					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P13					Título del documento: **Política de Clasificación y Etiquetado de la Información**							
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**

1. Propósito

1.1 Esta política define el marco formal para la clasificación y el etiquetado de los activos de información de la organización en función de su sensibilidad, exposición al riesgo y obligaciones regulatorias.

1.2 Garantiza que toda la información, ya sea almacenada, transmitida o procesada, se clasifique y etiquete de forma clara, de manera que comunique el nivel de protección y tratamiento requerido.

1.3 La política exige una clasificación estructurada alineada con las prácticas de gestión de riesgos de la organización, en apoyo de los objetivos de confidencialidad, integridad y disponibilidad tanto de la información digital como física.

1.4 Este control es esencial para habilitar el acceso basado en roles, la preparación para auditorías, el intercambio adecuado de información y la implantación eficaz de salvaguardas técnicas como el cifrado, las copias de seguridad y la monitorización.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los activos de información de la organización, incluidos documentos, bases de datos, registros y comunicaciones

2.1.2 Todos los formatos de información, incluidos los digitales, impresos, escritos o verbales

2.1.3 Todos los entornos: local, remoto, móvil y en la nube

2.1.4 Todos los empleados, contratistas, proveedores de servicios y terceros encargados del tratamiento que creen, manejen o almacenen información de la organización

2.2 El alcance abarca el contenido desarrollado internamente, los datos obtenidos externamente, los datos personales sujetos a obligaciones de la normativa de privacidad (por ejemplo, el RGPD de la UE) y la información intercambiada con clientes, socios y organismos reguladores.

2.3 Se aplica a todos los sistemas utilizados para almacenar o transmitir información, incluidas las aplicaciones de la organización, los servidores de archivos, los sistemas de correo electrónico, las plataformas en la nube y los repositorios de copias de seguridad.

3. Objetivos

3.1 Establecer un esquema de clasificación estandarizado para toda la organización, basado en el impacto de la exposición o el compromiso de la información.

3.2 Garantizar que toda la información esté etiquetada de forma visible y persistente para reflejar su nivel de clasificación y sus requisitos de tratamiento.

3.3 Exigir controles de acceso y de tratamiento de la información alineados con la clasificación, incluidos el cifrado, el registro de eventos, la protección de la transmisión y los plazos de conservación.

3.4 Apoyar el cumplimiento de normas internacionales (ISO/IEC 27001, 27002), marcos jurídicos (RGPD de la UE, Directiva NIS2 de la UE, DORA de la UE) y políticas internas de gestión de riesgos.

3.5 Garantizar que todos los usuarios comprendan sus responsabilidades en la protección de la información, la aplicación de etiquetas y el tratamiento correcto de la información clasificada.

3.6 Mantener la trazabilidad entre el estado de clasificación, los controles asociados y el Inventario de Activos de la organización a efectos de auditoría y cumplimiento.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es responsable de la política de clasificación y etiquetado de la información y garantiza su alineación con los requisitos regulatorios, contractuales y operativos.

4.1.2 Aprueba los niveles de clasificación, los estándares de etiquetado y las revisiones de la política.

4.1.3 Supervisa el cumplimiento de la política mediante auditorías, métricas y revisión de excepciones.

4.1.4 Coordina la gobernanza transversal con los equipos de Asesoría Jurídica, Privacidad y Riesgos.

4.2 Propietarios de la información

4.2.1 Son responsables de clasificar los activos de información bajo su control utilizando el esquema de clasificación de la organización.

4.2.2 Aplican las etiquetas de clasificación en el momento de la creación, actualización o recepción.

4.2.3 Revisan periódicamente la clasificación de los activos, especialmente en respuesta a cambios en la sensibilidad, el alcance regulatorio o el valor para la organización.

4.2.4 Garantizan que la información sensible se maneje y etiquete adecuadamente durante todo su ciclo de vida.

[... 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 anualmente para garantizar su alineación con:

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

9.1.2 Las actualizaciones de las directrices de clasificación de ISO/IEC 27001 o 27002

9.1.3 Los cambios organizativos que afecten a la sensibilidad de la información o a su titularidad

9.1.4 Los cambios tecnológicos, incluidas nuevas plataformas de gestión documental o de datos

9.2 El Director de Seguridad de la Información (CISO) deberá iniciar la revisión en colaboración con el Comité de Seguridad de la Información, la Asesoría Jurídica y las unidades de negocio afectadas.

