

DOCUMENTO TÉCNICO N°141

MODELAMIENTO DE RIESGOS Y CONTROLES EN LA GESTIÓN DOCUMENTAL INSTITUCIONAL

Este documento ofrece una guía general para el análisis de riesgos críticos en los procesos de gestión documental institucional. Identifica los riesgos asociados a sus subprocesos, presenta controles teóricos específicos y proporciona orientación sobre la documentación y evidencias necesarias para verificar la correcta implementación y efectividad de dichos controles.



ÍNDICE	
Índice	2
Nota: Presentación	3
Capítulo 1: Introducción	4
1.1 Propósito del Documento	6
1.2 Contexto y Alcance	8
1.2.1 Factores Críticos de Implementación	8
1.2.2 Oportunidades de Mejora	11
1.2.3 Principales Señales de Alerta	12
Capítulo 2: Fundamentos Teóricos	16
2.1 A) Planificación Documental	19
2.2 B) El Ciclo de Vida de la Gestión Documental	20
2.3 C) Identificación de las Etapas Relativas a la Eliminación de Documentos	24
2.4 D) Identificación de los Aspectos Relevantes del Resguardo de la Información	28
2.5 E) Plazos Legales de Conservación, Prescripción y Eliminación Documental	30
2.6 F) Plataformas Transversales para la Transformación Digital del Estado	35
Capítulo 3: Marco Regulatorio y Legal	37
3.1 Normativa Aplicable	38
3.2 Instrucciones y Dictámenes de la Contraloría General de la República	45
3.3 Estrategias Nacionales para la Transformación Digital	51
3.4 Normas Internacionales ISO	53
3.4.1 Normas e Informes Técnicos Relacionados con la Implementación de Procesos de Gestión Documental	54
3.4.2 Normas de Sistemas de Gestión Documental que Establecen el Marco de Gobernanza para los Documentos	59
Capítulo 4: Elementos Técnicos	61
4.1 Definición de una Tipología General de Riesgos	66
4.2 Estructura del Proceso de Gestión Documental	68
4.3 Matrices de Análisis de Riesgo y Control	70
4.3.1 Matriz de Análisis de la Planificación Documental	70
4.3.2 Matriz de Análisis de la Gestión del Ciclo de Vida Documental	77
4.3.3 Matriz de Análisis de la Eliminación de Documentos	92
4.3.4 Matriz de Análisis del Resguardo de la información	103
Capítulo 5: Conclusiones y Recomendaciones Finales	113
5.1 Recomendaciones Finales	112
Bibliografía	114

Nota**PRESENTACIÓN**

En cumplimiento de las instrucciones del Presidente de la República, Gabriel Boric Font, respecto del fortalecimiento de la Política de Auditoría Interna de Gobierno, el Consejo de Auditoría Interna General de Gobierno (CAIGG), entidad asesora del Supremo Gobierno en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza, presenta a la Red de Auditoría Gubernamental el Documento Técnico N° 145: Modelamiento de Riesgos y Controles en la Gestión Documental Institucional, versión 0.1.

A través de un enfoque metodológico, se detallan los aspectos técnicos fundamentales en la conciliación bancaria, como la obtención de antecedentes, comparación de saldos, revisión de transacciones y corrección de errores, así como en el análisis de cuentas contables, que incluye la trazabilidad de saldos, clasificación de transacciones y revisión de cuentas por cobrar y pagar. Se hace hincapié en la identificación de riesgos, el diseño de controles teóricos y la importancia de la automatización para minimizar errores humanos y mejorar la eficiencia.

Este documento ofrece una guía general para el análisis de riesgos críticos en los procesos de conciliación bancaria y análisis de cuentas contables, identificando los riesgos asociados a las etapas que componen dichos procesos, levantando controles teóricos específicos, y ofreciendo una orientación sobre la documentación y evidencia necesarias para verificar la ejecución y efectividad de dichos controles. Para su desarrollo, se considera el marco normativo relevante, incluyendo leyes y regulaciones, así como instrucciones y pronunciamientos de la Contraloría General de la República (CGR) y la Dirección de Presupuestos (DIPRES), proporcionando directrices claras para su implementación.

Con base en las oportunidades de mejora identificadas, se presentan recomendaciones específicas que incluyen la capacitación continua del personal, el fortalecimiento de los controles internos y la implementación de procesos automatizados, con el fin de optimizar la gestión de recursos públicos, garantizar la transparencia y establecer un marco de confianza con la ciudadanía.

Finalmente, este documento es un recurso valioso para todas las entidades del sector público, convirtiéndose en una herramienta esencial para aquellos comprometidos en mejorar sus sistemas de control interno y la calidad de su gestión financiera. Por lo tanto, la mejora continua y la adecuada documentación en los procesos de conciliación y análisis de cuentas son, sin lugar a duda, el camino hacia una administración pública más efectiva y responsable.

Santiago de Chile, 2025.



Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

INTRODUCCIÓN

Capítulo 1

INTRODUCCIÓN

El fortalecimiento de la gestión documental constituye una necesidad prioritaria para las instituciones públicas, tanto por las exigencias del marco regulatorio como por los desafíos derivados de la digitalización, la trazabilidad de la información y la protección de datos personales. Sin embargo, **la gestión documental no solo posee un carácter técnico y normativo, sino que también representa un eje estratégico** para garantizar la integridad, disponibilidad y resguardo de los documentos generados o recibidos por las instituciones del Estado. Por lo tanto, **el proceso debe abarcar todo el ciclo de vida documental**, en conformidad con los principios de probidad, legalidad, eficiencia y transparencia que orientan la función pública, y por el marco jurídico que regula la producción, clasificación, uso, conservación, acceso, eliminación y resguardo de la información, considerando además su valor legal, administrativo y patrimonial.

Considerando la magnitud, diversidad y criticidad de la información contenida en los documentos que administran los organismos públicos, la gestión documental enfrenta riesgos como el manejo inadecuado, la pérdida, el acceso no autorizado o la eliminación indebida de documentos. **Estos riesgos generan posibles consecuencias legales y administrativas** conforme al marco normativo vigente, pero también pueden afectar la continuidad operativa, la imagen institucional y la confianza pública.

Ante este escenario, **se requiere un enfoque preventivo y sistemático que permita identificar y analizar los riesgos asociados a la gestión documental, establecer controles proporcionales y generar evidencia verificable del cumplimiento institucional**. Dicho enfoque debe integrar tanto los aspectos técnicos vinculados al archivo, digitalización, conservación o eliminación de documentos, como aquellos relativos al cumplimiento normativo, la protección de datos personales, la seguridad de la información y la responsabilidad institucional frente a revisiones, fiscalizaciones o solicitudes de acceso. En este contexto, el presente documento desarrolla el modelamiento de riesgos y control en el proceso de gestión documental, sustentado en matrices de análisis que se encuentran estructuradas en torno a cuatro subprocesos clave:

Modelamiento de Riesgos y Control en el Proceso de Gestión Documental		
Subprocesos	1.	Planificación Documental
	2.	Ciclo de Vida de los Documentos
	3.	Resguardo Físico y Digital
	4.	Eliminación Regulada

Esta descomposición funcional incluye etapas operativas, riesgos específicos, controles orientadores y evidencias de respaldo, lo que permite su adaptación a instituciones de distinto tamaño, sector o nivel de complejidad, manteniendo su solidez técnica y el pleno cumplimiento del marco regulatorio.

Las matrices incluidas en el documento están diseñadas para contribuir al fortalecimiento de la gestión documental desde una perspectiva funcional, normativa y operativa, permitiendo a las instituciones alinear su práctica con las directrices y marcos normativos, técnicos y de control interno vigentes en el sector público. De esta manera, **el documento ofrece una visión integrada de los riesgos asociados** a cada etapa del proceso de gestión documental, **promoviendo un tratamiento preventivo respaldado en controles formales, evidencia verificable y cumplimiento normativo**, con el fin de asegurar la trazabilidad, la rendición de cuentas y la continuidad operativa en un entorno institucional cada vez más digital.

Por último, se invita a los equipos directivos, profesionales y responsables de archivos y procesos administrativos a explorar este documento, analizar sus contenidos, y utilizar como **guía práctica para fortalecer sus sistemas de gestión documental** y asegurar una administración más segura, eficiente y alineada con los principios que rigen la función pública.

Por ello, el presente documento técnico **tiene como propósito entregar un conjunto de buenas prácticas, lineamientos y herramientas para enfrentar los riesgos y fortalecer controles** en la gestión documental dentro de la organización. **Estas orientaciones podrán ser utilizadas como criterios de auditoría** y contribuirán al fortalecimiento de los procesos de evaluación del diseño e implementación de estas materias por parte de la función de auditoría interna en el sector público.⁽¹⁾

1. La elaboración de este documento contó en algunas de sus partes con redacción mejorada con inteligencia artificial, mediante el uso de asistentes lingüísticos basados en modelos de lenguaje natural, estas herramientas fueron empleadas con responsabilidad y supervisión, manteniendo los autores la plena responsabilidad sobre la exactitud y el contenido final.

1.1 PROPÓSITO DEL DOCUMENTO

En un contexto de transformación digital, de creciente demanda ciudadana por acceso a la información y de exigencias normativas cada vez más rigurosas, se vuelve imprescindible que los organismos públicos cuenten con herramientas que aseguren la integridad, trazabilidad y seguridad de los documentos durante todo su ciclo de vida. Al mismo tiempo, deben enfrentar desafíos y riesgos que requieren un tratamiento preventivo y controlado, en plena coherencia con los marcos legales, técnicos y de control vigentes.

El propósito principal de este documento es:



Proporcionar lineamientos técnicos claros para apoyar la identificación y análisis de riesgos críticos asociados a los procesos de gestión documental en instituciones del sector público. En particular, busca orientar la implementación de medidas preventivas y correctivas proporcionales al nivel de exposición de cada fase documental, considerando tanto los requisitos normativos como los desafíos operativos actuales. Para el modelamiento, se desarrollan matrices de análisis estructuradas en torno a subprocesos o etapas específicas, riesgos clave, controles orientadores de referencia y evidencia documental mínima requerida.

Para efectos de este documento, la gestión documental se entenderá como un proceso institucional que se descompone en los siguientes cuatro subprocesos:



Ahora bien, este documento se sustenta en el marco jurídico nacional aplicable a la gestión documental, incorporando **disposiciones y pronunciamientos de la CGR, el Archivo Nacional y la Ley N°21.180 sobre Transformación Digital del Estado**, junto con estándares internacionales de referencia, tales como **ISO 15489** (Gestión de documentos), **ISO 18128** (Riesgos asociados a los documentos) e **ISO 30301** (Sistemas de gestión para los documentos), reconocidos como buenas prácticas complementarias, siempre que no contravengan la normativa chilena vigente.

Por otra parte, el documento está dirigido a los equipos responsables de gestión documental, control interno, gestión de riesgos y auditoría interna, entre otros actores clave, y entrega un enfoque práctico para:

- Identificar riesgos documentales con base en tipologías claras.
- Formular controles orientadores alineados con el marco legal vigente.
- Verificar el cumplimiento mediante evidencia documental estandarizada.

Este documento busca aportar a la construcción o mejoramiento de una matriz institucional de riesgos en materia de gestión documental, coherente con los principios de legalidad, eficiencia administrativa, interoperabilidad, protección de datos personales y digitalización progresiva establecidos en la normativa vigente.

Por lo tanto, su aplicación tiene como finalidad **potenciar las capacidades institucionales para enfrentar los desafíos de la transformación digital**, prevenir la pérdida o uso indebido de información y dar respuesta a las crecientes exigencias en materia de probidad, transparencia y rendición de cuentas. Además, **puede ser utilizado como una fuente de criterios para la auditoría interna**, cuando preste servicios de aseguramiento sobre temas de gestión documental.

Finalmente, se espera que este documento **contribuya al fortalecimiento del control interno y la gestión de riesgos institucionales**, asegurando la legalidad de los procesos documentales, la trazabilidad de las actuaciones administrativas y la disponibilidad oportuna de los antecedentes para fines administrativos, jurídicos, patrimoniales y de fiscalización.

El documento tiene un **Enfoque Preventivo.**

| 1.2 CONTEXTO Y ALCANCE

La adecuada gestión documental en el sector público **exige una mirada integral sobre el ciclo de vida de los documentos**, que contemple no solo su generación, uso y conservación durante su vigencia administrativa y legal, sino también su planificación, disposición final, ya sea a través de la eliminación regulada o la transferencia a archivos históricos. En este contexto, **el resguardo seguro y continuo de la información bajo custodia institucional se configura como un principio transversal esencial para la integridad, disponibilidad y trazabilidad de los documentos públicos**.

Este enfoque integral adquiere especial relevancia en un entorno normativo en evolución, marcado por la implementación progresiva de la transformación digital del Estado y por el fortalecimiento de las exigencias en materia de protección de datos personales:

<i>Pronunciamiento</i>	<i>Elementos que lo Caracterizan</i>
Circular N° 28.704 de la CGR	- Regula la eliminación y destrucción de documentos públicos. - Constituye un referente normativo clave, al establecer condiciones, requisitos y procedimientos que deben ser cumplidos por las entidades del sector público.
Ley N° 19.628	- Regula la protección de la vida privada.
Ley N° 21.719	- Regula el tratamiento de datos personales. - Crea la Agencia de Protección de Datos Personales
Ley N° 21.180	- Regula la transformación digital del Estado.
Orientaciones del Archivo Nacional	- Cuya normativa técnica establece criterios específicos para la organización, conservación, transferencia y eliminación de documentos, en el marco de una gestión archivística estandarizada y coordinada a nivel institucional.

Estas disposiciones, en conjunto con los criterios técnicos establecidos para la gestión archivística, refuerzan la necesidad de que los organismos públicos cuenten con políticas y procedimientos actualizados en materia de gestión documental, sustentados en principios de seguridad de la información, tales como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, así como en criterios de eficiencia administrativa, transparencia institucional y coherencia normativa.

1.2.1 Factores Críticos de Implementación

La implementación de procesos institucionales relacionados con la planificación documental, ciclo de vida documental (incluyendo la eliminación regulada) y resguardo físico y digital exige **identificar los factores críticos que inciden directamente en su eficacia** y en el cumplimiento de las obligaciones normativas. Un elemento esencial para una gestión documental eficaz es **contar con mecanismos formales y actualizados de clasificación, evaluación y conservación de documentos**, alineados con el marco normativo vigente, en particular con lo dispuesto en la Ley N° 21.180 sobre Transformación Digital del Estado, el Decreto Supremo N° 10 de 2023 y las directrices técnicas emitidas por el Archivo Nacional y la CGR.

A continuación, se describen los principales factores críticos que condicionan la adecuada implementación de los procesos documentales institucionales, agrupados según las fases del ciclo de gestión documental: planificación, ciclo de vida (archivo de gestión, intermedio e histórico), eliminación regulada y resguardo físico y digital de la documentación.



