					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P33					Título del documento: **Política de Auditoría y Supervisión del Cumplimiento**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 9.2, 9.3, 10	
ISO/IEC 27002:2022	Controles 5.35–5.37	
RGPD de la UE	Artículos 24, 32, 33	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
Directiva NIS2 de la UE	Artículo 21(2)(g), 27	
DORA de la UE	Artículos 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Propósito

1.1 El propósito de esta política es establecer y regular el programa de auditoría y supervisión del cumplimiento de la organización para:

1.1.1 Validar la eficacia de los controles de seguridad y privacidad.

1.1.2 Garantizar la alineación con las normas aplicables, los marcos regulatorios y las obligaciones contractuales.

1.1.3 Detectar de forma oportuna no conformidades, ineficiencias y riesgos de cumplimiento.

1.1.4 Apoyar la mejora continua y la preparación para certificaciones, evaluaciones y revisiones regulatorias.

1.2 Esta política respalda la integridad y madurez del Sistema de Gestión de la Seguridad de la Información (SGSI) mediante la incorporación de prácticas estructuradas de auditoría y supervisión, basadas en riesgos y sustentadas en evidencias.

2. Alcance

2.1 Esta política aplica a:

2.1.1 Todas las unidades de negocio, funciones y departamentos internos.

2.1.2 Instalaciones físicas, entornos en la nube, plataformas SaaS y servicios externalizados.

2.1.3 Sistemas de información, aplicaciones, infraestructura y activos de datos regidos por el SGSI.

2.1.4 Empleados, contratistas y proveedores de servicios externos con obligaciones de auditoría o cumplimiento.

2.2 La política cubre:

2.2.1 Auditoría interna.

2.2.2 Auditorías externas y de certificación.

2.2.3 Supervisión técnica del cumplimiento.

2.2.4 Auditorías de proveedores y terceros.

2.2.5 Acciones correctivas y preventivas (CAPA).

2.2.6 Métricas, cuadros de mando e informes.

2.3 Aplica a todos los marcos relevantes a los que la organización esté sujeta, incluidos ISO/IEC 27001, el RGPD de la UE, la Directiva NIS2 de la UE, DORA de la UE y SOC 2, entre otros.

3. Objetivos

3.1 Verificar la idoneidad y eficacia de los controles, políticas y procedimientos implantados en el SGSI y en los entornos relacionados.

3.2 Identificar y subsanar cualquier deficiencia, no conformidad o fallo de control antes de que escale a incidentes o incumplimientos.

3.3 Garantizar una preparación sostenida para revisiones internas de gobernanza, auditorías externas y certificaciones independientes.

3.4 Generar evidencias defendibles y trazas de auditoría en apoyo de requisitos regulatorios, procedimientos legales o solicitudes de aseguramiento por parte de clientes.

3.5 Integrar los resultados de auditoría en la gestión de riesgos, las métricas de seguridad y las actividades de mejora continua de la organización.

4. Funciones y responsabilidades

4.1 Responsable de Auditoría Interna / Responsable de Cumplimiento

4.1.1 Planifica, programa y ejecuta auditorías internas en función de la prioridad del riesgo.

4.1.2 Mantiene el Registro de Auditorías, coordina las actividades de auditoría y realiza el seguimiento de las acciones correctivas.

4.2 Director de Seguridad de la Información (CISO)

4.2.1 Garantiza que el alcance de la auditoría cubra todos los elementos relevantes del SGSI y los controles del Anexo A.

4.2.2 Supervisa la verificación de las CAPA e integra los resultados de auditoría en el programa de seguridad.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Esta política deberá revisarse al menos una vez al año por el Responsable de Cumplimiento y el CISO, o antes en respuesta a:

9.1.1 Cambios en marcos regulatorios, contractuales o de certificación.

9.1.2 Hallazgos de auditoría significativos o fallos de control reiterados.

9.1.3 Reestructuración organizativa o cambios en el sistema GRC.

9.1.4 Recomendaciones de auditores externos u observaciones de reguladores.

9.2 El proceso de revisión deberá evaluar:

9.2.1 La metodología y la frecuencia de planificación de auditorías.

9.2.2 Los cambios en el alcance del SGSI o en la infraestructura.

9.2.3 Las actualizaciones del catálogo de controles o del registro legal.

9.2.4 La coherencia y calidad de las evidencias de auditoría y de los procesos CAPA.

9.3 Todos los cambios en las políticas deberán:

9.3.1 Documentarse en un repositorio sujeto a control de versiones.

9.3.2 Ser aprobados por la alta dirección.

9.3.3 Comunicarse a todo el personal afectado e integrarse en los procedimientos actualizados y en los programas de concienciación.

