					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P27S					Título del documento: **Política de Uso de la Nube**							
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	Cláusula 8	
ISO/IEC 27002:2022	Controles 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
RGPD de la UE	Artículo 28, 32 y capítulo V	
Directiva NIS2 de la UE	Artículos 21(2)(f), (i)	
DORA de la UE	Artículos 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Finalidad

1.1 Esta política define cómo pueden utilizarse de forma segura los servicios en la nube dentro de la organización. Garantiza que los datos tratados o almacenados en la nube estén protegidos, que el acceso esté controlado y que los riesgos se gestionen de forma responsable.

1.2 Ayuda a las pymes a cumplir las obligaciones legales y las expectativas de los clientes en materia de protección de información sensible, prevención de fugas de datos y gestión eficaz de los riesgos asociados a la nube, sin requerir una infraestructura de escala empresarial.

1.3 Esta política respalda la certificación ISO/IEC 27001, el cumplimiento del RGPD de la UE y el aseguramiento de la cadena de suministro mediante una gobernanza coherente de todos los servicios en la nube de terceros.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Cualquier servicio en la nube utilizado para almacenar, tratar o transmitir datos de la organización

2.1.2 Todo el personal, contratistas o proveedores de servicios que utilicen herramientas en la nube en nombre de la organización

2.1.3 Soluciones en la nube gratuitas y de pago, incluidas plataformas de correo electrónico, uso compartido de documentos, herramientas SaaS, plataformas de copia de seguridad, videoconferencia y plataformas de clientes

2.1.4 Cualquier dispositivo (equipo de sobremesa, móvil o tableta) que acceda a información de la organización a través de aplicaciones en la nube

2.2 Esto incluye, entre otros:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Herramientas de copia de seguridad y recuperación ante desastres basadas en la nube

2.2.5 Carpetas compartidas o aplicaciones utilizadas para facturación, gestión de proyectos o comunicación con clientes

3. Objetivos

3.1 Prevenir el uso no autorizado o de alto riesgo de servicios en la nube no aprobados.

3.2 Garantizar que los datos sensibles o regulados almacenados en la nube estén protegidos mediante controles técnicos y organizativos adecuados.

3.3 Definir responsabilidades claras para la aprobación, configuración, supervisión y retirada de servicios en la nube.

3.4 Controlar los flujos de datos y aplicar los requisitos de conservación, eliminación y privacidad sobre la información almacenada en la nube.

3.5 Reducir la dependencia de cuentas personales o herramientas no gestionadas exigiendo la aprobación de todos los sistemas en la nube utilizados con fines profesionales.

3.6 Cumplir los requisitos de ISO/IEC 27001:2022, RGPD de la UE, NIS2 y DORA para la gestión de dependencias externas de servicios en la nube.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba el uso de todos los nuevos servicios en la nube

4.1.2 Revisa los riesgos relacionados con los proveedores de servicios en la nube y los tipos de servicio

4.1.3 Hace cumplir esta política y supervisa las decisiones relativas a excepciones

4.2 Proveedor externo de TI o Soporte de TI

4.2.1 Evalúa e implanta una configuración segura para los servicios en la nube

4.2.2 Configura cuentas, controles de acceso y copias de seguridad

4.2.3 Supervisa el cumplimiento de los requisitos de contraseñas, autenticación multifactor y ajustes de configuración 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 debe revisarse al menos anualmente por el Director General, en coordinación con el proveedor externo de TI.