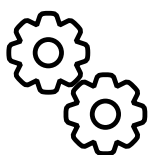
● **Disponibilidad de procedimientos internos estandarizados:**

La disponibilidad de procedimientos internos estandarizados permite establecer plazos de conservación y definir con precisión los criterios de disposición final, en concordancia con las orientaciones técnicas vigentes. Este aspecto es clave para garantizar la trazabilidad, seguridad jurídica y control institucional sobre los documentos públicos, tanto físicos como electrónicos.



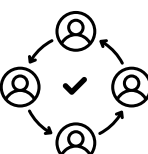
● **Actualización y vigencia de las Tablas de Retención Documental (TRD):**

Un aspecto igualmente relevante es la actualización y validación periódica de las TRD, conforme a los lineamientos técnicos establecidos por el Archivo Nacional. Por lo tanto, la vigencia y adecuación de las TRD es fundamental para definir correctamente los plazos de conservación, la disposición final de los documentos y los criterios de eliminación o transferencia archivística. Por el contrario, su desactualización o ausencia representa un riesgo institucional que puede comprometer tanto la legalidad de las actuaciones administrativas como la gestión eficiente de los recursos documentales.



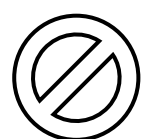
● **Formación técnica del personal responsable:**

La efectividad de la gestión documental institucional depende de factores clave como es la formación técnica del personal responsable, especialmente en áreas como digitalización de documentos, interoperabilidad de sistemas y resguardo de la información. Sin duda, que la ausencia de competencias especializadas en estos ámbitos puede afectar negativamente la correcta implementación de políticas documentales, así como el cumplimiento de los estándares normativos vigentes en materia de transformación digital y conservación documental.



● **Articulación entre unidades responsables:**

La dispersión de funciones documentales entre distintas unidades sin una coordinación efectiva representa un riesgo operativo crítico. La planificación, conservación, eliminación y resguardo suelen involucrar a áreas como gestión documental, informática, jurídica, archivo central y control interno. Sin una articulación formal, mediante comités, protocolos de coordinación o roles claramente definidos, se generan duplicidades, vacíos de responsabilidad o decisiones contradictorias que afectan la trazabilidad y legalidad del ciclo documental.



● **Existencia de condiciones para la eliminación segura:**

Otro factor crítico se relaciona con la existencia de condiciones técnicas, operativas y normativas que permitan realizar procesos de eliminación segura de documentos. Para ello, las instituciones deben contar con normativas internas claras, procedimientos formalizados y las autorizaciones correspondientes, especialmente en los casos que involucren datos personales o información sensible. En este ámbito, resulta fundamental aplicar lo dispuesto en la Circular N° 28.704 de la CGR, así como las normas específicas emitidas por el Archivo Nacional en materia de eliminación documental.



● **Integración de la gestión documental al control interno institucional:**

Un factor determinante para la consolidación de una gestión documental robusta es su integración efectiva con los instrumentos y procesos de control interno. Esto implica que las funciones documentales estén alineadas con los mapas de procesos institucionales, matrices de riesgo, mecanismos de supervisión, revisiones internas y sistemas de trazabilidad administrativa. La falta de esta integración puede debilitar la trazabilidad de decisiones, dificultar la rendición de cuentas y generar brechas normativas en la custodia documental.



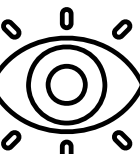
● **Implementación de plataformas tecnológicas conforme a la normativa vigente:**

Resulta indispensable que las instituciones públicas cuenten con plataformas tecnológicas que cumplan con los requisitos técnicos establecidos en el Decreto Supremo N° 10 de 2023 (MINSEGPRES), los cuales incluyen trazabilidad, seguridad, autenticidad, conservación digital y disponibilidad de los documentos. Dichas plataformas deben estar integradas en los flujos de tramitación administrativa electrónica y sujetas a criterios de interoperabilidad, con el fin de asegurar continuidad operativa, control documental y respaldo normativo.



● **Gobernanza de datos y de documentos en entornos digitales:**

En el contexto de la transformación digital del Estado, las instituciones deben adoptar enfoques integrados de gobernanza de datos y documentos. Esto incluye la definición de políticas institucionales sobre metadatos, estructuras de clasificación, resguardo de registros electrónicos, gestión de accesos y preservación digital a largo plazo. La ausencia de una gobernanza clara genera riesgos de pérdida de información, accesos indebidos o quiebres en la cadena de custodia digital, especialmente en plataformas con bajo nivel de interoperabilidad o escasa trazabilidad.



● **Mecanismos de monitoreo, evaluación y mejora continua:**

La implementación de procesos documentales no puede considerarse completa sin un sistema formal de seguimiento que permita verificar su funcionamiento, eficacia y cumplimiento normativo. Por lo tanto, es necesario establecer indicadores de desempeño, mecanismos de retroalimentación, revisiones documentales periódicas y revisiones técnicas que permitan identificar brechas y aplicar mejoras correctivas. La ausencia de estos mecanismos limita la capacidad institucional para responder a cambios normativos o tecnológicos, y compromete la sostenibilidad del sistema documental.



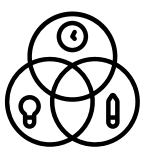
● **Controles proporcionales al nivel de criticidad de la información:**

El resguardo institucional de la información exige la implementación de condiciones que aseguren la confidencialidad, integridad, disponibilidad y trazabilidad de los documentos durante todo su ciclo de vida. Para ello, se deben establecer controles organizacionales proporcionales al nivel de criticidad de la información, definir medidas de respaldo y recuperación ante contingencias, y aplicar mecanismos de revisión periódica que aseguren la actualización continua frente a cambios normativos, tecnológicos o institucionales.

En definitiva, la identificación oportuna y gestión efectiva de estos factores críticos constituye una condición habilitante para la implementación sostenida de procesos documentales institucionales. Por ende, su abordaje permite no solo dar cumplimiento al marco normativo vigente, sino también fortalecer el control interno, reducir riesgos operacionales y asegurar la disponibilidad de información pública confiable, trazable y legalmente válida. Sin duda, que incorporar estos elementos en el diseño e implementación de los sistemas de gestión documental contribuye directamente a una administración pública más eficiente, transparente y preparada.

1.2.2 Oportunidades de Mejora

La gestión documental en el sector público presenta diversas oportunidades de mejora orientadas a fortalecer la trazabilidad, eficiencia y cumplimiento normativo de los procesos institucionales asociados a la planificación, ciclo de vida de la documentación (incluida la eliminación), y resguardo. A continuación, se describen las principales oportunidades identificadas, organizadas según ámbitos funcionales clave:



● **Enfoque sistémico e integración de procesos:**

Una primera oportunidad radica en la posibilidad de avanzar hacia enfoques integrados de gestión documental, que articulen de manera sistémica las etapas de captura, clasificación, conservación, eliminación y resguardo de los documentos. Para ello, se sugiere revisar y alinear los procedimientos institucionales existentes bajo un modelo normativo común, que permita garantizar la continuidad del ciclo de vida documental. Esta acción mejoraría la coherencia interna de los procesos, aseguraría su trazabilidad y fortalecería el cumplimiento de los marcos regulatorios vigentes.



● **Fortalecimiento de la eliminación documental regulada:**

En segundo lugar, se ha identificado la necesidad de formalizar los procedimientos vinculados a la eliminación documental, incorporando criterios de valoración, autorización y trazabilidad, conforme a las directrices del Archivo Nacional y las disposiciones emitidas por el órgano contralor. Para su implementación, se recomienda establecer protocolos escritos y mecanismos de validación que permitan registrar cada etapa del proceso de eliminación. Estas medidas contribuirían al cumplimiento riguroso de los plazos de conservación, al resguardo de evidencia documental y a una respuesta institucional oportuna ante requerimientos de control.

Asimismo, se destaca la oportunidad de implementar procedimientos periódicos de revisión documental, que permitan depurar los archivos activos en función de su pertinencia legal y administrativa. Para ello, se propone establecer ciclos de revisión calendarizados, sustentados en las TRD, con el fin de evitar acumulaciones innecesarias y asegurar el cumplimiento normativo. Esta práctica contribuiría a optimizar el uso de recursos institucionales y a mantener la eficiencia operativa de los archivos.



● **Seguridad de la información y digitalización con valor probatorio:**

Debe fortalecer los mecanismos de resguardo de la información institucional, considerando los aspectos organizacionales, tecnológicos y normativos que inciden en su protección. Para ello, se sugiere establecer responsabilidades claras, aplicar controles de acceso diferenciados, definir políticas de respaldo y recuperación ante contingencias, y mantener actualizadas las medidas de protección conforme a los cambios regulatorios. Estas acciones consolidan una cultura de mejora continua, gobernanza documental y control interno.

Asimismo, se plantea como oportunidad la eliminación del uso de soportes informales o no institucionales, tales como correos electrónicos personales, discos locales o dispositivos portátiles, en los procesos documentales institucionales. De forma complementaria, se sugiere aplicar criterios técnicos de digitalización que permitan otorgar valor probatorio a los documentos electrónicos, particularmente aquellos generados o gestionados en procedimientos administrativos. Para ello, se recomienda reforzar el uso exclusivo de plataformas institucionales autorizadas y aplicar lo establecido en el Decreto Supremo N° 10 de 2023, del Ministerio Secretaría General de la



● **Indicadores y seguimiento del desempeño documental:**

En cuarto lugar, se advierte la oportunidad de incorporar indicadores específicos que permitan monitorear el desempeño de la gestión documental institucional, tales como cumplimiento normativo, eficiencia operativa, calidad archivística y volumen tramitado. En este sentido, se recomienda desarrollar métricas objetivas y aplicables, integradas a los sistemas de seguimiento y evaluación institucional. Ciertamente, contar con estos indicadores permitiría establecer líneas base, monitorear avances y reportar resultados a los niveles superiores de gestión.



● **Coordinación institucional y estandarización operativa:**

Finalmente, se destaca la oportunidad de fortalecer la coordinación entre las unidades generadoras de documentos y los archivos institucionales centrales, con el fin de estandarizar los criterios de archivo, evitar duplicidades y asegurar procesos de eliminación documental debidamente autorizados. Para ello, se sugiere implementar mecanismos de articulación formal que integren a todas las áreas involucradas en la gestión documental institucional. Esta coordinación permitiría consolidar una gestión documental coherente, trazable y ajustada a las normas técnicas del Archivo Nacional.

Cabe señalar, que la implementación efectiva de las oportunidades de mejora identificadas permitirá a las instituciones públicas avanzar hacia una gestión documental más coherente, controlada y alineada con los estándares normativos vigentes. En conjunto, estas medidas fortalecen el control interno, reducen la exposición a riesgos legales y operacionales, y refuerzan la rendición de cuentas ante organismos fiscalizadores y la ciudadanía.

De igual forma, la adopción de enfoques integrados y sistemáticos, que articulen planificación, conservación, eliminación regulada y resguardo de la información, contribuye a consolidar una cultura organizacional orientada a la trazabilidad, la interoperabilidad y la mejora continua. Indudablemente, este enfoque no solo favorece el cumplimiento legal, sino que también optimiza el uso de los recursos institucionales, asegura la disponibilidad oportuna de los antecedentes y sustenta la toma de decisiones en entornos administrativos progresivamente digitalizados.

De este modo, las oportunidades de mejora aquí descritas constituyen insumos estratégicos para el diseño de planes de acción institucionales, programas de fortalecimiento documental o iniciativas de modernización orientadas a cumplir con las exigencias de la transformación digital del Estado.

1.2.3 Principales Señales de Alerta

Durante la implementación y evaluación de los procesos asociados a la planificación, ciclo de vida documental, incluyendo la eliminación regulada y el resguardo de la información, es posible **identificar condiciones institucionales que operan como señales tempranas de alerta**. Estas señales permiten anticipar debilidades operativas o normativas, **facilitando la adopción de medidas preventivas o correctivas en el marco de una adecuada gestión documental y de riesgos institucionales**. Entre las principales señales de alerta que podrían presentarse en instituciones públicas, se identifican a modo referencial las siguientes:



● **Ausencia de instrumentos técnicos de planificación documental:**

La inexistencia de políticas institucionales, TRD vigentes o manuales de procedimiento limita la coherencia del sistema de archivos y debilita el cumplimiento de estándares normativos y técnicos desde su etapa inicial.



● **Ausencia de procedimientos documentados para la eliminación de documentos:**

La inexistencia de protocolos formales o la presencia de prácticas no reguladas, sin resolución ni actas de eliminación, vulnera principios de trazabilidad y control institucional.



● **Falta de trazabilidad en el ciclo de vida documental:**

La ausencia de registro claro en etapas como la captura, clasificación o transferencia a archivo intermedio impide acreditar el tránsito, resguardo y disponibilidad de la documentación institucional.



● **Inexistencia de criterios técnicos de valoración documental:**

La ausencia de parámetros normativos para decidir la conservación, eliminación o transferencia de documentos puede derivar en pérdidas de antecedentes con valor legal, administrativo o patrimonial.



● **Almacenamiento inseguro de información sensible:**

La inexistencia de medidas como control de acceso, respaldo digital o formatos estandarizados expone a la institución a riesgos de pérdida, acceso no autorizado o vulneración de datos personales y confidenciales.



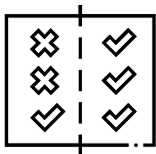
● **Uso de soportes no institucionales para documentos activos:**

El empleo de dispositivos personales o correos electrónicos particulares compromete la seguridad, integridad y legalidad del proceso documental.



● **Conservación prolongada de documentos fuera de los plazos normativos:**

La retención de documentos sin valor administrativo o más allá de lo establecido en la normativa vigente genera saturación de archivos, mayores costos operacionales y debilita la organización y recuperación documental.



● **Debilidad en la documentación de respaldo de procesos de eliminación:**

La existencia de actas incompletas, ausencia de certificados de destrucción o falta de registro institucional compromete la evidencia y control del proceso de disposición final.

**• Desconocimiento o interpretación disímil de la normativa vigente:**

La falta de comprensión homogénea de normas como por ejemplo la Ley N° 21.719, la Ley N° 21.180 y la Circular N° 28.704 puede dar lugar a prácticas no alineadas con el marco legal aplicable.

**• Falta de verificación sobre cumplimiento de plazos de conservación:**

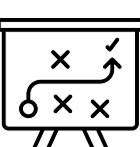
La inexistencia de mecanismos que controlen la vigencia de los documentos según las TRD puede derivar en omisiones graves o incumplimientos normativos.

**• Desactualización de inventarios o registros de archivo:**

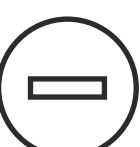
La omisión de revisiones periódicas limita la capacidad institucional de gestión, afecta la trazabilidad y dificulta la respuesta ante revisiones, solicitudes de transparencia o fiscalizaciones.

**• Baja integración entre sistemas físicos y digitales:**

La falta de sincronización entre plataformas genera duplicidades, retrasa el acceso y debilita el resguardo de la información institucional.

**• Falta de procedimientos de clasificación y categorización documental:**

La carencia de criterios institucionales funcionales o temáticos dificulta la organización, recuperación oportuna y conservación adecuada de los documentos.

