					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P33S					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 aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 9.2, 10	auditorías internas, mejora continua y corrección de no conformidades
ISO/IEC 27002:2022	Controles 5.35, 5.37	revisiones internas programadas, revisiones independientes para procesos externalizados
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	evaluaciones de seguridad, monitorización continua, revisión, análisis e informes de auditoría
RGPD de la UE	Artículos 24 y 32	auditoría de medidas técnicas y organizativas, evidencias de la eficacia de los controles
Directiva NIS2 de la UE	Artículo 21(2)(f)	revisión proactiva y cumplimiento basado en evidencias
DORA de la UE	Artículo 10	gestión del riesgo de las TIC, supervisión e información
COBIT 2019	MEA01, MEA03	supervisión y evaluación de la conformidad, cumplimiento y preparación para revisiones de terceros

1. Propósito

1.1 Esta política establece el enfoque de la organización para la realización de auditorías internas, verificaciones de controles de seguridad y supervisión del cumplimiento. Garantiza que todos los controles, políticas, sistemas y proveedores de servicios estén sujetos a una revisión periódica y estructurada.

1.2 El propósito es detectar fallos de control, prevenir incumplimientos y demostrar diligencia debida de conformidad con ISO/IEC 27001, el RGPD de la UE y marcos relacionados.

1.3 Permite a las pymes mantener el control operativo y la preparación para la certificación, incluso sin una función de cumplimiento dedicada, mediante listas de verificación sencillas y repetibles, y hallazgos priorizados en función del riesgo.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los departamentos internos y proveedores de servicios externos con responsabilidades relacionadas con sistemas de TI, información de identificación personal (PII) y servicios críticos para las operaciones de la organización

2.1.2 Todos los controles y sistemas incluidos en el alcance del Sistema de Gestión de la Seguridad de la Información (SGSI)

2.1.3 Todas las auditorías internas, revisiones de controles de seguridad y verificaciones de cumplimiento, ya sean realizadas internamente o por un consultor externo, un cliente o un regulador

2.2 Esta política también se aplica a la recopilación de evidencias y la elaboración de informes para:

2.2.1 Auditorías de certificación y recertificación de ISO/IEC 27001

2.2.2 Auditorías de protección de datos de conformidad con el RGPD de la UE o con términos contractuales

2.2.3 Cuestionarios de seguridad impulsados por clientes o revisiones de diligencia debida

2.2.4 Cualquier revisión regulatoria o independiente en virtud de la Directiva NIS2 de la UE o del Reglamento DORA, cuando resulte aplicable

3. Objetivos

3.1 Garantizar que todos los controles y políticas clave se revisen periódicamente en cuanto a su eficacia y cumplimiento.

3.2 Mantener trazas de auditoría y registros de acciones correctivas para demostrar responsabilidad proactiva y mejora.

3.3 Preparar la certificación, la recertificación y los programas de aseguramiento para clientes (por ejemplo, ISO 27001, incorporación de proveedores).

3.4 Identificar deficiencias de control de forma temprana, permitiendo una corrección rápida antes de que los problemas escalen o provoquen incumplimientos.

3.5 Permitir que el Director General y el proveedor externo de TI coordinen las revisiones con una complejidad mínima, garantizando al mismo tiempo resultados defendibles.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Supervisa el programa de auditoría

4.1.2 Aprueba los planes y hallazgos de revisión interna

4.1.3 Asigna y supervisa las acciones correctivas

4.1.4 Autoriza la contratación de auditores o consultores externos

4.2 Proveedor externo de TI / Administrador

4.2.1 Proporciona evidencias durante auditorías internas y externas (por ejemplo, registros, configuraciones, registros de control de acceso)

4.2.2 Colabora en las verificaciones técnicas (por ejemplo, estado de las copias de seguridad, estado de cumplimiento de parches)

4.2.3 Mantiene el repositorio de evidencias de auditoría

[... 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 Revisión anual de la política y del plan de auditoría

9.1.1 El Director General (DG) debe revisar esta política y el calendario de auditoría al menos una vez al año.

9.1.2 La revisión debe evaluar:

9.1.2.1 la eficacia de las auditorías para identificar deficiencias de control

9.1.2.2 la tasa de finalización de las auditorías y de las acciones correctivas

9.1.2.3 los cambios en los requisitos legales, regulatorios o de certificación aplicables