9.2 También debe realizarse una revisión formal:

9.2.1 Después de un incidente de seguridad relacionado con la nube (por ejemplo, violación de seguridad, pérdida de datos)

9.2.2 Cuando se introduzca una nueva plataforma principal en la nube

9.2.3 Si cambian los requisitos legales o reglamentarios (por ejemplo, actualizaciones del RGPD de la UE, NIS2 o DORA)

9.2.4 Si las actividades de supervisión revelan usos indebidos o nuevos riesgos

9.3 El Director General debe garantizar:

9.3.1 Que el Registro de Servicios en la Nube se actualice con servicios nuevos o retirados

9.3.2 Que los requisitos legales y de privacidad sigan cumpliéndose

9.3.3 Que todos los cambios se comuniquen a los usuarios y partes interesadas pertinentes

9.4 Las versiones archivadas deben almacenarse de forma segura, y las versiones anteriores de la política deben gestionarse conforme a la P14S – Política de conservación y eliminación de datos de la organización.

10. Políticas relacionadas y vinculaciones

10.1 Esta política debe utilizarse en coordinación con las siguientes políticas de seguridad de la información alineadas con las pymes:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: define la responsabilidad proactiva para aprobar servicios en la nube y gestionar las relaciones con proveedores.

10.1.2 P4S – Política de control de acceso: respalda las prácticas de inicio de sesión seguro, gestión de sesiones y revocación requeridas para las plataformas en la nube.

10.1.3 P14S – Política de conservación y eliminación de datos: regula cómo se realiza la copia de seguridad, conservación y eliminación de los datos basados en la nube de conformidad con las obligaciones legales.

10.1.4 P17S – Política de protección de datos y privacidad: garantiza que cualquier dato personal almacenado en servicios en la nube se trate de acuerdo con los principios del RGPD de la UE.

10.1.5 P30S – Política de respuesta a incidentes: proporciona procedimientos estructurados para responder a incidentes de seguridad en la nube, incluida la recopilación de evidencias y la notificación externa.

10.2 En conjunto, estas políticas garantizan que el uso de la nube sea seguro, conforme y operacionalmente resiliente.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 8.1 exige que las organizaciones implanten controles operativos para la gestión de datos, incluidos los relativos a sistemas basados en la nube.

11.2 ISO/IEC 27002

11.2.1 El control 5.23 exige la gobernanza del uso de servicios en la nube y herramientas SaaS de terceros.

11.2.2 El control 5.24 exige una política definida de uso de la nube alineada con el riesgo y los requisitos reglamentarios.

11.2.3 El control 5.25 exige que las organizaciones garanticen que los controles de seguridad en entornos en la nube satisfacen las necesidades de la organización.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 exige políticas formales de uso para sistemas externos, como los servicios en la nube.

11.3.2 SC-12 y SC-13 abordan el cifrado de los datos en tránsito y en reposo en entornos en la nube.

11.3.3 SR-5 cubre los controles de riesgo de la nube y de terceros dentro de la cadena de suministro.

11.4 RGPD de la UE (2016/679)

11.4.1 El artículo 28 exige que los proveedores de servicios en la nube que actúen como encargados del tratamiento cumplan obligaciones contractuales vinculantes.

11.4.2 El artículo 32 exige controles técnicos y organizativos para el tratamiento de datos basado en la nube.

11.4.3 El capítulo V prohíbe las transferencias internacionales no autorizadas de datos personales almacenados en la nube.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 El artículo 21(2)(f), (i) exige que las entidades esenciales e importantes implanten políticas adecuadas para la seguridad de los servicios en la nube y el control de la cadena de suministro.

11.6 DORA de la UE (2022/2554)

11.6.1 El artículo 5(2) exige que las pymes financieras integren la seguridad de la nube en sus marcos de gestión del riesgo de las TIC.

11.6.2 El artículo 28 establece normas de supervisión para los terceros proveedores críticos de servicios TIC, incluidos los proveedores de servicios en la nube.

11.7 COBIT 2019

11.7.1 DSS01 – «Gestionar las operaciones» aborda la integridad operativa de los servicios en la nube.

11.7.2 DSS05 – «Gestionar los servicios de seguridad» incluye protecciones y supervisión específicas para la nube.

11.7.3 BAI04 – «Gestionar la disponibilidad y la capacidad» garantiza la continuidad del negocio y el rendimiento en entornos en la nube.