**• Falta de políticas institucionales en materia de gestión documental:**

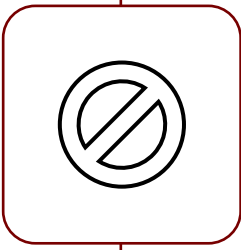
La ausencia de lineamientos formales sobre digitalización, conservación y eliminación documental genera dispersión de criterios, inseguridad jurídica y prácticas discrecionales.

**• Uso de plataformas no certificadas para almacenamiento documental:**

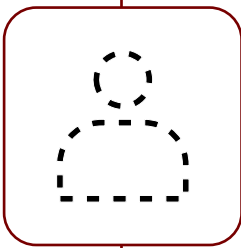
El empleo de sistemas transitorios o sin validación normativa para conservar documentos operativos o legales compromete su valor probatorio y la conservación institucional.



● **Ausencia de planes de respaldo o recuperación ante contingencias:**
La inexistencia de protocolos de respaldo, recuperación y continuidad operativa frente a incidentes técnicos, desastres naturales o fallos de infraestructura compromete la disponibilidad e integridad de los documentos institucionales.



● **Exclusión de la gestión documental del sistema de control interno:**
La omisión en matrices de riesgo, mapas de procesos o revisiones internas dificulta la supervisión de procesos críticos y limita las posibilidades de mejora continua.



● **Ausencia de designación formal de responsables de gestión documental:**
La omisión de revisiones periódicas limita la capacidad institucional de gestión, afecta la trazabilidad y dificulta la respuesta ante revisiones, solicitudes de transparencia o fiscalizaciones.



● **Almacenamiento físico en espacios no habilitados:**
El uso de bodegas, oficinas o recintos sin condiciones técnicas apropiadas afecta la integridad de los documentos y su valor legal o administrativo.

Finalmente, estas señales deben ser consideradas como indicadores estratégicos para la evaluación del nivel de madurez del proceso de gestión documental institucional, permitiendo a los funcionarios responsables identificar desviaciones críticas respecto del marco normativo, la gobernanza y el control interno, y contribuir así a la mejora continua del cumplimiento, integridad y transparencia institucional.

Capítulo 2

FUNDAMENTOS TEÓRICOS

Capítulo 2

FUNDAMENTOS TEÓRICOS

La gestión documental en el sector público se sustenta principalmente en el de ciclo de vida de los documentos, entendido como el conjunto de etapas por las que transita la información institucional desde su creación hasta su disposición final. En este contexto, el enfoque adoptado permite planificar el uso y tratamiento de los documentos de acuerdo con criterios de valor administrativo, legal o patrimonial, en coherencia con la normativa vigente y los estándares internacionales aplicables. Desde una perspectiva técnica, se distinguen tres tipologías principales:

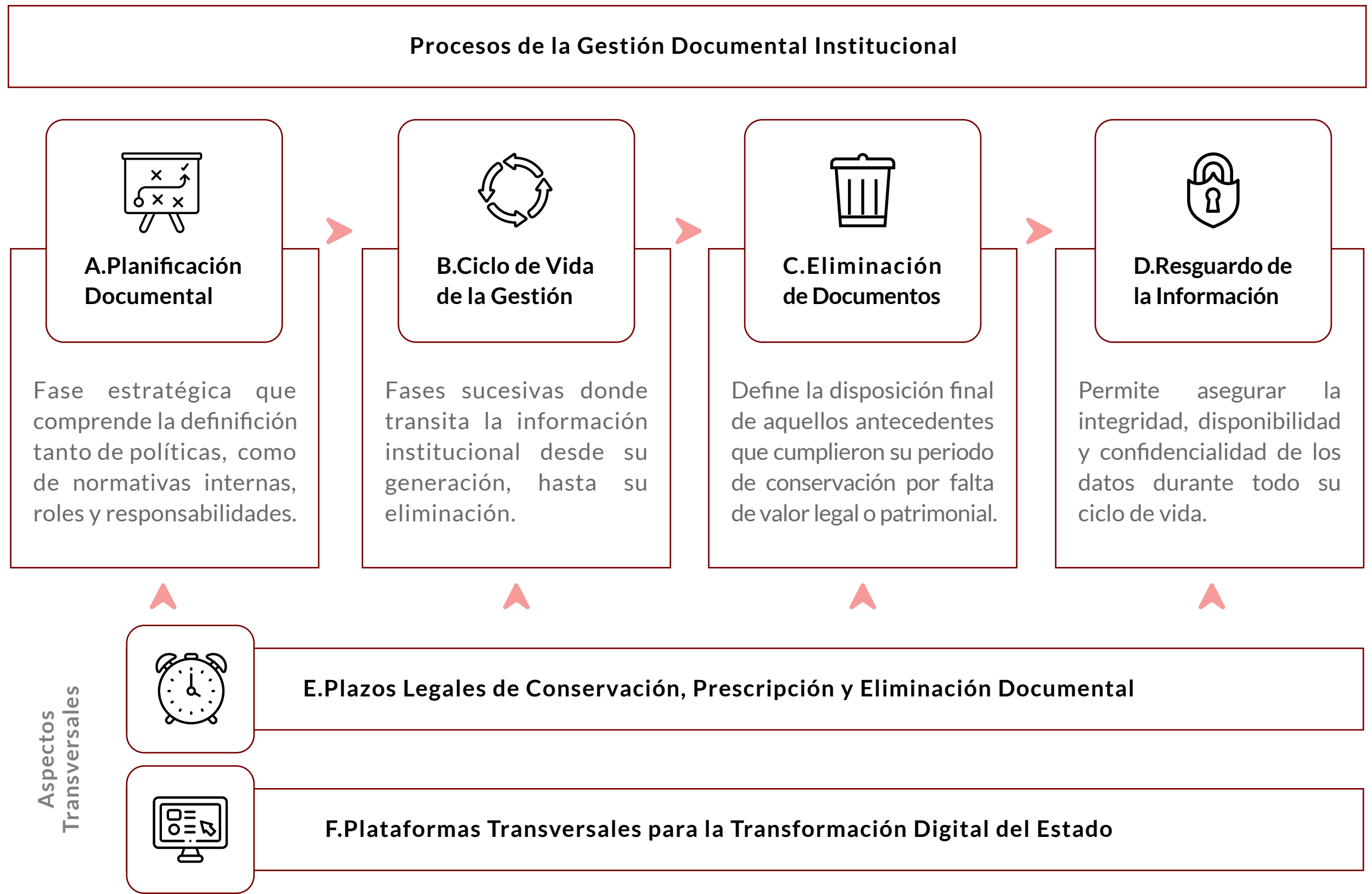
- Documentos de Uso Frecuente
- Documentos con Utilidad Residual
- Documentos sin Valor Operativo

A partir de esta clasificación, se aplican medidas diferenciadas para la conservación, transferencia o eliminación documental, lo que contribuye a optimizar recursos institucionales y a fortalecer la trazabilidad de la información pública.

A continuación se describen algunos procesos reelevantes que se desarrollan durante el ciclo de vida de los documentos:

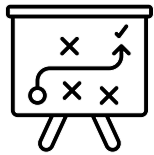
Proceso Relevante	Características
Clasificación Documental	Representa un eje fundamental para la definición de políticas de acceso, conservación y eliminación. En tal sentido, para su adecuada aplicación, deben considerarse factores como el tipo de información (pública, reservada, secreta, con datos sensibles, etc.), su nivel de criticidad y el valor institucional que representa. En consecuencia, resulta indispensable disponer de instrumentos técnicos, tales como cuadros de clasificación documental, que permitan establecer plazos de retención y criterios específicos de resguardo. De este modo, la categorización favorece la aplicación de controles proporcionales al riesgo y facilita la toma de decisiones ajustadas al marco normativo vigente.
Eliminación Documental	La eliminación documental debe ejecutarse mediante etapas técnicas claramente definidas, que incluyen la valoración documental, la elaboración de inventarios justificativos y la autorización formal por parte del organismo competente. Para asegurar legalidad y trazabilidad, cada fase o etapa debe estar debidamente documentada, especialmente en los casos que involucren antecedentes con valor legal, administrativo o patrimonial. Por tanto, mantener evidencia verificable del cumplimiento normativo permite acreditar que la eliminación fue realizada conforme a las disposiciones establecidas por el Archivo Nacional y otras entidades fiscalizadoras.
Resguardo de la Información	En paralelo, el resguardo de la información requiere un enfoque integral que combine continuidad operativa y protección institucional. Desde el punto de vista técnico, esto implica implementar medidas de seguridad física y lógica, como controles de acceso, respaldos periódicos, monitoreo del estado de conservación y protocolos para situaciones de contingencia. Igualmente, es necesario establecer estructuras de responsabilidad interna que garanticen la sostenibilidad de estas medidas y su revisión periódica frente a posibles cambios tecnológicos o regulatorios.
Políticas Institucionales	De forma transversal, resulta imprescindible contar con políticas institucionales que estructuren y respalden los procedimientos definidos en materia de gestión documental. Que incorporen mecanismos de evaluación, mejora continua y monitoreo sistemático, junto con herramientas que permitan registrar, verificar y auditar los procesos vinculados a la conservación, eliminación y resguardo documental. Gracias a ello, se consolida una base organizativa alineada con los principios de legalidad, eficiencia y control interno, que fortalece la toma de decisiones en el contexto de una gestión pública moderna.

Ahora bien, con el fin de sistematizar el análisis de riesgos y controles, se presenta a continuación una desagregación analítica de los cuatro procesos clave definidos en este documento técnico: planificación documental, ciclo de vida de la gestión documental, eliminación regulada y resguardo físico y digital de la documentación institucional. Esta estructura permite abordar cada subproceso en profundidad, considerando sus principales objetivos, actividades operativas, riesgos críticos y controles orientadores, conforme al enfoque metodológico adoptado para este documento.



A. Planificación Documental:

> Constituye una fase estratégica que precede e informa el desarrollo de todas las etapas del ciclo de vida de los documentos, y comprende la definición de políticas, normativa interna, roles y responsabilidades, así como el establecimiento de instrumentos técnicos como las TRD y los cuadros de clasificación, criterios de resguardo y protocolos de disposición final.



Esta fase resulta esencial para garantizar una gestión documental coherente, trazable y alineada con los principios de legalidad, eficiencia administrativa y control interno. Su adecuada implementación permite anticipar riesgos documentales, definir controles proporcionales y asegurar que los documentos cumplan su función como evidencia de la gestión institucional, desde su creación hasta su disposición final. Por ello, antes de ejecutar procedimientos específicos, es indispensable contar con una base institucional sólida que oriente y sustente cada fase del ciclo de vida documental, favoreciendo el cumplimiento normativo, la trazabilidad y la mejora continua.

A continuación, se describen los componentes específicos de este proceso de planeación:

1. Definición de política institucional y normativa aplicable:

Corresponde a la elaboración de una política formal de gestión documental, aprobada por la autoridad institucional y alineada con los marcos legales vigentes (Ley N° 21.180, Ley N° 19.628, Circular N° 28.704 de la CGR, entre otros). Debe establecer principios rectores, roles, niveles de responsabilidad, recursos asignados y compromisos institucionales. Además, debe acompañarse de normativa interna que regule procedimientos específicos como clasificación, conservación, eliminación y acceso a la información.

2. Identificación de procesos y flujos documentales:

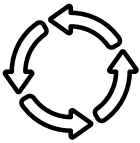
Implica el levantamiento sistemático de los procesos institucionales generadores de documentación, mapeando sus flujos, formatos y soportes utilizados. Este diagnóstico permite reconocer los puntos críticos donde es necesario aplicar controles documentales, asegurar el resguardo de la información y garantizar su trazabilidad. Asimismo, la identificación de flujos documentales es clave para estructurar series documentales coherentes y definir responsabilidades operativas.

3. Establecimiento de instrumentos técnicos:

Requiere la construcción o actualización de herramientas como el cuadro de clasificación documental (CCD) y las tablas de retención documental (TRD), conforme a los lineamientos del Archivo Nacional. Estos instrumentos permiten: organizar la documentación institucional por funciones, establecer plazos de conservación diferenciados y definir el destino final de los documentos (eliminación o transferencia). Por ende, su existencia y aplicación sistemática son condiciones habilitantes para una gestión documental eficiente y jurídicamente respaldada, y compatible con revisiones internas y externas.

4. Definición de recursos, estructura organizacional, roles y responsabilidades:

Consiste en identificar y asignar los recursos humanos, tecnológicos y presupuestarios necesarios para implementar y sostener el SGD. Asimismo, se deben establecer estructuras funcionales, como unidades de archivo o encargados responsables, y definir sus competencias, perfiles y articulación con otras áreas de la institución. La planificación de recursos garantiza la viabilidad operativa del modelo documental y contribuye a su institucionalización como parte de la función pública.



B. Ciclo de Vida de la Gestión Documental:

> La gestión documental en el sector público se articula en torno al concepto de ciclo de vida del documento, entendido como el conjunto de fases sucesivas por las que transita la información institucional desde su generación hasta su conservación definitiva o eliminación.

Este enfoque permite a las organizaciones públicas establecer procedimientos diferenciados de tratamiento documental (ej. conservación, resguardo y acceso), alineados con criterios de valor legal, administrativo y patrimonial, así como con las directrices técnicas emitidas por el Archivo Nacional.

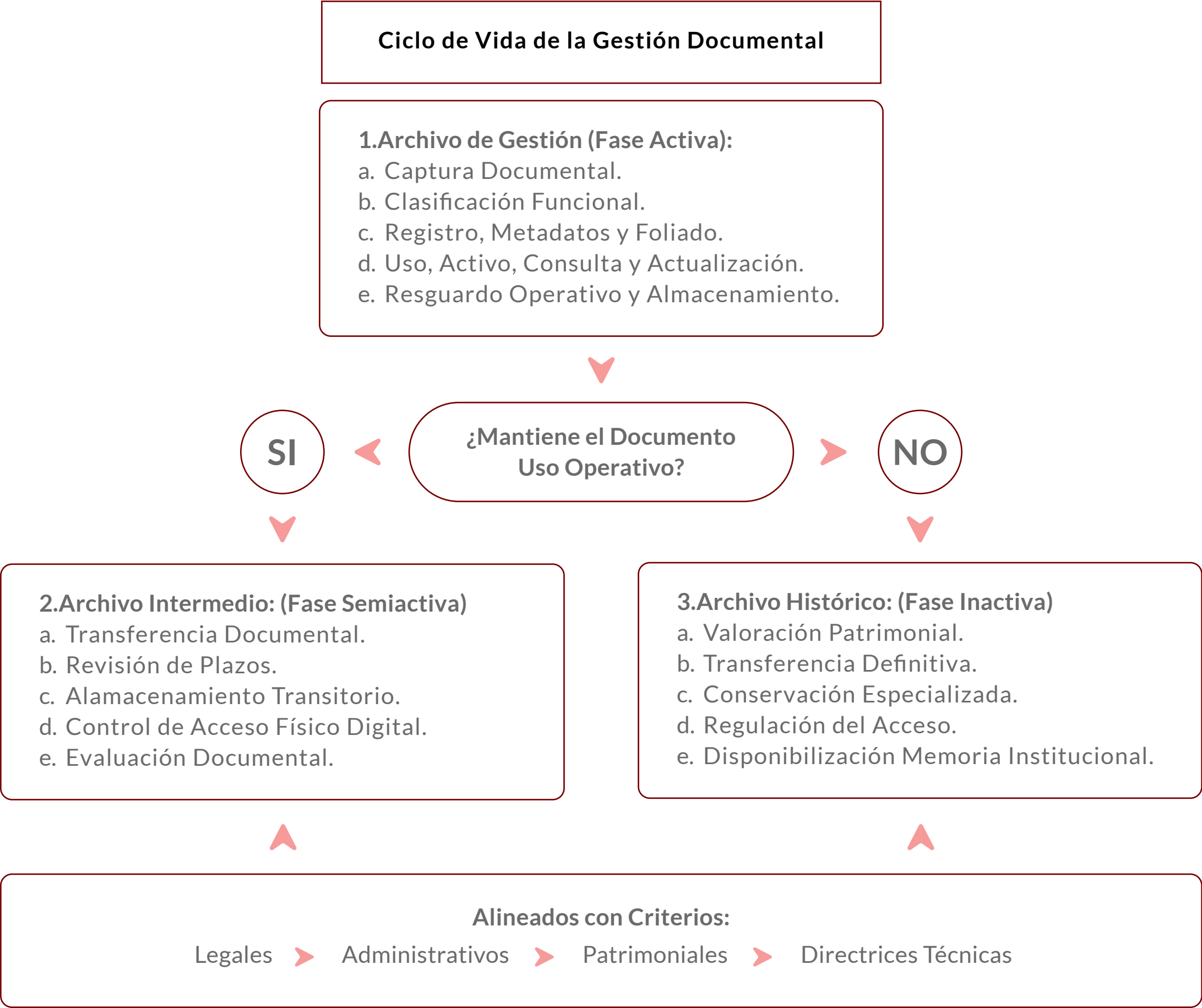


Figura N°2: El Ciclo de Vida de la Gestión Documental. Elaboración Propia.