9.2 Actualizaciones motivadas por eventos desencadenantes

9.2.1 La política debe revisarse y actualizarse cuando:

9.2.2 una auditoría de certificación o de seguimiento dé lugar a una no conformidad mayor

9.2.3 cambien los marcos legales o regulatorios (por ejemplo, nuevas directrices del RGPD de la UE, transposición nacional de NIS2)

9.2.4 los cambios en la organización afecten a los sistemas, procesos o proveedores incluidos en el alcance de auditoría

9.2.5 un incidente crítico o una brecha de seguridad revele deficiencias de control no detectadas previamente

9.3 Documentación de las actualizaciones

9.3.1 Todas las revisiones deben registrarse en un control de versiones de políticas

9.3.2 Las actualizaciones deben distribuirse a todos los miembros del equipo implicados en auditorías

9.3.3 Debe incluirse un resumen de cambios con la política actualizada para garantizar su comprensión

10. Políticas relacionadas y vinculaciones

10.1 Esta política se apoya en otras políticas de la pyme y las refuerza:

10.1.1 P1S – Política de Seguridad de la Información: establece la base de todas las expectativas de control y exige su verificación mediante auditorías.

10.1.2 P2S – Política de funciones y responsabilidades de gobernanza: establece la responsabilidad proactiva para la planificación de auditorías, su ejecución y la titularidad de las acciones correctivas.

10.1.3 P6S – Política de gestión de riesgos: identifica debilidades de control detectadas en auditorías y garantiza que los hallazgos se documenten en el Registro de Riesgos.

10.1.4 P17S – Política de Protección de Datos y Privacidad: define los controles del RGPD de la UE que deben auditarse, incluidos el tratamiento de datos, la respuesta ante brechas de seguridad y los avisos de privacidad.

10.1.5 P22S – Política de registro y supervisión: proporciona los registros de auditoría y los datos forenses utilizados durante las revisiones de cumplimiento y de controles.

10.1.6 P30S – Política de Respuesta a Incidentes: exige la auditoría periódica de los registros de incidentes y las revisiones posteriores a los eventos para verificar la eficacia de la respuesta.

10.1.7 P31S – Política de Recopilación de Evidencias y Análisis Forense: proporciona los procedimientos para recopilar evidencias verificables con cadena de custodia durante las auditorías.

10.2 En conjunto, estas políticas crean un entorno de control de ciclo cerrado que permite la verificación interna, el aseguramiento externo y una gobernanza alineada con normas.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:

11.1.1 cláusula 9.2: requiere auditorías internas para evaluar el desempeño del SGSI y su alineación con los requisitos.

11.1.2 cláusula 10.1: exige la mejora continua basada en los resultados de auditoría y la corrección de no conformidades.

11.2 ISO/IEC 27002:

11.2.1 control 5.35: exige revisiones internas programadas de controles y procesos.

11.2.2 control 5.37: enfatiza las revisiones independientes, especialmente para procesos externalizados.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – evaluaciones de seguridad: exige auditorías de los controles implantados para verificar su eficacia.

11.3.2 CA-7 – monitorización continua: enfatiza la detección proactiva y la revisión de debilidades de control.

11.3.3 AU-6 – revisión, análisis e informes de auditoría: exige el análisis periódico y la resolución de registros y hallazgos de auditoría.

11.4 RGPD de la UE:

11.4.1 artículos 24 y 32: exigen la implantación y auditoría de medidas técnicas y organizativas, incluidas evidencias de la eficacia de los controles y de la mejora a lo largo del tiempo.

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

11.5.1 artículos 20–21: exigen revisión proactiva de controles, cumplimiento basado en evidencias y capacidad de auditoría para entidades esenciales e importantes.

11.6 COBIT 2019:

11.6.1 MEA01 – supervisar, evaluar y valorar el desempeño y la conformidad: exige la evaluación periódica del desempeño de procesos y controles frente a normas y objetivos.

11.6.2 MEA03 – garantizar el cumplimiento de requisitos externos: se centra en la supervisión interna y la preparación para auditorías de terceros y revisiones regulatorias.