					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P27					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	Requisitos de planificación y control operacional de la nube.
ISO/IEC 27002:2022	Controles 5.23–5.25	Requisitos relativos al uso, la política y la seguridad de los servicios en la nube.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Uso de sistemas externos, requisitos contractuales y técnicos, protecciones criptográficas y seguridad de la cadena de suministro.
RGPD de la UE	Artículos 28, 32, Capítulo V	Requisitos aplicables a los encargados del tratamiento en la nube, seguridad del tratamiento y transferencias de datos.
Directiva NIS2 de la UE	Artículo 21(2)(f, i)	Riesgo de terceros y requisitos de la cadena de suministro.
DORA de la UE	Artículos 5(2), 28	Supervisión de las TIC y de terceros (nube) para entidades financieras.
COBIT 2019	BAI04, DSS01, DSS05	Disponibilidad de la nube, operaciones y gestión de la seguridad.

1. Propósito

1.1 Esta política establece los requisitos obligatorios de la organización para el uso seguro, conforme y responsable de los servicios de computación en la nube en los modelos de servicio Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS).

1.2 La política tiene por objeto garantizar que los servicios en la nube se adopten y se gobiernen de manera que protejan la confidencialidad, integridad y disponibilidad de los activos de información, al tiempo que se cumplan las obligaciones regulatorias, legales y contractuales.

1.3 Define controles para gestionar el riesgo asociado a la nube, proteger los datos, supervisar el cumplimiento de los proveedores y eliminar el uso no autorizado. Asimismo, respalda la innovación en las operaciones de la organización mediante plataformas en la nube, alineando la seguridad, la resiliencia operativa y la eficiencia de costes.

2. Alcance

2.1 Esta política se aplica a todos los empleados, contratistas, proveedores de servicios externos y consultores externos que aprovisionen, configuren, accedan, administren o utilicen servicios en la nube en nombre de la organización.

2.2 Se aplica a todos los entornos en los que se traten los datos o las cargas de trabajo de la organización, incluidos:

2.2.1 Despliegues de nube pública, privada, híbrida y comunitaria

2.2.2 Todos los modelos de servicio en la nube (IaaS, PaaS, SaaS)

2.2.3 Arquitecturas multinube y federadas

2.2.4 Uso de shadow IT o de cuentas personales de nube con fines profesionales

2.3 Abarca todos los niveles de clasificación de la información y se aplica tanto a los sistemas internos como a las plataformas alojadas por proveedores en las que se almacenen o traten datos propiedad de la organización o datos regulados.

3. Objetivos

3.1 Garantizar un uso seguro y coherente de las tecnologías en la nube mediante directrices de uso claramente definidas, configuraciones base de seguridad y funciones de gobernanza.

3.2 Minimizar los riesgos operativos y regulatorios asociados a la computación en la nube, incluidos el acceso no autorizado, las brechas de seguridad de los datos, las configuraciones incorrectas, el incumplimiento y la interrupción del servicio.

3.3 Aplicar requisitos de seguridad y privacidad a todos los proveedores de nube y verificar su cumplimiento mediante cláusulas contractuales, evaluaciones y derechos de auditoría.

3.4 Permitir una adopción escalable y resiliente de la nube sin comprometer la postura de seguridad, los requisitos legales ni la continuidad del negocio.

3.5 Alinear la gobernanza y el uso de la nube con el marco del SGSI de la organización, las obligaciones legales (por ejemplo, RGPD de la UE, DORA de la UE), las directrices sectoriales y las buenas prácticas reconocidas del sector (por ejemplo, NIST, COBIT).

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Aprueba la Política de Uso de la Nube y la hoja de ruta estratégica para la adopción de la nube.

4.1.2 Revisa y respalda las excepciones de alto riesgo a los requisitos estándar de gobernanza de la nube.

4.1.3 Garantiza que las iniciativas de nube dispongan de financiación, supervisión e integración adecuadas con los marcos de gestión de riesgos corporativos.

4.2 Director de Seguridad de la Información (CISO)

4.2.1 Es el propietario de esta política y del Registro de Servicios en la Nube de la organización.

4.2.2 Aprueba el alta de nuevos proveedores de nube con base en la diligencia debida y la evaluación de riesgos.

4.2.3 Revisa la documentación de cumplimiento del proveedor y valida la adecuación de los controles 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 y actualizarse cuando sea necesario para mantener la alineación con:

9.1.1 La evolución de los requisitos legales y regulatorios (por ejemplo, RGPD de la UE, Directiva NIS2 de la UE, DORA de la UE)

9.1.2 Los cambios en las normas ISO/IEC 27001 o ISO/IEC 27002

9.1.3 Las actualizaciones de la arquitectura en la nube de la organización, el panorama de riesgos o la cartera de servicios

9.1.4 Las investigaciones de incidentes, los resultados de auditoría o las lecciones aprendidas del uso operativo

9.2 El Director de Seguridad de la Información es responsable de iniciar la revisión y convocar a las partes interesadas pertinentes, incluidos:

9.2.1 Arquitecto de Seguridad de la Nube

9.2.2 Equipo Jurídico y de Cumplimiento

9.2.3 Responsables de Compras y Gestión de Proveedores

9.2.4 Propietarios del servicio y Operaciones de TI

9.3 Todas las actualizaciones deben:

9.3.1 Estar sujetas a control de versiones y fechadas

9.3.2 Ser aprobadas por la Alta Dirección

9.3.3 Comunicarse a las partes afectadas, incluidos empleados, contratistas y terceros

9.3.4 Archivarse de conformidad con las políticas internas de documentación

9.4 Las revisiones intermedias podrán activarse por:

9.4.1 Nuevas contrataciones de CSP o migraciones importantes

9.4.2 Amenazas emergentes contra la infraestructura en la nube

9.4.3 Cambios sustanciales en obligaciones contractuales, legales o sectoriales

10. Políticas relacionadas y vinculaciones

10.1 Esta política está estrechamente vinculada con las siguientes políticas internas y depende de ellas:

10.1.1 P1 – Política de Seguridad de la Información: Establece los principios generales que rigen la operación segura de sistemas y servicios, que esta política aplica en el contexto de la nube.