El ciclo de vida documental se puede estructurar de distintas maneras, pero para efectos de este documento lo hemos organizado en tres fases fundamentales que son: archivo de gestión, archivo intermedio y archivo histórico. Cada una de estas fases responde a un momento específico en el uso y conservación de los documentos, permitiendo adoptar medidas técnicas y organizacionales proporcionales al nivel de vigencia y criticidad de la información contenida.

Con el propósito de fortalecer la aplicación práctica del modelamiento de riesgos y controles, este documento presenta una desagregación de las fases generales del ciclo documental en etapas operativas. Esta estructuración favorece la asignación de responsabilidades internas, facilita el control del flujo de información y refuerza la trazabilidad documental, contribuyendo a la implementación de controles adecuados, al cumplimiento normativo y al fortalecimiento del resguardo institucional de la documentación pública. A continuación, se describen las fases que conforman el ciclo de vida de la gestión documental institucional.

1. Archivo de Gestión (Fase Activa):

Corresponde a la fase inicial, en la cual los documentos son generados o recibidos por las unidades responsables y utilizados activamente como soporte para la ejecución de trámites, la toma de decisiones o el cumplimiento de funciones institucionales. Durante este periodo, los documentos deben mantenerse accesibles, organizados y protegidos, siendo objeto de clasificación, registro y consulta frecuente por los equipos responsables de su procesamiento. Esta fase constituye la base de la trazabilidad documental. Asimismo, establece un control riguroso sobre los documentos, facilitando su incorporación a los sistemas de gestión documental y su posterior transición hacia etapas de conservación o disposición final:

- **1A) Captura Documental y Registro Inicial:**

La captura representa el inicio del ciclo de vida documental e incluye tanto la generación interna de documentos como la recepción de aquellos provenientes de fuentes externas. Esta etapa abarca todos los registros que ingresan a la organización para respaldar actos administrativos, cumplir funciones legales o prestar servicios institucionales. En consecuencia, cada documento, físico o digital, debe ser formalmente incorporado al SGD institucional. Esta acción marca el punto de partida para su control, clasificación y seguimiento, reconociendo al documento como un activo informativo relevante para la operación institucional. Asegurando la trazabilidad desde el origen y facilitando el cumplimiento normativo.

- **1B) Clasificación Funcional:**

Posteriormente corresponde asignarle una categoría conforme al proceso institucional que le da origen bajo el proceso de clasificación funcional, que se lleva a cabo utilizando cuadros de clasificación documental definidos por la entidad o validados por el Archivo Nacional. Esto permite agrupar los documentos en series coherentes, vinculadas a funciones o actividades, facilitando su organización, recuperación y administración conforme a criterios técnicos y normativos.

- **1C) Registro, Metadatos y Foliado en Sistema de Gestión Documental:**

Posteriormente, el documento debe ser incorporado formalmente en los sistemas administrativos y de gestión documental institucional, incluyendo el registro de metadatos esenciales, tales como fecha de ingreso, tipo documental, unidad responsable, número de folio y código de clasificación. El registro y foliado garantizan la trazabilidad, evitando duplicidades, fortaleciendo la integridad y asegurando su adecuada localización dentro del sistema institucional.

- **1D) Uso Activo, Consulta y Actualización:**

El documento es utilizado con frecuencia por las unidades responsables como soporte para la toma de decisiones, la atención de requerimientos ciudadanos, revisiones o el cumplimiento de funciones legales y administrativas. La documentación se mantiene en constante consulta, puede ser actualizada o enriquecida con antecedentes complementarios y constituye evidencia esencial. Por tanto, debe mantenerse disponible, accesible y actualizada durante toda su vigencia operativa.

- **1E) Resguardo Operativo y almacenamiento en condiciones Seguras:**

En paralelo es indispensable aplicar medidas de resguardo como controles de acceso interno, organización física o digital adecuada, respaldo de la información y monitoreo básico de seguridad. Para prevenir la pérdida, deterioro o uso no autorizado del documento mientras conserva valor funcional, garantizando trazabilidad y cumplimiento normativo.

2. Archivo Intermedio (Fase Semiactiva):

Corresponde a la fase en la cual los documentos han perdido su uso operativo cotidiano, pero deben mantenerse en custodia institucional durante un período determinado por razones legales, administrativas o fiscales. Esta fase constituye un almacenamiento transitorio en el que los antecedentes documentales permanecen disponibles de forma controlada, hasta que se defina su disposición final. Su principal finalidad es descongestionar las unidades operativas sin comprometer información. Para ello, se deben aplicar condiciones adecuadas de conservación, tanto en entornos físicos como digitales y establecer mecanismos formales de registro, monitoreo y consulta, que permitan verificar la ubicación, contenido y vigencia de los documentos bajo resguardo. La correcta gestión del archivo intermedio contribuye a optimizar el volumen documental institucional, cumplir con las exigencias normativas y resguardar la continuidad administrativa.

- **2A) Transferencia desde Unidades Generadoras:**

Consiste en el traslado formal de documentos que han concluido su uso activo hacia la unidad de archivo intermedio. Esta transferencia debe estar autorizada y debidamente registrada, conforme a los procedimientos institucionales y a las orientaciones del Archivo Nacional. Aquí el objetivo es liberar espacio operativo y garantizar la custodia temporal de documentos que aún poseen valor legal, administrativo o fiscal.

- **2B) Revisión de Plazos de Conservación:**

Consiste en la verificación de los períodos definidos en las TRD u otros instrumentos normativos aplicables. Esta revisión permite determinar si los documentos han cumplido su plazo de conservación o si requieren permanecer bajo resguardo hasta que se defina su destino final. En esta etapa resulta clave aplicar criterios técnicos actualizados y garantizar la trazabilidad de la revisión.

- **2C) Almacenamiento Transitorio:**

Corresponde al resguardo físico o digital de los documentos durante su permanencia en el archivo intermedio. Esta etapa exige condiciones adecuadas de conservación, que aseguren la integridad, trazabilidad y disponibilidad controlada de la documentación. Por ende, se deben aplicar medidas proporcionales a la criticidad de los antecedentes y establecer mecanismos que permitan su localización y recuperación eficiente.

- **2D) Control de Acceso Físico o Digital:**

Corresponde a la implementación de restricciones de consulta en función del nivel de sensibilidad, confidencialidad o relevancia de los documentos almacenados. El acceso debe limitarse al personal autorizado y registrarse adecuadamente, resguardando así la confidencialidad institucional, los derechos de los titulares de la información y el cumplimiento de la normativa sobre protección de datos personales.

- **2E) Evaluación para Disposición Final o Transferencia Histórica:**

Comprende la preparación de inventarios y antecedentes técnicos que permitan determinar el destino definitivo de los documentos. Ahora, según su valoración institucional, esta evaluación definirá si los antecedentes deben ser eliminados de forma segura o transferidos al archivo histórico. Sin duda que esta etapa es clave para garantizar que la disposición final se realice con criterios normativos, técnicos y de transparencia.

3. Archivo Histórico (Fase Inactiva):

Representa el cierre del ciclo de vida documental y se caracteriza por la conservación permanente de aquellos documentos que han sido evaluados y seleccionados por su valor patrimonial, testimonial o institucional. Esta documentación, al formar parte del acervo histórico de la entidad, constituye una fuente insustituible para comprender la evolución de sus decisiones, funciones y actuaciones a lo largo del tiempo. Desde un enfoque técnico y normativo, la gestión del archivo histórico debe garantizar condiciones de preservación, seguridad y accesibilidad que permitan resguardar la integridad de los documentos a largo plazo. A su vez, requiere el desarrollo de políticas institucionales que regulen su consulta pública, su digitalización progresiva y su difusión responsable, promoviendo un equilibrio entre transparencia, conservación y protección de la información.

- **3A) Valoración Patrimonial:**

Corresponde al proceso técnico mediante el cual se determina si un documento debe ser conservado de forma permanente, para esto, considerando su relevancia histórica, jurídica, institucional o social. Esta valoración se basa en criterios definidos por el Archivo Nacional o por la propia institución, conforme a su marco regulatorio en específico.

- **3B) Transferencia Definitiva:**

Consiste en el acto formal por el cual los documentos seleccionados para conservación permanente son incorporados al archivo histórico institucional o transferidos al Archivo Nacional. Este proceso debe estar debidamente documentado y autorizado, asegurando la trazabilidad y legitimidad de la operación anteriormente mencionada.

- **3C) Conservación Especializada:**

Corresponde a la adopción de medidas técnicas específicas para preservar los documentos a largo plazo, tales como el control ambiental (temperatura, humedad, iluminación), la digitalización preventiva, y, cuando sea necesario, la restauración física. Estas acciones buscan asegurar la integridad y disponibilidad de los antecedentes patrimoniales de manera tanto física como digital.

- **3D) Regulación del Acceso:**

Corresponde a la definición de condiciones bajo las cuales la ciudadanía, investigadores u otros actores pueden consultar la documentación histórica. Estas políticas deben resguardar la integridad de los documentos y considerar tanto la normativa sobre protección de datos personales como las obligaciones de acceso a la información pública.

- **3E) Disponibilización para fines de Memoria Institucional:**

Consiste en fomentar el uso de los documentos históricos como recurso para investigaciones, procesos de fiscalización, acciones de transparencia, rendición de cuentas y fortalecimiento de la identidad institucional. De esta manera, el archivo histórico cumple una función activa en la consolidación de una cultura pública basada en la memoria y la legalidad.

C. Identificación de las Etapas Relativas a la Eliminación de Documentos:

> La eliminación de documentos constituye una etapa crítica dentro del ciclo de vida documental, debido a que define la disposición final de aquellos antecedentes que han cumplido su periodo de conservación y carecen de valor legal, administrativo o patrimonial.

Esta actividad se ubica funcionalmente en la fase de archivo intermedio, y debe desarrollarse conforme a criterios técnicos y jurídicos claramente establecidos por el Archivo Nacional, la CGR y otras entidades reguladoras. Sin embargo, por su nivel de criticidad, para efecto de este documento será tratado de forma independiente, ya que su correcta ejecución permite asegurar la legalidad, trazabilidad y respaldo institucional del proceso, minimizando riesgos asociados a la pérdida de información relevante, la eliminación indebida o la falta de evidencia documental.

Desde una perspectiva operativa, el proceso de eliminación se estructura en etapas sucesivas que van desde la identificación documental hasta el registro institucional de la eliminación, que permiten integrar el análisis del valor documental con la ejecución de medidas administrativas y técnicas. Esta segmentación facilita la aplicación de criterios diferenciados según el tipo de documento, su soporte y sus exigencias legales de conservación. A su vez, permite acreditar formalmente que la eliminación se realizó conforme a lo requerido por la normativa vigente, fortaleciendo el control interno y la transparencia institucional.

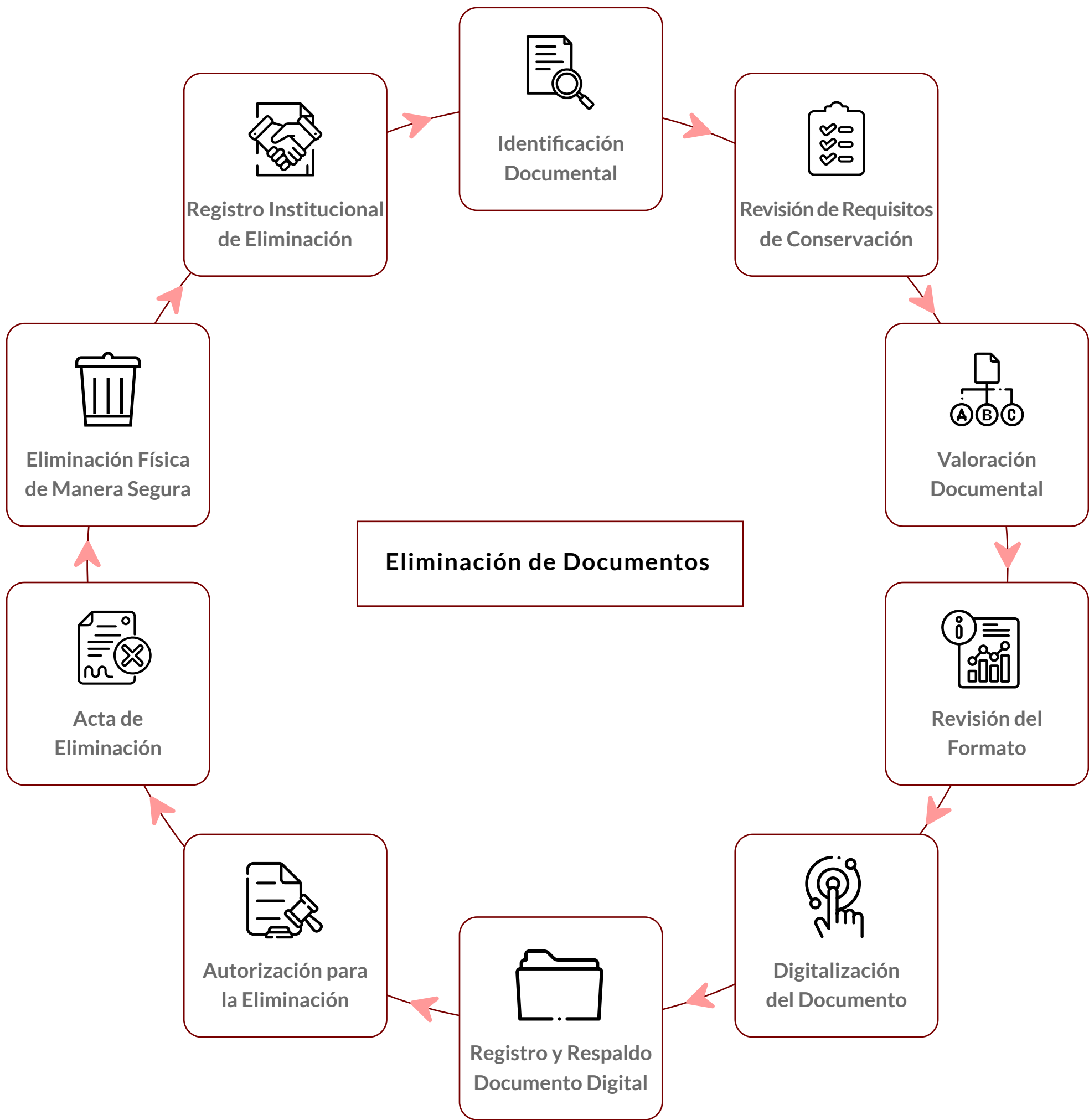


Figura N°3: Etapas de la Eliminación de Documentos. Elaboración Propia.