9.4 La validación posterior a la revisión deberá confirmar que los requisitos actualizados se reflejan en el Registro de Auditorías, las herramientas de cumplimiento y los cuadros de mando internos de supervisión.

10. Políticas relacionadas y vinculaciones

10.1 Esta política se alinea con las siguientes políticas organizativas relacionadas:

10.1.1 P1 – Política de Seguridad de la Información: Define el SGSI y establece la responsabilidad proactiva sobre el cumplimiento y la mejora continua.

10.1.2 P5 – Política de gestión de cambios: Garantiza la visibilidad de auditoría sobre los cambios de infraestructura y configuración que afectan a los entornos de control.

10.1.3 P6 – Política de gestión de riesgos: Integra los resultados de auditoría en las actividades de evaluación y tratamiento de riesgos a nivel organizativo.

10.1.4 P14 – Política de conservación y eliminación de datos: Regula la conservación de evidencias de auditoría, registros y documentación de cumplimiento.

10.1.5 P18 – Política de Controles Criptográficos: Da soporte al almacenamiento y la transferencia seguros de datos sensibles de auditoría.

10.1.6 P26 – Política de Seguridad de Terceros y Proveedores: Cubre los derechos de auditoría, la documentación de aseguramiento y la supervisión del cumplimiento de proveedores.

10.1.7 P30 – Política de Respuesta a Incidentes: Alinea las auditorías de los procesos de gestión de incidentes con los objetivos de aseguramiento del SGSI.

10.1.8 P32 – Política de Continuidad del Negocio y Recuperación ante Desastres: Exige la verificación de las pruebas de continuidad y del cumplimiento del DRP durante los ciclos de auditoría.

11. Normas y marcos de referencia

11.1 Esta política está alineada con normas globales y requisitos legales en materia de auditoría y validación continua del cumplimiento.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 9.2 – Auditoría interna: Exige auditorías periódicas del SGSI basadas en riesgos para evaluar la eficacia y la conformidad.

11.2.2 Cláusula 9.3 – Revisión por la dirección: Los resultados de auditoría deben incorporarse a la revisión estratégica y a la mejora.

11.2.3 Cláusula 10.1 – No conformidad y acción correctiva: Los hallazgos de auditoría deben abordarse mediante procedimientos CAPA documentados.

11.3 ISO/IEC 27002:2022 – Controles 5.35–5.37:

11.3.1 Controles del Anexo A 5.35–5.37: Cubren la revisión independiente, el cumplimiento de requisitos legales y contractuales, y el registro de auditoría.

11.3.2 Proporcionan orientación de implantación para planificar, ejecutar y mejorar los programas de auditoría y cumplimiento.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Evaluaciones de controles: Exige la revisión rutinaria de los controles de seguridad implantados.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): Se alinea con el seguimiento y la remediación de hallazgos de auditoría.

11.4.3 CA-7 – Supervisión continua: Da soporte a evaluaciones proactivas y automatizadas del cumplimiento.

11.5 RGPD de la UE (2016/679):

11.5.1 Artículos 24 y 32: Exigen evidencias de la implantación y eficacia de los controles de seguridad mediante estructuras de gobernanza apropiadas.

11.5.2 Artículo 33: Refuerza la necesidad de trazas de auditoría verificadas en la respuesta y notificación de brechas de seguridad de los datos.

11.6 Directiva NIS2 de la UE (2022/2555):

11.6.1 Artículo 21(2)(g): Exige la auditoría de políticas y procedimientos como parte de las medidas mínimas de gestión de riesgos de ciberseguridad.

11.6.2 Artículo 27: Las autoridades nacionales podrán realizar o exigir auditorías a entidades esenciales e importantes.

11.7 DORA de la UE (2022/2554):

11.7.1 Artículo 10(2)(e): Las entidades deben realizar auditorías internas y externas de las prácticas de gestión del riesgo de las TIC.

11.7.2 Artículo 25 – Requisitos de auditoría: Exige auditorías periódicas realizadas por auditores internos o externos independientes con visibilidad regulatoria.

11.8 COBIT 2019:

11.8.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Garantiza que la eficacia de los controles se verifique y se informe a los órganos de gobernanza.

11.8.2 MEA03 – Monitor, Evaluate and Assess Compliance: Exige la alineación de las prácticas de la organización con requisitos legales, contractuales y basados en normas.