10.1.2 P5 – Política de Gestión de Cambios: Todos los cambios de configuración en la nube deben seguir los procedimientos de control de cambios definidos en P5.

10.1.3 P13 – Política de Clasificación y Etiquetado de Datos: Determina cómo se evalúan los datos antes de su transferencia a la nube y cómo se aplican controles como el cifrado y la residencia de los datos.

10.1.4 P18 – Política de Controles Criptográficos: Proporciona estándares para el cifrado, la gestión de claves y el uso de algoritmos criptográficos, aplicados directamente en las configuraciones de los servicios en la nube.

10.1.5 P22 – Política de Registro de Eventos y Monitorización: Especifica los requisitos de recopilación, conservación y análisis de registros que deben aplicarse en entornos en la nube.

10.1.6 P30 – Política de Respuesta a Incidentes: Define los procedimientos de escalado, contención y remediación para eventos de seguridad relacionados con la nube.

10.1.7 P33 – Política de Supervisión de Auditoría y Cumplimiento: Respalda la preparación para auditorías y la garantía continua de que los controles de la nube se aplican y supervisan.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001: cláusula 8.1 – Planificación y control operacional: exige que las organizaciones implanten y controlen los procesos necesarios para cumplir los requisitos de seguridad de la información, incluidos los que afectan a entornos en la nube.

11.2 ISO/IEC 27002:2022 – controles 5.23 a 5.25:

11.2.1 Anexo A, control 5.23 – Uso de servicios en la nube: exige evaluación basada en riesgos, autorización formal y documentación del uso de servicios en la nube.

11.2.2 Anexo A, control 5.24 – Política de uso de la nube: exige el establecimiento y la aplicación de políticas formales de uso de la nube alineadas con las necesidades y riesgos de la organización.

11.2.3 Anexo A, control 5.25 – Seguridad en los servicios en la nube: exige la integración de la seguridad, las protecciones contractuales y la supervisión de las cargas de trabajo y los datos alojados en la nube.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Uso de sistemas externos: exige reglas y condiciones definidas para acceder a recursos de la organización desde sistemas externos o basados en la nube.

11.3.2 SA-9(5) – Servicios de sistemas de información externos: exige requisitos contractuales de seguridad, supervisión y monitorización continua para sistemas en la nube de terceros.

11.3.3 SC-12 a SC-28 – Protecciones criptográficas, protección del perímetro e integridad de la transmisión: se alinean con los requisitos de cifrado, identidad y acceso para servicios alojados en la nube y datos en tránsito.

11.3.4 SR-5 – Protección de la cadena de suministro: respalda la evaluación y el control contractual sobre los CSP implicados en la prestación del servicio.

11.4 RGPD de la UE (2016/679):

11.4.1 Artículo 28 – Obligaciones del encargado del tratamiento: exige contratos formales con proveedores de nube para garantizar la seguridad, la confidencialidad y la auditabilidad del tratamiento de datos personales.

11.4.2 Artículo 32 – Seguridad del tratamiento: respalda la aplicación de cifrado, controles de acceso, registro de eventos y otras salvaguardas en entornos en la nube.

11.4.3 Capítulo V – Transferencias internacionales de datos: exige la transferencia lícita de datos fuera de la UE/EEE mediante salvaguardas como las CCT o decisiones de adecuación.

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

11.5.1 Artículo 21(2)(f, i): exige que las entidades gestionen los riesgos derivados de proveedores terceros de servicios en la nube y garanticen la integridad de la cadena de suministro digital mediante medidas contractuales y técnicas.

11.6 DORA de la UE (2022/2554):

11.6.1 Artículo 5(2) – Gobernanza de los riesgos de las TIC: exige integrar el riesgo de terceros de TIC, incluidos los servicios en la nube, en la gobernanza general de riesgos.

11.6.2 Artículo 28 – Supervisión de proveedores terceros críticos de TIC: exige que las entidades financieras supervisen, controlen e informen sobre las dependencias de proveedores de nube, su postura de seguridad y su resiliencia.

11.7 COBIT 2019:

11.7.1 BAI04 – Gestionar la disponibilidad y la capacidad: garantiza que los servicios en la nube sean resilientes, estén monitorizados y cumplan los criterios de rendimiento definidos.

11.7.2 DSS01 – Gestionar las operaciones: respalda la integración operativa, la gestión de incidentes y las configuraciones base en plataformas alojadas en la nube.

11.7.3 DSS05 – Gestionar los servicios de seguridad: orienta la implantación de controles de seguridad específicos para la nube, la monitorización y la prevención de incidentes en los servicios digitales.