A continuación, se describen las etapas que conforman este proceso y los requisitos asociados a su correcta implementación.:

● **1) Identificación Documental:**

Esta etapa tiene como propósito la detección de los documentos que han cumplido con su vida útil desde el punto de vista administrativo, legal o informativo. Pues con este objetivo, las unidades responsables revisan sus archivos y registros para identificar aquellas series documentales que han dejado de tener uso frecuente y que han superado los plazos mínimos de conservación establecidos por la normativa vigente. A partir de dicha revisión, se elabora un listado preliminar de documentos que podrían ser eliminados. Esta lista se construye mediante el análisis del tipo de documento, su antigüedad y su relevancia actual para la gestión institucional, excluyendo aquellos que aún se encuentran en uso o vinculados a procedimientos activos. En síntesis, se busca organizar los antecedentes que requerirán evaluación posterior.

● **2) Revisión de Requisitos Legales y Plazos de Conservación:**

Una vez identificados los documentos, corresponde verificar si su eliminación está permitida conforme a las exigencias legales y normativas aplicables. En este análisis se consideran aspectos como el valor legal, fiscal, histórico o informativo del documento, así como la existencia de normativas sectoriales que exijan su conservación por períodos específicos. Se debe realizar una revisión documental detallada, contrastando la información disponible con la normativa vigente, incluyendo circulares, leyes sectoriales, instrucciones internas y directrices de organismos fiscalizadores. En caso de duda, debe primar el principio de precaución, resguardando la documentación hasta contar con certeza jurídica.

● **3) Valoración Documental:**

La valoración documental es un proceso técnico mediante el cual se determina el destino final de los documentos identificados. En este procedimiento se evalúa si los documentos deben conservarse de forma permanente, transferirse a un archivo histórico o ser eliminados definitivamente. Esto bajo criterios establecidos por el Archivo Nacional y la institución respectiva. Se consideran factores como la relevancia institucional del documento, su utilidad potencial para investigaciones futuras, su valor probatorio, su frecuencia de consulta y los costos asociados a su conservación. Así, se busca equilibrar la necesidad de resguardo con la eficiencia en la gestión documental.

● **4) Análisis del Formato:**

Posteriormente, se deben clasificar los documentos según su soporte, determinando si se trata de documentos físicos, digitalizados o digitales nativos. Esta distinción resulta esencial, ya que determina los procedimientos específicos que deben aplicarse para su eliminación conforme a la legislación vigente. Por ejemplo, los documentos físicos pueden ser eliminados una vez digitalizados, siempre que se cumplan los requisitos legales aplicables. En cambio, los documentos digitales nativos al no existir aún una normativa específica que regule su eliminación deben conservarse. En definitiva, esta revisión permite diseñar el proceso con base en el tipo de documento y su medio de almacenamiento, asegurando su integridad y trazabilidad.

● **5) Digitalización:**

Si los documentos a eliminar son físicos y se considera necesario conservar su contenido, corresponde su digitalización, la cual debe llevarse a cabo bajo los estándares de la Ley N° 18.845, respetando las exigencias de fidelidad del contenido. La digitalización implica la conversión del documento físico en una copia electrónica exacta, utilizando equipos y protocolos que aseguren la preservación del contenido original. Adicionalmente, se debe registrar el proceso detalladamente, incluyendo la fecha, el formato y el responsable de la digitalización.

● 6) Registro y Respaldo del Documento Digital:

Una vez completada la digitalización, los documentos deben ser formalmente incorporados a los sistemas de gestión documental institucional. Esto incluye su integración al expediente electrónico correspondiente y la verificación de que el archivo digital cumple con las condiciones de integridad, trazabilidad y disponibilidad exigidas por la Ley N° 21.180. Simultáneamente, se deben implementar mecanismos de respaldo y protección que prevengan la pérdida de información por fallas técnicas o accesos no autorizados. En términos de gestión documental, la consistencia de estos respaldos es fundamental para asegurar la seguridad y disponibilidad futura de los documentos.

● 7) Emisión de Resolución de Autorización para Eliminación:

En los casos de documentos en desuso o que hayan perdido su utilidad, debe emitirse una resolución administrativa que autorice la eliminación de los documentos. Este acto debe estar debidamente fundamentado, identificando con precisión los documentos que serán eliminados, su volumen, la normativa aplicable y los responsables del procedimiento. Adicionalmente, esta resolución debe ser firmada por la jefatura superior del servicio o la autoridad competente, y su contenido debe ajustarse a lo establecido en la Circular N° 28.704 de la CGR. En consecuencia, la resolución forma parte esencial del respaldo institucional del proceso de eliminación y debe quedar registrada para su eventual revisión.

● 8) Elaboración de Acta de Eliminación:

La ejecución del proceso de eliminación debe quedar registrada mediante un acta formal que detalle todas las condiciones del procedimiento. Específicamente, se debe incluir la fecha del acto, el método de destrucción utilizado, el volumen de documentos eliminados y la identificación de los funcionarios intervinientes. Además, esta acta debe ser firmada por todos los participantes del proceso (en lo posible designar un funcionario como ministro de fe) y archivada como parte del expediente institucional. Si se estima necesario, también puede complementarse con evidencias gráficas o audiovisuales, con el fin de reforzar la trazabilidad y transparencia del procedimiento.

● 9) Eliminación Física Segura:

La eliminación física de los documentos debe realizarse utilizando métodos que aseguren la destrucción total e irreversible del soporte. Entre los métodos recomendados se encuentran la trituration, la desintegración, la incineración controlada, la disolución química, u otros procedimientos que garanticen que la información contenida no pueda ser recuperada. En caso de que la institución contrate a un proveedor externo para la destrucción, se debe exigir un certificado que acredite el cumplimiento del servicio. Además, deben observarse criterios medioambientales y de confidencialidad, especialmente cuando los documentos contienen datos personales o sensibles. Es fundamental que el proceso sea supervisado por personal autorizado institucionalmente.

En este mismo contexto, la destrucción de documentos públicos que contienen información clasificada como secreta, reservada o con datos personales sensibles debe abordarse con especial rigor normativo, técnico y ético, dada su relevancia para la protección de derechos fundamentales, la seguridad nacional y el cumplimiento de principios de transparencia y responsabilidad institucional.

Según lo señala la Asesoría Técnica Parlamentaria de la Biblioteca del Congreso Nacional de Chile (2023), en nuestro ordenamiento jurídico chileno no existe una norma única y general que regule la destrucción de este tipo de documentación. En su lugar, se aplica un marco normativo fragmentado y sectorial, compuesto por leyes especiales, reglamentos, decretos y jurisprudencia administrativa, que establecen disposiciones diferenciadas en función del tipo documental, soporte físico o electrónico, y ámbito institucional de origen. En todos los casos, la eliminación de documentos clasificados o que contengan datos sensibles debe ser previamente valorada, justificada técnicamente y autorizada conforme a derecho, manteniendo siempre el principio de legalidad y el deber de custodia institucional hasta su destrucción material.

- **10) Registro Institucional de Eliminación:**

Finalmente, se debe compilar y conservar toda la documentación asociada al procedimiento de eliminación. Esta documentación incluye la resolución de autorización, el acta de eliminación, los certificados de destrucción y cualquier otro antecedente que respalde el proceso. Este expediente debe ser almacenado por la unidad de archivo o gestión documental, de acuerdo con los plazos definidos por la institución. En términos de control interno, su función principal es proporcionar trazabilidad y respaldo ante eventuales revisiones, fiscalizaciones o requerimientos de información pública, asegurando una entrega oportuna y documentada de los antecedentes requeridos.



D. Identificación de los Aspectos Relevantes del Resguardo de la Información:

> Constituye un componente fundamental y transversal dentro de la gestión documental ya que permite asegurar la integridad, disponibilidad y confidencialidad de los datos durante todo su ciclo de vida. En términos prácticos, esta función se materializa mediante la adopción de medidas organizacionales, procedimentales y tecnológicas, destinadas a proteger los documentos frente a accesos no autorizados, pérdidas accidentales o deterioro por condiciones inadecuadas de almacenamiento.

Cabe destacar que esta función no se limita a la fase final del proceso documental, sino que debe estar presente desde la captura inicial de los documentos hasta su conservación o eliminación, integrándose como una dimensión transversal del sistema institucional de gestión de la información.

Desde esta perspectiva, se identifican aspectos clave que permiten fortalecer las capacidades institucionales en materia de resguardo. Entre estos se incluyen la definición de responsabilidades internas, la delimitación de accesos conforme a perfiles, el diseño de planes de respaldo y recuperación ante fallos, así como la aplicación de controles periódicos sobre la infraestructura tecnológica y los soportes documentales.

Asimismo, resulta fundamental establecer lineamientos normativos internos que regulen el tratamiento de la información en sus distintos formatos, considerando criterios como sensibilidad, criticidad y vigencia. En conjunto, esta aproximación favorece el cumplimiento de los marcos legales vigentes, refuerza la continuidad operativa de los servicios públicos y promueve una administración responsable y segura de la información institucional.

1. Levantamiento y Clasificación de Información Sensible:

El primer paso para asegurar el resguardo es identificar y clasificar los datos almacenados institucionalmente. En este proceso se deben diferenciar categorías como información pública, datos personales y datos sensibles, garantizando que cada tipo cuente con medidas de protección adecuadas. En particular, una correcta clasificación permite establecer niveles de acceso y restricciones según su criticidad, en concordancia con la Ley N° 19.628 y la Ley N° 21.719.

Con ese propósito, se deben definir criterios claros de categorización, asignando responsabilidades a cada unidad o departamento. Además, es recomendable utilizar tecnologías de etiquetado de datos que faciliten su trazabilidad y permitan aplicar controles de acceso adecuados. Posteriormente, se debe actualizar periódicamente la clasificación, incorporando nuevas categorías o ajustes conforme a cambios normativos. Esta sistematización, cuando es integrada al SGD, refuerza la seguridad y eficiencia del manejo institucional de la información.

2. Diagnóstico de Riesgos y Planificación de Medidas de Protección:

Con el fin de fortalecer la seguridad de la información, resulta esencial realizar un diagnóstico de riesgos que permita identificar posibles vulnerabilidades en su tratamiento. Para ello, se recomienda aplicar Evaluaciones de Impacto en Protección de Datos Personales (EIPDP), que analizan los riesgos asociados al uso de la información y permiten establecer medidas de mitigación pertinentes. Este análisis debe repetirse periódicamente y ajustarse a los avances tecnológicos y actualizaciones normativas.

Sobre esa base, una planificación adecuada permitirá definir estrategias claras de prevención frente a incidentes de seguridad, asignando funciones y responsabilidades al interior de la organización. Asimismo, la incorporación de criterios de evaluación y monitoreo facilita la implementación de planes de acción que garanticen la continuidad operativa y el cumplimiento de las exigencias establecidas por la Agencia de Protección de Datos Personales (APDP).

● 3. Diseño e Implementación de Políticas de Resguardo y Acceso:

Constituyen un pilar esencial para asegurar el cumplimiento normativo y la protección de la información. Estas políticas deben incluir principios de seguridad de datos, regular procedimientos de acceso y almacenamiento, y establecer mecanismos formales de notificación y respuesta ante incidentes de seguridad. Adicionalmente, se recomienda que estas políticas incorporen medidas específicas para recuperación de datos y continuidad operativa, fortaleciendo la resiliencia institucional frente a fallas o ciberataques. Las políticas deben formalizarse mediante directrices internas y difundirse entre el personal a través de capacitaciones, protocolos operativos y manuales institucionales.

● 4. Implementación de Medidas de Seguridad y Continuidad Operativa:

En esta dimensión, las entidades públicas deben adoptar tecnologías y procedimientos que garanticen la seguridad de la información institucional. Esto incluye el uso de sistemas de autenticación multifactorial, cifrado de datos sensibles y monitoreo continuo, con el fin de prevenir accesos no autorizados. A la par, la incorporación de herramientas de detección de amenazas facilita una respuesta oportuna ante incidentes de seguridad.

Adicionalmente, los planes de continuidad operativa deben contemplar mecanismos de respaldo y recuperación de información que garanticen su disponibilidad. Para ello, resulta indispensable realizar pruebas periódicas de recuperación y mantener actualizados los planes de contingencia, minimizando así el impacto de interrupciones en procesos críticos institucionales.

● 5. Monitoreo, Revisiones y Evaluación de Impacto:

El monitoreo y la evaluación permanente de los sistemas de seguridad resultan esenciales para detectar brechas y fortalecer los mecanismos de control. En este sentido, se sugiere implementar indicadores de cumplimiento y reportabilidad, alineados con los estándares definidos por la Agencia de Protección de Datos Personales y con buenas prácticas internacionales.

Asimismo, las revisiones internas y externas permiten evaluar el cumplimiento normativo y detectar áreas de mejora. Estas acciones deben programarse con una frecuencia definida, documentar los hallazgos y establecer medidas correctivas, garantizando la trazabilidad y mejora continua de los sistemas de seguridad de la información.

● 6. Generaciones de Reportes y Mejora Continua:

El proceso de protección de datos debe contemplar la generación de reportes técnicos que respalden la toma de decisiones informadas. En dichos reportes debe incluirse información sobre incidentes de seguridad, evaluaciones internas y nivel de cumplimiento de obligaciones legales, lo que permite identificar oportunidades de mejora.

A su vez, la mejora continua debe constituirse como un principio rector en la gestión del resguardo de la información. Esto implica actualizar periódicamente las políticas, procedimientos y tecnologías, incorporando nuevas regulaciones y herramientas que refuercen la seguridad institucional y la protección de datos personales.