9.3 Las revisiones deberán incluir:

9.3.1 La eficacia de la aplicación de la clasificación y el grado de cumplimiento por parte de los usuarios

9.3.2 El análisis de incidentes o excepciones vinculados a clasificaciones incorrectas

9.3.3 La retroalimentación de los usuarios sobre herramientas de etiquetado o materiales de orientación

9.3.4 La comparación con estándares de clasificación del sector

9.4 Las actualizaciones de la política deben estar sujetas a control de versiones, documentarse en el repositorio del SGSI y comunicarse a todo el personal pertinente, con especial énfasis en nuevas responsabilidades o cambios en las herramientas.

9.5 Las nuevas incorporaciones deben recibir la versión vigente de la política durante el proceso de alta. Todos los empleados deben completar formación de reciclaje tras cambios significativos en la política.

10. Políticas relacionadas y vinculaciones

10.1 Esta política está respaldada directamente por los controles descritos en las siguientes políticas relacionadas y los hace exigibles:

10.1.1 P4 - Política de Control de Acceso: el acceso a la información se rige por niveles de clasificación; la información más sensible requiere mecanismos más estrictos de control de acceso y autorización.

10.1.2 P11 - Política de gestión de cuentas de usuario y privilegios: refuerza la asignación de privilegios basada en la necesidad de conocer, determinada por los niveles de clasificación.

10.1.3 P12 - Política de gestión de activos: garantiza que cada activo del inventario incluya su clasificación y etiqueta, respaldando la trazabilidad y la responsabilidad.

10.1.4 P14 - Política de conservación y eliminación de datos: las reglas de eliminación y conservación se determinan por el nivel de clasificación de la información y los mandatos regulatorios de conservación.

10.1.5 P18 - Política de controles criptográficos: aplica los estándares de cifrado adecuados en función de la clasificación del activo de información.

10.1.6 P22 - Política de registro de eventos y monitorización: permite la supervisión del acceso a la información clasificada y de su movimiento, garantizando la auditabilidad y la detección de etiquetado incorrecto o uso indebido.

10.2 Cada vinculación garantiza una protección coherente de la información a lo largo de su ciclo de vida, desde su creación y clasificación hasta su tratamiento seguro, almacenamiento, transmisión y destrucción final.

11. Normas y marcos de referencia

11.1 Esta política está alineada con normas reconocidas internacionalmente y marcos regulatorios que rigen la clasificación y el etiquetado de información sensible.

11.2 ISO/IEC 27001

11.2.1 Cláusula 4.2 - Comprensión de las necesidades y expectativas de las partes interesadas. Los requisitos de clasificación suelen derivarse de obligaciones legales, regulatorias o contractuales impuestas por las partes interesadas (por ejemplo, el RGPD de la UE, acuerdos de confidencialidad con clientes), que deben reflejarse en la política.

11.2.2 Cláusula 6.1.3 - Tratamiento de riesgos de seguridad de la información. La clasificación afecta directamente a la selección de controles de tratamiento de riesgos, incluidos el control de acceso, el cifrado y la conservación, en función de la sensibilidad de la información.

11.2.3 Cláusula 7.2 - Competencia. La política exige que el personal responsable de la clasificación y el etiquetado esté formado, lo cual se encuadra dentro de los requisitos de competencia.

11.2.4 Cláusula 7.3 - Concienciación. La política exige que todos los usuarios conozcan los niveles de clasificación y sus responsabilidades en el tratamiento de la información, en línea con las obligaciones de concienciación.

11.2.5 Cláusula 7.5 - Información documentada. La propia política de clasificación es un documento controlado, y los procedimientos, registros de formación y etiquetas de clasificación forman parte de la información documentada.

11.2.6 Cláusula 8.1 - Planificación y control operacional. La clasificación y el etiquetado son procesos operativos integrados en la gestión del ciclo de vida de la información, y esta cláusula garantiza que dichas actividades se planifiquen, implanten y controlen.

