información												X	X				
5.26 Respuesta a incidentes de seguridad de la información												X	X				
5.27 Aprender de los incidentes de seguridad de la información												X	X				
5.28 Recopilación de evidencias												X	X				
5.29 Seguridad de la información durante una interrupción												X	X				
5.30 Preparación de las TIC para la continuidad de negocio												X	X				
5.31 Requisitos legales, legales, reglamentarios y contractuales Control												X	X				
5.32 Derechos de propiedad intelectual												X	X				
5.33 Protección de registros												X	X				
5.34 Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)												X	X				
5.35 Revisión independiente de la seguridad de la información												X	X				
5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información												X	X				
5.37 Procedimientos operativos documentados												X	X				



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código SIG-FOR-007-01

Versión 12

Fecha 2023-06-08

Página 7 de 9

PROCESOS	Administración Institucional													Aseguramiento de la calidad Ins.			
	Rectoría-Comunicaci	Vice Adm Y Fin	Jardín Botánico	Facultades	Secretaría general	Gestión de documentos	Jurídica	Planeación	Gestión financiera (Compras)	Gestión TH	Gestión de servicios	Gestión TISI	Recursos Informáticos y edu	Vice Académica	Planeación	Sistema IG	Vice IIE
REQUISITOS NTC:ISO 27001:2022 UTP																	
A6 Controles de Personas																	
6.1 Selección							X			X							
6.2 Términos y condiciones de empleo							X			X							
6.3 Conciencia de seguridad de la información, educación y formación												X	X			X	
6.4 Proceso disciplinario							X										
6.5 Responsabilidades después de la terminación o cambio de empleo							X			X		X	X			X	
6.6 Acuerdos de confidencialidad o no divulgación							X										
6.7 Trabajo remoto							X			X		X	X				
6.8 Informes de eventos de seguridad de la información												X	X				
A7 Controles físicos																	
7.1 Perímetros de seguridad física											X	X	X				
7.2 Entrada física											X	X	X				
7.3 Asegurar oficinas, habitaciones e instalaciones											X	X	X				
7.4 Monitoreo de la seguridad física											X	X	X				
7.5 Protección contra amenazas físicas y ambientales											X	X	X				
7.6 Trabajar en áreas seguras											X	X	X				
7.7 Escritorio y pantalla limpios												X	X				
7.8 Emplazamiento y protección de equipos											X	X	X				
7.9 Seguridad de los activos fuera de las instalaciones											X	X	X				
7.10 Medios de almacenamiento												X	X				
7.11 Servicios públicos de apoyo											X						
7.12 Seguridad del cableado											X	X	X				
7.13 Mantenimiento de equipos											X	X	X				
7.14 Disposición o reutilización segura de los equipos												X	X				



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código SIG-FOR-007-01

Versión 12

Fecha 2023-06-08

Página 8 de 9

PROCESOS	Administración Institucional													Aseguramiento de la calidad Ins.				
	Rectoría-Comunicación	Vice Adm Y Fin	Jardín Botánico	Facultades	Secretaría general	Gestión de documentos	Jurídica	Planeación	Gestión financiera (Compras)	Gestión TH	Gestión de servicios	Gestión TISI	Recursos Informáticos y edu	Vice Académica	Planeación	Sistema IG	Vice IIE	
REQUISITOS NTC:ISO 27001:2022 UTP																		
A8 Controles tecnológicos																		
8.1 Dispositivos de punto final de usuario												X	X					
8.2 Derechos de acceso privilegiado												X	X					
8.3 Restricción de acceso a la información												X	X					
8.4 Acceso al código fuente												X	X					
8.5 Autenticación segura												X	X					
8.6 Gestión de la capacidad												X	X					
8.7 Protección contra malware												X	X					
8.8 Gestión de vulnerabilidades técnicas												X	X					
8.9 Gestión de la configuración												X	X					
8.10 Eliminación de información												X	X					
8.11 Enmascaramiento de datos												X	X					
8.12 Prevención de fugas de datos												X	X					
8.13 Copia de seguridad de la información												X	X					
8.14 Redundancia de las instalaciones de procesamiento de información												X	X					
8.15 Registro												X	X					
8.16 Actividades de seguimiento												X	X					
8.17 Sincronización de reloj												X	X					
8.18 Uso de programas de utilidad privilegiados												X	X					
8.19 Instalación de software en sistemas operativos												X	X					
8.20 Seguridad de redes												X	X					
8.21 Seguridad de los servicios de red												X	X					
8.22 Segregación de redes												X	X					
8.23 Filtrado web												X	X					
8.24 Uso de la criptografía												X	X					
8.25 Ciclo de vida de desarrollo seguro												X	X					
8.26 Requisitos de seguridad de las aplicaciones												X	X					
8.27 Arquitectura de sistemas seguros y principios de ingeniería												X	X					
8.28 Codificación segura												X	X					
8.29 Pruebas de seguridad en el desarrollo y aceptación												X	X					
8.30 Desarrollo externalizado												X	X					
8.31 Separación de entornos de desarrollo, evidencia y producción												X	X					
8.32 Gestión del cambio												X	X					
8.33 Información de las pruebas												X	X					
8.34 Protección de los sistemas de información durante las pruebas de auditoría												X	X					



GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

PROGRAMA DE AUDITORÍA INTERNA

Código	SIG-FOR-007-01
Versión	12
Fecha	2023-06-08
Página	9 de 9

10. OTROS ASPECTOS DE LA AUDITORÍA

Confidencialidad del equipo auditor:	Firma del compromiso de 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, solo en caso de ser necesario como evidencia de la auditoría.
Seguridad equipo auditor:	N.A.
Riesgos del programa de auditoría	- Cambio de fecha por parte de los Jefes de área o dependencia, que conlleve a la no realización de la auditoría. - Conceder insuficiente tiempo para el desarrollo de la auditoría

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

Ninguna

Fecha elaboración: 2024/04/02

Fecha actualización: N.A.

APROBADO POR:

ELABORADO POR:

Cargo: Profesional Especializado III

Cargo: Profesional