● 7. Gestión de Cumplimiento y Sanciones:

Con el objetivo de garantizar el cumplimiento normativo en materia de protección de datos, las instituciones deben establecer mecanismos de supervisión que permitan detectar, registrar y corregir eventuales incumplimientos. Entre ellos, resulta útil definir un régimen interno de sanciones que clasifique faltas leves, graves o muy graves, y que aplique medidas correctivas proporcionales.

Por otra parte, es recomendable implementar planes de gestión de riesgos legales, orientados a prevenir sanciones externas y reducir la exposición institucional a multas por parte de la APDP.



E. Plazos Legales de Conservación, Prescripción y Eliminación Documental:

> La regulación chilena sobre conservación y destrucción de documentos establece plazos diferenciados según la naturaleza del documento, el soporte, la función administrativa que cumple y, en ciertos casos, su valor histórico o cultural.

Estos plazos se encuentran dispersos en diversas normas, desde circulares de la CGR y Archivo Nacional hasta leyes sectoriales, lo que obliga a las instituciones a contar con criterios claros para garantizar el cumplimiento legal y la preservación de la memoria institucional. Sin duda, que el respeto a estos plazos no solo asegura la disponibilidad de la información para fines administrativos, jurídicos y probatorios, sino que también previene la eliminación indebida de antecedentes con valor patrimonial o que contengan datos sensibles.

La Circular N° 28.704 de 1981 de la CGR fija reglas generales y especiales para la eliminación, estableciendo que la autorización para eliminar corresponde, en lo medular, al Presidente de la República en los Servicios de la Administración propiamente tal, y a la jefatura superior en organismos con autonomía administrativa (mediante decreto o resolución exenta).

Entre sus disposiciones se encuentran por ejemplo: los libros, documentos y cuentas sujetos a control deben conservarse por tres años contados desde su revisión definitiva por la CGR, salvo reparos u observaciones pendientes (en cuyo caso se mantienen hasta su finiquito); los documentos vinculados a deuda pública, especies valoradas y efectos análogos se conservan dos años desde su examen por la CGR y su destrucción requiere la intervención del Contralor o delegado; los documentos ministeriales que alcancen cinco años, y las actas municipales con más de sesenta, se remiten al Archivo Nacional (teniendo en cuenta su capacidad de recepción y las normas de selección); los antecedentes de personal se recomiendan de conservación indefinida, pudiendo prescindirse de documentos con más de cinco años si la información consta íntegra en fichas, libros o tarjetas individuales; los documentos operacionales se conservan cinco años; los representativos de obligaciones pendientes se mantienen incluso después de la extinción de la obligación, hasta que los órganos de control concluyan sus exámenes. La Circular, además, recomienda que la destrucción se disponga por acto administrativo y se documente mediante acta, siguiendo los principios también reforzados por la Circular N° 51, que imparte disposiciones y recomendaciones sobre conservación, transferencia y eliminación de documentos, con énfasis en la correcta selección documental y en la obligación de remitir al Archivo Nacional los documentos con valor histórico o permanente.

Por su parte, el tratamiento de documentos secretos o reservados se rige por la Ley N° 20.285, que en términos generales, señala que la calificación de secreto o reserva (dispuesta por ley de quórum calificado o normas reconocidas como tales) conlleva custodia en condiciones de preservación y seguridad por un plazo de diez años, prorrogable por cinco años adicionales tras evaluación del peligro de daño por divulgación. En materias de defensa nacional, integridad territorial y política exterior grave, la ley prevé supuestos de secreto o reserva de carácter indefinido.

Respecto de documentos originales en papel que han sido microcopiados o micrograbados, el Decreto con Fuerza de Ley N° 1 de 2020 (dictado en el marco de la Ley N° 18.845) autoriza su destrucción transcurridos diez años desde la elaboración de la microforma, con excepciones para casos en que el Archivo Nacional se oponga fundadamente por su valor histórico o cultural, o en que existan restricciones legales específicas (por ejemplo, tributarias).

En cuanto a la disposición de bienes muebles en desuso en los servicios de la Administración del Estado (categoría que, una vez cumplidas las normas archivísticas, puede incluir papel y archivos en desuso), se encuentra regulada actualmente por el Decreto Supremo N° 662 de 2025 del Ministerio de Hacienda, el cual establece que los bienes dados de baja por no ser necesarios para el cumplimiento de los fines institucionales podrán ser dispuestos mediante resolución o acto fundado y, de ser reutilizables, deberán ofrecerse gratuitamente a otros organismos a través de la plataforma de economía circular, informando sus características, estado, valor y condiciones de manejo, así como resguardando su custodia hasta la entrega material. La documentación oficial, en todo caso, continúa sujeta a las normas especiales de conservación, transferencia y eliminación que le sean aplicables antes de poder ser tratada como bien mueble en desuso.

En materia previsional, el Decreto Ley N° 2.412 de 1978 permite la destrucción de documentación (incluida la que contiene datos sensibles) una vez microfilmada o reproducida electromagnéticamente, previa autorización expresa de la Superintendencia de Seguridad Social.

● 1) Tributario - Contable:

En el ámbito tributario y contable, los plazos de conservación y eventual eliminación varían según el tipo de registro documental, por ejemplo: los libros contables principales, como el Libro Diario, Libro Mayor y los Estados de Situación Financiera (denominados anteriormente “Balances Generales”), suelen mantenerse de forma permanente o, como mínimo, hasta que transcurran tres años desde su revisión definitiva y aprobación por la CGR, conforme a la Ley N° 10.336, y en ciertos casos durante toda la existencia de la entidad. De igual forma los estados financieros y cuentas anuales aprobadas siguen igualmente la regla de los tres años posteriores a su revisión definitiva como mínimo legal, aunque en la práctica suelen custodiarse por períodos más extensos debido a su valor histórico y de referencia. Mientras que los registros auxiliares y comprobantes de respaldo, como facturas, boletas y recibos, se conservan habitualmente por cinco años desde el cierre del ejercicio, salvo que se trate de documentos sujetos a los plazos de prescripción establecidos en el Código Tributario, entre ellos, el plazo general de seis años para la fiscalización por parte del SII, el cual prevalece sobre cualquier otro en materia tributaria.

Dichos plazos también se vinculan a condiciones técnicas específicas, como la microcopia conforme a la Ley N° 18.845, cuya aplicación requiere cumplir con las autorizaciones y requisitos de integridad y autenticidad establecidos. Ahora, cumplido el período de seis años exigido por el SII, y siempre que no exista fiscalización, proceso administrativo o judicial pendiente, la destrucción de los libros y respaldos contables deja de estar sujeta a sanción tributaria, sin perjuicio de que, por su valor histórico o referencial, muchas entidades opten por su custodia por períodos más extensos.

● 2) Auditoría Interna:

En el ámbito de la auditoría interna en el sector público, no existe una norma única y transversal que fije de manera expresa y uniforme un plazo legal obligatorio para la conservación de informes finales, papeles de trabajo e información de respaldo, ya sea en formato físico o digital, de manera que permitan sustentar las conclusiones y hallazgos.

Las Normas Globales de Auditoría Interna (NOGAI), emitidas por Instituto de Auditoría Interna (IIA), no establecen plazos específicos, pero en su lugar, algunos estudios realizados³ proporcionan lineamientos generales como conservar durante un período razonable o mayores a cinco años en términos orientativos. En tal sentido, las NOGAI requieren que la función de auditoría interna defina y documente una política de retención alineada con la legislación vigente, regulaciones sectoriales y el valor institucional de la documentación. Ahora, en la práctica, la mayoría de las unidades de auditoría interna del sector público adoptan como estándar mínimo un periodo de cinco años desde la emisión del informe, lo que permite cubrir la mayoría de los plazos de prescripción administrativa y atender revisiones posteriores de la CGR u otros órganos de control. Sin embargo, algunas entidades optan por conservarlos por períodos más largos, dependiendo de la complejidad de la auditoría o si involucra materias que podrían derivar en acciones judiciales o sumarios.

En casos donde los papeles de trabajo contienen información sujeta a reserva o clasificada, o datos personales o sensibles, resultan aplicables las disposiciones de la Ley N° 20.285 sobre Acceso a la Información Pública y de la Ley N° 19.628 sobre Protección de la Vida Privada, lo que puede extender la custodia a diez años o más, según la naturaleza de la información y los riesgos asociados a su divulgación. Ahora, si la documentación se conserva en formato digital, deben cumplirse las exigencias de integridad, autenticidad y disponibilidad establecidas en la Ley N° 19.799 sobre Documentos y Firma Electrónica, asegurando que los archivos permanezcan íntegros, inalterados y accesibles durante todo el periodo definido.

Por otra parte, existen contextos sectoriales con requisitos más estrictos, tal es el caso de entidades públicas sometidas a supervisión de la Comisión para el Mercado Financiero (CMF), como bancos estatales u otras empresas públicas fiscalizadas, la Ley General de Bancos exige la conservación por un mínimo de seis años de toda documentación vinculada a operaciones registradas, lo que se extiende a los informes y papeles de trabajo de auditoría interna que respalden dichas operaciones. Este plazo también coincide con el establecido por el Código Tributario para la conservación de registros con implicancias fiscales, el cual prevalece sobre cualquier otro en materia tributaria.

En todos los casos, los papeles de trabajo e informes deben mantenerse mientras exista posibilidad de revisión, fiscalización o uso como evidencia en procesos administrativos o judiciales, y de acuerdo con las políticas internas de archivo del servicio respectivo. Asimismo, las mejores prácticas internacionales recomiendan no destruir documentación que contenga hallazgos relevantes pendientes de seguimiento o que haya servido de base para investigaciones, hasta la conclusión de dichas instancias. De esta manera, la política de conservación no solo cumple los requisitos legales y regulatorios, sino que también asegura la trazabilidad, transparencia y sustentabilidad de la función de auditoría interna.

● 3) Salud Pública:

En el ámbito de la salud pública, los plazos de conservación varían según el tipo de documento y su finalidad. En el caso de las fichas clínicas, la Ley N.º 20.584 y su reglamento (Decreto N.º 41 de 2012 del Ministerio de Salud) establecen que deben conservarse por un mínimo de quince años desde el último registro. Transcurrido ese plazo, su eliminación requiere procedimientos que aseguren la confidencialidad y la destrucción efectiva, con constancia en acta y, tratándose de prestadores institucionales públicos, mediante resolución administrativa. En cuanto a los registros de vacunación, incorporados desde 2017 al Registro Nacional de Inmunizaciones (RNI), carecen de un plazo de caducidad legal y se conservan de manera permanente por su relevancia epidemiológica y sanitaria. Mientras que los registros epidemiológicos, como las notificaciones obligatorias de enfermedades y reportes de brotes, no tienen plazo de eliminación fijado y, conforme al régimen general de archivos públicos, deben remitirse al Archivo Nacional transcurridos cinco años, manteniéndose como documentación histórica de valor científico. A su vez, los informes sanitarios, tales como fiscalizaciones o reportes técnicos de la autoridad de salud, se sujetan igualmente a la normativa general de archivos, resguardándose mientras conserven valor administrativo o probatorio y siendo transferidos posteriormente a archivos históricos. Respecto a la documentación administrativa hospitalaria, los antecedentes contables y tributarios, se aplican los mismos criterios que en el resto del sector público, es decir se guardan por los plazos previstos en el Código Tributario (tres años como regla general y seis años en casos de prescripción especial), mientras que los contratos, expedientes y resoluciones administrativas se archivan, al menos, por cinco años antes de su eventual transferencia al Archivo Nacional o eliminación conforme a la ley. En todos los casos, la conservación, sea en formato físico o digital, debe garantizar la integridad, confidencialidad y disponibilidad de la información durante todo el período legalmente exigido.

● 4) Fuerzas Armadas:

En el ámbito de las Fuerzas Armadas de Chile, los plazos de conservación de documentos se encuentran determinados por los Reglamentos de Correspondencia y Archivo de cada rama institucional, dictados por el Ministerio de Defensa Nacional, así como la demás normativa técnica aplicable en el sector público. En este sentido, los documentos de conservación permanente incluyen, entre otros, las órdenes y directivas generales, las resoluciones y decretos institucionales, los expedientes de personal, los antecedentes históricos y los registros vinculados a derechos humanos, los cuales se mantienen de forma indefinida en los archivos históricos institucionales. Mientras que los documentos operativos clasificados como secretos o reservados se conservan, al menos, por un período mínimo de diez años conforme a la Ley N.º 20.285 y su reglamento, plazo que puede prorrogarse mediante resolución fundada, resguardándose con las medidas de seguridad establecidas. A su vez, en el campo militar, el Reglamento de Correspondencia y Documentación del Ejército (RAA-03006) dispone que, al término del ciclo de archivo, la documentación clasificada como reservada o secreta debe ser destruida siguiendo los procedimientos de seguridad institucional y levantando el acta respectiva, que deja constancia de la autorización, fecha, método y responsables de la destrucción. Asimismo, tratándose de documentación generada en actividades de inteligencia a cargo de las Direcciones de Inteligencia de las Fuerzas Armadas o de Orden y Seguridad Pública, resulta aplicable la Ley N.º 19.974, que califica como secretos y de circulación restringida todos los antecedentes, informaciones y registros en poder de dichos organismos, permitiendo su desclasificación solo por resolución del Director o Jefe competente y estableciendo control externo por la CGR, Tribunales de Justicia y Cámara de Diputados mediante conductos y actuaciones reservadas; el deber de secreto se mantiene aun después del cese de funciones, con sanciones penales por su infracción. En consecuencia, las tablas de retención y los procedimientos de archivo deben armonizarse con este régimen: rotulado con base legal, accesos y trazabilidad reforzados, remisión por canales reservados, y, al cierre del ciclo, eliminación conforme a los reglamentos de correspondencia y archivo de cada rama, levantando el acta respectiva.

En cuanto, a los documentos administrativos ordinarios y financieros, así como informes operativos no clasificados, se mantienen por un plazo mínimo de cinco años desde su emisión o desde que dejan de tener vigencia, pudiendo eliminarse posteriormente con las autorizaciones correspondientes y previa formalización mediante actas de destrucción. Asimismo, en materia contable y tributaria, se aplican los mismos criterios que en el resto del sector público, es decir rigen los plazos establecidos en el Código Tributario y en las instrucciones del SII, que fijan una conservación mínima de tres a seis años según el caso, sin perjuicio de la aplicación de plazos internos más extensos por razones de control y auditoría.

También, la normativa institucional contempla la posibilidad de sustituir soportes físicos por microformas o copias electrónicas, conforme a la Ley N.º 18.845, siempre que se cumplan los requisitos de autenticidad e integridad documental y sin que ello autorice la destrucción de documentos de valor histórico o cultural. Ahora, cumplidos los plazos legales y siempre que no exista proceso judicial, administrativo o fiscalización pendiente, la eliminación de los documentos no permanentes puede autorizarse; no obstante, por su valor histórico, jurídico o estratégico, muchos son transferidos a los archivos históricos institucionales para su conservación indefinida.