11.2.7 Cláusula 9.1 - Seguimiento, medición, análisis y evaluación. La política incluye disposiciones para el seguimiento del cumplimiento de la clasificación, las tendencias de incidentes y la eficacia del esquema de etiquetado.

11.2.8 Cláusula 10.1 - No conformidad y acción correctiva. La política define respuestas ante clasificaciones incorrectas, incluidas acciones correctivas como formación correctiva, actualizaciones y gestión de excepciones.

11.3 ISO/IEC 27002:2022

11.3.1 Control 5.12 - Clasificación de la información. Este control garantiza que la información se clasifique en función de su sensibilidad, valor y criticidad, que es precisamente lo que formaliza esta política.

11.3.2 Control 5.13 - Etiquetado de la información. Este control exige el etiquetado adecuado de la información conforme a su nivel de clasificación, aspecto plenamente abordado en la política.

11.3.3 Control 5.10 - Uso aceptable de la información y de otros activos asociados. La política exige la forma en que los usuarios deben manejar la información clasificada, respaldando directamente el uso aceptable y evitando el uso indebido.

11.3.4 Control 5.11 - Devolución de activos. La clasificación ayuda a garantizar que la información sensible se identifique y se devuelva o sanitice de forma segura cuando un empleado o proveedor cause baja.

11.3.5 Control 5.9 - Inventario de la información y otros activos asociados. La clasificación suele estar vinculada al inventario de activos, que debe reflejar el nivel de clasificación de cada elemento para respaldar la correcta asignación de controles.

11.3.6 Control 5.14 - Transferencia de información. Los niveles de clasificación influyen en los controles sobre las transferencias internas y externas de información (por ejemplo, cifrado, aprobación, restricciones de acceso).

11.3.7 Control 8.12 - Prevención de fuga de datos. La exigencia de clasificación y etiquetado ayuda a prevenir la divulgación no autorizada y la pérdida de información.

11.3.8 Control 8.11 - Enmascaramiento de datos. Determinados niveles de clasificación (por ejemplo, Confidencial, Restringido) pueden exigir enmascaramiento cuando los datos se utilicen en pruebas, desarrollo o analítica.

11.4 NIST SP 800-53 Rev. 5

11.4.1 PL-2 - Política y procedimientos de protección del sistema y las comunicaciones: respalda las políticas de clasificación como parte de la protección general de la información.

11.4.2 AC-16 - Atributos de seguridad: implementa la aplicación del acceso basada en metadatos de clasificación y permisos de usuario.

11.4.3 MP-3 / MP-5 - Marcado de soportes y protección en el transporte: exige el etiquetado y la protección de la información en reposo y en tránsito según su clasificación.

11.5 RGPD de la UE (2016/679)

11.5.1 Artículo 5 - Principios de protección de datos: exige que los datos personales se traten de forma segura y proporcionada a su sensibilidad.

11.5.2 Artículo 32 - Seguridad del tratamiento: refuerza la clasificación como mecanismo de protección de datos basado en riesgos y de adopción de medidas técnicas adecuadas.

11.6 Directiva NIS2 de la UE (2022/2555)

11.6.1 Artículo 21(2)(a): exige políticas para la gestión de riesgos de seguridad de la información, incluidos controles de clasificación de activos y datos.

11.6.2 Artículo 21(3): fomenta la adopción de medidas para exigir un tratamiento adecuado de los datos, respaldado mediante etiquetado basado en clasificación.

11.7 DORA de la UE (2022/2554)

11.7.1 Artículo 5 - Gobernanza y control: exige marcos de gobernanza que clasifiquen los activos de información para el control del riesgo de las TIC.

11.7.2 Artículo 9 - Gestión del riesgo de las TIC: impone medidas técnicas y organizativas para activos TIC críticos, incluida su clasificación y etiquetado.

11.8 COBIT 2019

11.8.1 DSS05.02 - Gestionar los servicios de seguridad: exige clasificaciones de seguridad de la información para garantizar la protección de la información de la organización.

11.8.2 MEA03 - Supervisar, evaluar y valorar el cumplimiento: respalda la auditoría y revisión periódicas de las prácticas de clasificación para garantizar el cumplimiento de la política y su madurez.