				Introduzca aquí la denominación de la entidad jurídica registrada						
Número de documento: P13S				Título del documento: **Política de Clasificación y Etiquetado de Datos**						
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**

Alineada con normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.3, 8	
ISO/IEC 27002:2022	Controles 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Directiva NIS2 de la UE	Artículo 21(2)(a)	
DORA de la UE	Artículo 5(8)	
COBIT 2019	BAI03.05, DSS05	
RGPD de la UE	Artículos 5, 32	

1. Propósito

1.1 Esta política define cómo debe clasificarse y etiquetarse toda la información tratada por la organización para garantizar el mantenimiento de su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.

1.2 Permite una gestión coherente de los datos mediante la asignación de niveles de protección adecuados a la información en función de su sensibilidad, impacto para la organización u obligaciones legales.

1.3 La clasificación y el etiquetado ayudan a reducir el riesgo de divulgación accidental, acceso no autorizado o tratamiento inadecuado de datos sensibles, especialmente en pymes que pueden depender de sistemas más sencillos y de controles menos formalizados.

1.4 Esta política es fundamental para la certificación ISO/IEC 27001 y el cumplimiento normativo, en particular en relación con leyes de protección de datos como el RGPD de la UE y marcos de ciberseguridad como la Directiva NIS2 de la UE y DORA de la UE.

2. Alcance

2.1 Esta política se aplica a todos los datos de la organización, con independencia de su formato o ubicación, incluidos:

2.1.1 Documentos electrónicos, hojas de cálculo, correos electrónicos, formularios, imágenes y archivos escaneados.

2.1.2 Documentos físicos, como registros impresos, informes, facturas y notas.

2.1.3 Datos almacenados o tratados en servicios en la nube, servidores locales, medios extraíbles o dispositivos de propiedad personal utilizados con fines profesionales.

2.1.4 Datos temporales o transitorios generados durante las operaciones de la organización (p. ej., registros, archivos de caché, correos electrónicos).

2.2 Todo el personal, los contratistas, los trabajadores temporales y los proveedores externos con acceso a datos de la organización deben cumplir esta política.

2.3 Esta política se aplica durante todo el ciclo de vida de los datos: desde su creación y almacenamiento, pasando por el acceso y la transferencia, hasta su archivo o eliminación.

3. Objetivos

3.1 Definir un esquema de clasificación sencillo y exigible que pueda entenderse y aplicarse fácilmente en toda la organización.

3.2 Exigir que cada activo de datos se clasifique según su sensibilidad y se etiquete en consecuencia para orientar su tratamiento, almacenamiento y acceso adecuados.

3.3 Garantizar que las prácticas de etiquetado de datos se integren en los flujos de trabajo de la organización, como la incorporación de personal, el inicio de proyectos y la configuración de sistemas.

3.4 Reducir el riesgo de incidentes de seguridad de los datos mediante la aplicación de controles de tratamiento (p. ej., cifrado, restricción de acceso) según el nivel de clasificación.

3.5 Garantizar el cumplimiento de las leyes de privacidad y seguridad de la información demostrando que los datos sensibles (p. ej., personales, financieros o de carácter propietario) están correctamente etiquetados y gestionados.

3.6 Establecer una rendición de cuentas proactiva sobre las decisiones de clasificación y garantizar revisiones periódicas y actualizaciones basadas en la evolución de las necesidades de la organización y de los requisitos legales.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Es responsable de esta política y aprueba el esquema de clasificación.

4.1.2 Proporciona supervisión para garantizar que las responsabilidades de clasificación se deleguen y se apliquen.

4.1.3 Debe revisar y autorizar cualquier excepción a los requisitos de clasificación o etiquetado.

4.1.4 Garantiza que las prácticas de gestión de datos cumplan los requisitos normativos conforme a leyes como el RGPD de la UE y DORA de la UE.

4.2 Propietario de la información / Responsable de datos

4.2.1 Asigna una clasificación inicial a cada nuevo conjunto de datos o activo de información en el momento de su creación o adquisición.

4.2.2 Garantiza que se apliquen etiquetas visibles, cuando corresponda, como encabezados, pies de página, marcas de agua o nombres de carpetas.

4.2.3 Revisa periódicamente las clasificaciones para verificar su vigencia, exactitud y cualquier cambio necesario (p. ej., tras la desclasificación o publicación).

4.2.4 Trabaja con el Responsable de TI para aplicar protecciones técnicas en función de la clasificación (p. ej., derechos de acceso, cifrado).

[... 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 ser revisada anualmente por el Director General y el Responsable de datos para asegurar que refleje:

9.1.1 Cambios en las operaciones de la organización o en los tipos de datos.

9.1.2 Nuevos requisitos reglamentarios (p. ej., privacidad de los datos o supervisión financiera).

9.1.3 Cambios tecnológicos que afecten a las capacidades de etiquetado o clasificación.

9.2 La revisión debe incluir actualizaciones de las categorías de clasificación, herramientas o prácticas de etiquetado, así como del contenido de concienciación y formación.

9.3 Las revisiones de la política deben ser aprobadas por el Director General y comunicadas a todo el personal. Debe conservarse un registro de cambios de versión con fines de auditoría.

10. Políticas relacionadas y vinculaciones

10.1 P2S – Política de funciones y responsabilidades de gobernanza: asigna la rendición de cuentas proactiva sobre la titularidad y la aplicación de la política.

10.2 P4S – Política de Control de Acceso: alinea el acceso a los sistemas con los niveles de clasificación de los datos.

10.3 P12S – Política de gestión de activos: realiza el seguimiento de los activos físicos y digitales que almacenan datos clasificados.

10.4 P17S – Política de Protección de Datos y Privacidad: regula la protección de los datos personales, muchos de los cuales se clasifican como Confidenciales.

10.5 P30S – Política de Respuesta a Incidentes: define las vías de escalado y los procedimientos de respuesta en caso de incumplimientos de clasificación o exposición de datos.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 5.3 exige responsabilidades claramente definidas para la gestión y protección de los datos.

11.1.2 La cláusula 8.1 exige planificación y controles operativos, incluidos los vinculados a la categorización de los datos.

11.2 ISO/IEC 27002

11.2.1 El control 5.12 proporciona directrices sobre clasificación de la información basada en riesgos y en requisitos reglamentarios.

11.2.2 El control 5.13 detalla mecanismos prácticos de etiquetado y reglas de tratamiento asociadas.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16 exige el marcado de la información para garantizar que las medidas de protección estén alineadas con la clasificación.

11.3.2 MP-3 / MP-5 proporcionan directrices sobre etiquetado y control de medios y salidas.

11.4 RGPD de la UE

11.4.1 Los artículos 5 y 32 exigen minimización de datos e integridad mediante salvaguardas adecuadas de clasificación y tratamiento.

11.5 Directiva NIS2 de la UE

11.5.1 El artículo 21(2)(a) exige controles técnicos y organizativos para la protección de datos basada en riesgos.

11.6 DORA de la UE

11.6.1 El artículo 5(8) exige que las entidades clasifiquen los activos de datos como parte de su programa de gestión del riesgo de las TIC.

11.7 COBIT 2019

11.7.1 BAI03.05 exige clasificación de la información y protección ajustada al riesgo.

11.7.2 DSS05.02 aborda la aplicación de controles basados en la clasificación y su seguimiento.