● 5) Poder Judicial:

En el ámbito judicial, los plazos de conservación de documentos varían según la naturaleza y función del registro. En el caso de los expedientes judiciales afinados (causas concluidas), estos deben remitirse al Archivo Judicial correspondiente dentro de los tres meses siguientes a la orden de archivo, conforme al Código Orgánico de Tribunales, para su custodia indefinida o hasta su eventual traspaso al Archivo Nacional por su valor histórico. A su vez, Las sentencias y resoluciones se conservan permanentemente como parte de los expedientes, en libros copiadores y en registros electrónicos oficiales administrados por el Poder Judicial, garantizando su disponibilidad histórica. Mientras que los oficios, actas y registros administrativos asociados a la gestión judicial suelen conservarse, como mínimo, por cinco años, en concordancia con plazos de prescripción administrativa y laboral, pudiendo prolongarse su guarda en atención a su valor probatorio o institucional. Asimismo, la documentación contable y presupuestaria del Poder Judicial, sigue los mismos criterios que en el resto del sector público, es decir se rige por las exigencias de la CGR y el SII, manteniéndose habitualmente por seis años desde el cierre del ejercicio, salvo que medien auditorías o procesos en curso. Ahora, la eliminación de cualquier documento judicial o administrativo solo procede con autorización del Archivo Nacional, previa digitalización o microfilmación y publicación en el Diario Oficial.

● 6) Educación:

En el ámbito educativo, los plazos de conservación de documentos se encuentran determinados por la normativa general aplicable al sector público y por disposiciones específicas según el nivel educativo. El Decreto con Fuerza de Ley N° 5.200 de 1929 establece que los documentos oficiales de los organismos públicos con más de cinco años de antigüedad deben ser transferidos al Archivo Nacional, lo que implica que, como regla general, estos documentos no se eliminan, sino que pasan a una custodia permanente. A su vez, la Ley N° 18.845 autoriza la reproducción de documentos en formato digital o microfilmado con valor legal equivalente al original y permite la eliminación del soporte físico una vez transcurridos cinco años desde su reproducción, sin que ello modifique la obligación general de conservación de la información.

En el ámbito de la educación escolar, que comprende establecimientos municipales, de administración delegada y particulares subvencionados, la Ley N° 20.529 y la Circular N° 1/2014 de la Superintendencia de Educación disponen que los documentos y registros esenciales deben mantenerse disponibles por un período mínimo de cinco años para efectos de fiscalización. Este deber incluye libros oficiales como el libro de clases, registros de matrícula y calificaciones, actas de consejos y comités, expedientes de alumnos, reglamentos internos y documentación financiera asociada a la subvención. Sin perjuicio de ello, los registros académicos oficiales, tales como las actas de calificaciones finales, actas de promoción y licencias de enseñanza media, tienen carácter de conservación indefinida, debido a su valor probatorio y al respaldo que mantiene el Ministerio de Educación. Los expedientes de alumnos deben conservarse al menos hasta su egreso, siendo recomendable su archivo permanente.

En materia laboral, tanto para docentes como para personal administrativo, los contratos, finiquitos, registros de remuneraciones y cotizaciones previsionales deben conservarse durante toda la vigencia de la relación laboral y, a lo menos, por cinco años posteriores a su término. En el caso de establecimientos municipales, estos antecedentes suelen incorporarse a los archivos institucionales del sostenedor, quedando sujetos al régimen de conservación permanente propio del sector público.

Respecto de la educación superior, la Ley N° 21.091 faculta a la Superintendencia de Educación Superior para determinar la documentación que debe mantenerse disponible de forma permanente para fiscalización, lo que en la práctica se traduce en la conservación indefinida de registros académicos, administrativos y financieros esenciales. Las instituciones de educación superior conservan de manera permanente actas de títulos y grados, actas de exámenes de titulación, concentraciones de notas y fichas de alumnos, a fin de garantizar la certificación de estudios y la emisión de duplicados. En las universidades estatales, las resoluciones y decretos de titulación se transfieren al Archivo Nacional una vez transcurridos cinco años. En todos los niveles educativos, prevalece el principio de que los documentos oficiales con valor probatorio o histórico no deben eliminarse, sino conservarse de forma permanente, asegurando su trazabilidad y disponibilidad en el tiempo.

● 7) Seguridad Pública:

En el ámbito de la seguridad pública y, específicamente, en la gestión documental de las Policías, los plazos de conservación de documentos se encuentran determinados por los Reglamentos de Documentación y Archivo de cada institución, aprobados por los Decretos Supremos N° 322 y N° 323 de 2023 del Ministerio del Interior, así como por la demás normativa técnica aplicable en el sector público.

Respecto, a los documentos de conservación permanente incluyen, entre otros, las Órdenes Generales, las resoluciones institucionales, los antecedentes históricos, las materias de personal y los registros relacionados con derechos humanos, los cuales se mantienen de forma indefinida. A su vez, los partes policiales remitidos a tribunales se conservan al menos cinco años después de concluido el proceso judicial asociado, mientras que las denuncias y constancias no judicializadas, así como los informes operativos y demás documentos administrativos ordinarios, se mantienen por un plazo mínimo de diez años desde su emisión o desde que dejan de tener efecto, pudiendo ser eliminados posteriormente con las autorizaciones correspondientes.

En el caso de los registros audiovisuales obtenidos mediante cámaras corporales o sistemas de video vigilancia institucional, la Ley N° 21.638 establece una conservación mínima de dos años, salvo que se trate de material vinculado a investigaciones judiciales, en cuyo caso se resguarda por el período que determine el Ministerio Público. Asimismo, la normativa contempla la posibilidad de sustituir soportes físicos por microformas o copias electrónicas conforme a la Ley N° 18.845, siempre que se cumplan los requisitos de autenticidad e integridad documental. Cumplidos los plazos legales y siempre que no exista proceso judicial, administrativo o fiscalización pendiente, la eliminación de los documentos no permanentes puede autorizarse, sin perjuicio de que, por su valor histórico, jurídico o institucional, muchos sean transferidos al Archivo Nacional o conservados por períodos más extensos.



F. Plataformas Transversales para la Transformación Digital del Estado:

> En el marco de la Ley N°21.180 de Transformación Digital del Estado y su implementación gradual, el Gobierno de Chile ha desarrollado un conjunto de plataformas digitales transversales que permiten a los órganos de la Administración del Estado avanzar hacia la gestión completamente electrónica de los procedimientos administrativos. Estas herramientas no solo permiten cumplir con las disposiciones legales en materia de digitalización, sino que además fortalecen los sistemas institucionales de gestión documental, interoperabilidad, autenticación, trazabilidad y transparencia.

Las principales plataformas transversales son:

1. Identidad Digital:

- Clave Única: Sistema de autenticación digital obligatorio que permite a los órganos públicos validar la identidad de las personas en sus interacciones electrónicas, y constituye el mecanismo central para garantizar la integridad y autoría de las transacciones digitales y del acceso a expedientes electrónicos.
- FirmaGob: Plataforma estatal de firma electrónica avanzada dirigida a funcionarios públicos, que permite firmar digitalmente actos administrativos, resoluciones, oficios y documentos institucionales, fortaleciendo la trazabilidad y autenticidad documental conforme a lo dispuesto en la Ley N°21.180.

2. Digitalización de Trámites:

- CPAT (Catálogo de Procedimientos Administrativos y Tramitaciones): Herramienta oficial de caracterización y monitoreo de los procedimientos administrativos del Estado, la cual es clave para identificar procesos institucionales que deben ser digitalizados y para documentar su trazabilidad dentro del expediente electrónico.
- SIMPLE: Plataforma para la digitalización de trámites de baja complejidad, que facilita la automatización de procesos internos, aportando agilidad y eficiencia a los procedimientos administrativos y reduciendo el uso de papel.

3. Interoperabilidad Institucional:

- PISEE 1: Infraestructura estatal para integrar servicios electrónicos entre instituciones, habilitando la interoperabilidad en tiempo real entre plataformas públicas. Aunque no es de uso obligatorio, representa un primer paso hacia la conectividad institucional.
- PISEE 2: Plataforma obligatoria para el intercambio electrónico de datos, documentos y expedientes entre organismos públicos, conforme a los estándares de interoperabilidad definidos en la Ley de Transformación Digital, la cual permite el traspaso seguro de información interinstitucional, con control de acceso, trazabilidad y auditoría.

4. Comunicaciones Oficiales:

- DocDigital: Sistema oficial obligatorio para la emisión, recepción, distribución y archivo digital de comunicaciones entre organismos públicos. Esta reemplaza el uso del papel, asegurando una trazabilidad completa de oficios, resoluciones y demás documentos administrativos, y es la plataforma central para el cumplimiento del eje “Cero Papel” del Instructivo Presidencial.

5. Datos Abiertos:

- DatosGob: Repositorio de acceso público de datos gubernamentales en formato abierto. No obligatoria, esta herramienta complementaria promueve la transparencia y reutilización de información pública, incluyendo bases documentales institucionales.

6. Evaluación de Proyectos Tecnológicos:

- EvalTI: Plataforma de evaluación técnica de proyectos TI institucionales. Si bien no está vinculada directamente con la gestión documental, EvalTI cumple un rol estratégico en la validación técnica de iniciativas de digitalización que incluyen sistemas de archivos, expediente electrónico, gestión de documentos y plataformas interoperables.

Capítulo 3

MARCO REGULATORIO Y LEGAL

Capítulo 3

MARCO REGULATORIO Y LEGAL

La gestión documental en el sector público chileno se sustenta en un **entramado normativo que regula integralmente las etapas del ciclo de vida de los documentos institucionales y procesos relacionados**. En este contexto, el marco establece **criterios obligatorios** para su conservación, eliminación y resguardo, reconociendo que **cada fase requiere condiciones específicas** de trazabilidad, control y cumplimiento legal. En particular, la normativa vigente vinculada a la protección de la vida privada y al proceso de transformación digital del Estado busca asegurar que el tratamiento de la información pública se realice bajo principios de legalidad, transparencia, responsabilidad institucional y respeto a los derechos asociados a los datos contenidos en los documentos.

En lo relativo a la conservación, se establecen lineamientos para garantizar la custodia de los documentos mientras mantengan valor administrativo, legal o histórico. Para ello, deben aplicarse criterios técnicos de clasificación, preservación y acceso, conforme a lo determinado por el Archivo Nacional y por las TRD definidas institucionalmente.

En cuanto a la eliminación, la normativa dispone requisitos formales que obligan a fundamentar la disposición final mediante evaluaciones archivísticas y autorizaciones institucionales, especialmente en aquellos casos que involucren documentos con información personal o sensible.

En materia de resguardo documental, se requiere la implementación de medidas organizacionales, procedimentales y tecnológicas que aseguren la integridad, disponibilidad y confidencialidad de la información, tanto en soporte físico como digital. En consecuencia, este resguardo debe abordarse como una dimensión transversal del sistema documental, en coherencia con los principios establecidos en la Ley N° 21.180 sobre Transformación Digital del Estado y la Ley N° 19.628 sobre Protección de la Vida Privada.

Finalmente, el marco normativo se compone de leyes, reglamentos, resoluciones, instrucciones técnicas y dictámenes emitidos por organismos como el Archivo Nacional, la Contraloría General de la República y el Consejo para la Transparencia. En virtud de ello, **su aplicación efectiva requiere que cada institución cuente con procedimientos formalizados, personal capacitado y mecanismos de control interno** que aseguren el cumplimiento normativo en todas las etapas del ciclo documental.

3.1 NORMATIVA APLICABLE

A continuación, se expone una revisión de los principales cuerpos normativos, dictámenes, circulares e instructivos técnicos que conforman el marco regulatorio vigente en materia de gestión documental en el sector público. En términos funcionales, estos instrumentos definen criterios específicos para las distintas etapas del ciclo de vida de la documentación, incluyendo su conservación, eliminación y resguardo.

	Normativa
1.	Constitución Política de la Republica: El artículo 19 N°4 consagra como garantía constitucional el respeto y la protección a la vida privada y a la honra de la persona y su familia. En consecuencia, establece que el tratamiento de los datos personales debe realizarse conforme a lo dispuesto por la ley, imponiendo a los órganos públicos y privados la obligación de resguardar la privacidad de los ciudadanos en el manejo de su información. Asimismo, el artículo 8° establece el principio de publicidad como regla general en el actuar de los órganos del Estado. Según su inciso segundo, los actos y resoluciones de los organismos públicos, así como sus fundamentos y procedimientos, son de carácter público. No obstante, se faculta únicamente a una ley de quórum calificado para establecer excepciones mediante reserva o secreto, cuando la divulgación de dicha información comprometa el cumplimiento de funciones institucionales, los derechos de las personas, la seguridad de la Nación o el interés nacional. En este sentido, la gestión documental en el sector público debe armonizar el respeto a la privacidad con la transparencia institucional, conforme a los límites establecidos por la propia Constitución.

	Normativas
2.	Decreto N°2421 de 1964, del Ministerio de Hacienda, que fija el texto refundido de la Ley 10.336 de Organización y Atribuciones de la Contraloría General de la República: Este cuerpo legal establece atribuciones clave en materia de gestión y fiscalización documental. En particular, el artículo 7 fija la competencia exclusiva del Contralor(a) General, entre otras cosas, en el examen y juzgamiento de todas las cuentas de los empleados que custodien, administren, recauden o inviertan rentas, fondos o bienes fiscales, municipales y de la beneficencia pública, o de toda persona o entidad que deba rendir sus cuentas a la CGR o que esté sometida a su fiscalización. Bajo esta atribución el artículo 14 otorga al Contralor(a) General la facultad de adoptar las medidas que estime pertinentes para supervisar la destrucción o incineración de documentos vinculados a la deuda pública, especies valoradas u otros efectos similares. Por su parte, el artículo 21 impone a la CGR el deber de realizar el examen e inspección de los libros, registros y documentos relacionados con la contabilidad gubernamental. Además, dispone que aquellos antecedentes contables ya aprobados deben ser incinerados una vez transcurridos tres años desde su revisión definitiva, salvo que el propio Contralor(a) determine su conservación por razones de interés institucional. En consecuencia, esta normativa establece criterios concretos para la eliminación documental bajo supervisión de la CGR, asegurando el resguardo y legalidad del procedimiento.
3.	Ley N°19.628 de 1999, sobre Protección de la Vida Privada: Esta ley establece el marco normativo vigente en materia de tratamiento de datos personales en Chile. Asimismo, define el concepto de datos personales, regula su uso por parte de instituciones públicas y privadas, y consagra derechos fundamentales de los titulares, tales como el acceso, la rectificación, la cancelación y la oposición al uso de su información. En consecuencia, las instituciones públicas deben implementar medidas organizacionales, procedimentales y tecnológicas que aseguren el tratamiento seguro y conforme a los principios de licitud, finalidad y proporcionalidad. Entre estas medidas se incluyen controles de acceso, protocolos de almacenamiento y mecanismos de eliminación documental que resguarden la información frente a riesgos de filtración, pérdida o uso indebido. Asimismo, se exige que los datos sean utilizados exclusivamente para los fines establecidos y, en aquellos casos en que aplique, con el consentimiento informado de los titulares. En este sentido, el artículo 6 exige a los encargados del tratamiento de datos su eliminación o cancelación cuando su almacenamiento carezca de fundamento legal o cuando estos hayan caducado. En caso de incumplimiento, la ley contempla sanciones económicas y administrativas, así como eventuales responsabilidades civiles y penales para los funcionarios encargados. Por tal motivo, es esencial que los organismos públicos cuenten con políticas institucionales claras, realicen capacitaciones periódicas y adopten herramientas tecnológicas adecuadas para fortalecer la cultura de protección de datos y seguridad de la información. Una consideración importante a tener en cuenta es que, a la fecha de publicación de este documento, ya se encuentra promulgada la Ley N° 21.719, la cual regula el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Esta nueva normativa moderniza el régimen anterior, fortalece los derechos de los titulares, establece deberes más estrictos para los responsables y contempla un sistema sancionatorio robusto. No obstante, su entrada en vigencia está prevista para el 1 de diciembre de 2026. Por tanto, durante el periodo de vacancia legal se mantiene plenamente vigente la Ley N° 19.628 y sus disposiciones deben ser igualmente observadas por las instituciones del sector público.

	Normativas
4.	Ley N° 19.880 de 2003, que establece Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado: Esta ley regula los principios y procedimientos que deben observar los órganos públicos en su actuación administrativa. Por lo tanto, su observancia es fundamental para la gestión documental, en tanto establece las reglas generales sobre la conformación, conservación y acceso a los expedientes administrativos, así como los derechos que asisten a los ciudadanos durante su tramitación. Particular relevancia adquieren las disposiciones incorporadas por la Ley N° 21.180 sobre Transformación Digital del Estado, especialmente aquellas referidas al expediente electrónico y a los procedimientos tramitados mediante medios digitales. Al respecto, el artículo 16 bis establece los principios que deben regir estos procedimientos electrónicos, incluyendo legalidad, interoperabilidad, neutralidad tecnológica, accesibilidad y seguridad. Asimismo, el artículo 17 consagra los derechos de las personas frente a la Administración del Estado, como el derecho a una atención respetuosa, oportuna, accesible y a la información clara del estado de tramitación de sus solicitudes. Entre estos derechos, se incluye el acceso al expediente administrativo, que debe contener todos los actos, documentos y diligencias realizadas. Por su parte, el artículo 18 establece que los actos administrativos deben quedar debidamente registrados y formar parte de un expediente electrónico institucional, consolidando así la trazabilidad, el resguardo y la integridad documental a lo largo del procedimiento administrativo. Este marco refuerza la necesidad de contar con sistemas de gestión documental que sean compatibles con las exigencias del procedimiento electrónico, asegurando la custodia, disponibilidad y legalidad de la información generada o recibida en el marco de la actividad pública.
5.	Ley N° 20.285 de 2008, sobre Acceso a la Información Pública: Esta ley reconoce y garantiza el derecho de toda persona a acceder a la información en poder de los órganos del Estado, conforme lo establece su artículo 10. Dicho acceso se configura como un principio rector de la función pública, orientado a fortalecer la transparencia, la participación ciudadana y la rendición de cuentas. No obstante, este derecho admite excepciones fundadas en la protección de la seguridad nacional, los derechos de terceros o el adecuado cumplimiento de las funciones institucionales, entre otros. Desde la perspectiva de la gestión documental, esta normativa exige a los organismos públicos implementar sistemas que aseguren la disponibilidad, integridad y accesibilidad de los documentos que obran en su poder, en lo que respecta a la transparencia activa. Para ello, deben establecer criterios de clasificación, digitalización y custodia que permitan identificar qué información es pública, cuál debe ser reservada y por cuánto tiempo. En este marco, la gestión de archivos debe contemplar el desarrollo de procedimientos que garanticen una respuesta oportuna, fundada y proporcional a las solicitudes de acceso presentadas por la ciudadanía. En paralelo, la ley impone la obligación de proteger los datos personales contenidos en los documentos institucionales. Esto exige a las entidades públicas resguardar adecuadamente la información sensible, aplicar restricciones de acceso y adoptar medidas que eviten su divulgación indebida. De no cumplirse con estas obligaciones, los organismos pueden ser objeto de sanciones administrativas, e incluso enfrentar acciones legales por vulneración de derechos fundamentales. A su vez, esta ley establece las causales para declarar documentos como secretos o reservados, en conformidad con el artículo 8° de la Constitución Política, y exige su conservación mínima por diez años, salvo normas especiales que regulen su ingreso al Archivo Nacional. Por estas razones, resulta esencial que cada institución disponga de políticas internas claras, sistemas de gestión documental eficientes y plataformas tecnológicas que faciliten tanto el acceso legítimo a la información como el cumplimiento del deber de confidencialidad. Este equilibrio constituye un pilar para la transparencia activa, la confianza institucional y la buena administración pública.

	Normativas
6.	Ley N° 18.845 de 1989, establece Sistemas de Microcopia o Micrograbación de Documentos: Esta normativa establece el marco legal para la implementación de sistemas de microcopia o micrograbación como mecanismos válidos para la reproducción, conservación y respaldo de documentos, tanto en el ámbito público como privado. Su objetivo es permitir la sustitución de los documentos originales por copias microfilmadas, siempre que estas se generen conforme a requisitos técnicos específicos y bajo condiciones autorizadas por la autoridad competente. En virtud de esta ley, las copias obtenidas mediante procesos de microcopia debidamente autorizados y autenticados adquieren el mismo valor probatorio que los documentos originales. Para ello, deben cumplirse estándares de fidelidad, integridad y autenticación documental, resguardando así la validez jurídica del contenido reproducido. La normativa también establece que las instituciones que apliquen estos sistemas deben conservar registros del proceso de microfilmación y garantizar la trazabilidad de los documentos. Desde la perspectiva de la gestión documental en el sector público, esta ley constituye una herramienta relevante para la conservación de archivos, permitiendo reducir el volumen físico de almacenamiento, prevenir el deterioro de documentos originales y facilitar el acceso controlado a la información.
7.	Ley N° 21.180 de 2019, sobre Transformación Digital del Estado: Esta ley fue publicada en noviembre de 2019 y entró en vigencia desde el 9 de junio de 2022, en esta se establece que el ciclo completo de los procedimientos administrativos desarrollados por los órganos de la Administración del Estado debe ejecutarse en formato electrónico. Por lo tanto, su aplicación implica un cambio estructural en la forma de gestionar la información y los documentos públicos, consolidando la digitalización como principio rector de la función administrativa, con importantes implicancias para la gobernanza documental, la interoperabilidad institucional y la trazabilidad de las actuaciones del Estado. En tal sentido, la norma modifica las disposiciones de la Ley N°19.880 sobre bases de los procedimientos administrativos y promueve un modelo basado en expedientes electrónicos, comunicaciones oficiales digitales, notificaciones electrónicas y digitalización sistemática de documentos presentados en soporte papel. Esta transformación se realiza en base al principio de interoperabilidad, que exige a los organismos públicos asegurar la conexión e intercambio de datos entre plataformas, garantizando seguridad, eficiencia y continuidad operativa. Ahora, uno de los elementos centrales de esta legislación es la creación y mantenimiento de expedientes electrónicos, que deberán registrar todas las actuaciones asociadas a un procedimiento administrativo, respetando los principios de integridad, disponibilidad, trazabilidad y confidencialidad de la información. Además, cualquier ingreso, solicitud o documento que forme parte de un procedimiento administrativo debe realizarse mediante plataformas electrónicas oficiales, salvo que el solicitante esté imposibilitado de utilizar medios digitales, en cuyo caso el órgano deberá realizar la digitalización correspondiente e integrarla al expediente electrónico. Esta ley establece también una gradualidad de implementación, regulada mediante el DFL N°1 de 2020, del Ministerio Secretaría General de la Presidencia y modificada por la Ley N°21.464 de 2022, que introduce una nueva fase de preparación, la que obliga a los servicios públicos a identificar, caracterizar y registrar sus procedimientos administrativos en el Catálogo de Procedimientos Administrativos y Trámites (CPAT), herramienta oficial puesta a disposición por la División de Gobierno Digital. Las etapas posteriores deberán implementarse progresivamente, con plazo final al 31 de diciembre de 2027. Desde una perspectiva de gestión documental, la Ley N°21.180 exige que cada institución del Estado cuente con políticas, procesos y sistemas adecuados para la producción, clasificación, digitalización, acceso, conservación, transferencia y eliminación de documentos en formato digital, conforme a los estándares de transparencia, probidad, eficiencia y control exigidos por la normativa chilena y los principios internacionales de gestión documental.

	Normativas
8.	Decreto con Fuerza de Ley N° 1 de 2021 del Ministerio Secretaría General de la Presidencia: Como se mencionó precedentemente, este decreto reglamenta la aplicación del artículo 1° de la Ley N° 21.180 sobre Transformación Digital del Estado, estableciendo la gradualidad y condiciones bajo las cuales los organismos públicos deben implementar procedimientos administrativos electrónicos. Define criterios operativos para la adopción de sistemas digitales, con plazos diferenciados según el grupo al que pertenezca cada entidad. Entre los componentes clave de la implementación, se destacan los siguientes: •Comunicaciones oficiales electrónicas: Registro obligatorio de las comunicaciones interinstitucionales en plataformas como DocDigital. •Notificaciones electrónicas: deberán realizarse a través de medios digitales, vinculados al Servicio de Registro Civil e Identificación. •Ingreso digital de procedimientos administrativos: toda solicitud o documento deberá presentarse electrónicamente. •Expedientes electrónicos: cada procedimiento debe tener un expediente íntegramente digital. •Digitalización de documentos físicos: en casos excepcionales, los documentos en papel deben ser digitalizados por el órgano correspondiente. •Interoperabilidad y ciberseguridad: las plataformas utilizadas deben cumplir con estándares definidos por el reglamento, incluyendo interoperabilidad, trazabilidad, respaldo e integridad. Además, confiere validez jurídica a los actos administrativos tramitados por medios digitales, y dispone que todo procedimiento regulado por ley especial se someta progresivamente a los lineamientos de la Ley N° 21.180. De este modo, el decreto fortalece la transición digital institucional, estandariza el uso de tecnologías en la gestión pública y consolida el expediente electrónico como soporte oficial de la tramitación administrativa.
9.	Ley N° 21.464 de 2022, que modifica diversos cuerpos legales, en materia de Transformación Digital del Estado: Esta ley introduce modificaciones clave a la Ley 21.180 sobre Transformación Digital del Estado, con el propósito de permitir una implementación más gradual y realista de la digitalización de los procedimientos administrativos en los órganos de la Administración del Estado, especialmente en municipalidades y entidades con menores capacidades tecnológicas. Entre sus principales aportes, la ley establece una nueva “Fase de Preparación”, que obliga a las instituciones públicas a identificar y registrar sus procedimientos administrativos y políticas de notificación. Esta etapa debe realizarse con el apoyo técnico de la Secretaría de Gobierno Digital del Ministerio de Hacienda (anteriormente División de Gobierno Digital del Ministerio de Secretaría General de la Presidencia). Además, se reorganiza el cronograma de implementación, extendiendo el plazo final de cumplimiento al 31 de diciembre de 2027, y diferenciando tres grupos de instituciones (A, B y C) según su nivel de complejidad y capacidades operativas. Estas modificaciones refuerzan la importancia de estructurar adecuadamente los procesos de gestión documental desde sus etapas más tempranas, asegurando la interoperabilidad, trazabilidad y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Asimismo, la extensión de plazos y la fase preparatoria permiten a los organismos fortalecer su infraestructura documental y avanzar hacia la plena digitalización en forma ordenada, progresiva y con soporte técnico institucional.

	Normativas
10.	Decreto Supremo N° 4 de 2021 del Ministerio Secretaría General de la Presidencia, que aprueba el reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos: Este reglamento complementa la Ley N° 21.180 sobre Transformación Digital del Estado, estableciendo normas específicas para la gestión documental electrónica en el sector público, y su objetivo principal es normar el funcionamiento de los procedimientos administrativos tramitados por medios electrónicos, definiendo condiciones para la presentación de documentos, la conformación de expedientes y el uso de plataformas tecnológicas institucionales. En efecto, el decreto regula aspectos esenciales como la creación, ingreso, notificación y conservación de documentos electrónicos; la identificación electrónica de las personas naturales o jurídicas que intervienen en los procedimientos; el uso obligatorio de plataformas interoperables; y los estándares de integridad, trazabilidad y seguridad de los documentos digitales. Asimismo, establece que todo expediente debe conformarse con documentos electrónicos firmados digitalmente y almacenados en condiciones que aseguren su conservación, integridad y acceso. En consecuencia, se refuerza la obligatoriedad de implementar sistemas de gestión documental electrónicos como parte de la infraestructura institucional. Desde la perspectiva de la gestión documental, este decreto constituye una referencia clave para asegurar la legalidad y validez de los actos administrativos electrónicos, y a su vez, refuerza también la necesidad de contar con sistemas que registren, controlen y resguarden adecuadamente los antecedentes generados o recibidos en formato digital por los organismos del Estado.
11.	Decreto con Fuerza de Ley N° 5.200 de 1929, del Ministerio de Educación Pública, sobre Instituciones Nacionales Patrimoniales Dependientes del Servicio Nacional del Patrimonio Cultural: En su artículo 14, establece la obligación de remitir anualmente al Archivo Nacional una serie de documentos provenientes de diversas entidades públicas. Entre ellos se incluyen los documentos generados por los Departamentos de Estado que hayan cumplido cinco años de antigüedad, así como los pertenecientes a las Intendencias y Gobernaciones, actualmente Delegaciones Presidenciales Regionales y Provinciales, que hayan alcanzado sesenta años de antigüedad. Esta disposición tiene como finalidad garantizar la conservación del patrimonio documental del país, resguardando aquellos antecedentes que poseen valor histórico, jurídico o institucional para su preservación permanente en el Archivo Nacional. De esta manera, se consolida un mecanismo legal que regula el ingreso sistemático de documentación relevante al acervo patrimonial del Estado.
12.	Resolución Exenta N° 173 de 2021, del Ministerio de las Culturas, las Artes y el Patrimonio: Esta resolución emitida por el Servicio Nacional del Patrimonio Cultural aprueba el procedimiento para la eliminación de documentos originales conforme a la Ley N°18.845, que regula los sistemas de microcopia o micrograbación de documentos. Además, establece un conjunto de directrices destinadas a las instituciones de la Administración Pública, registros públicos y archivos privados declarados monumento nacional, orientadas a regular la eliminación de documentos originales que hayan sido previamente microcopiados o micrograbados. Este procedimiento define etapas específicas para la eliminación de documentos en soporte papel que carezcan de valor histórico o cultural, detallando responsabilidades institucionales y del Archivo Nacional. Entre los principios rectores se incluyen la autorización previa, la destrucción segura, la trazabilidad documental y la documentación del proceso completo. Asimismo, se estipulan las fases del procedimiento, desde la identificación de los documentos hasta la publicación en el Diario Oficial y su posterior destrucción. Se prohíbe eliminar documentos calificados como de valor histórico o cultural por parte del Conservador del Archivo Nacional, toda solicitud de eliminación debe ser evaluada técnicamente por dicha entidad. También, la resolución subraya que la eliminación documental constituye una medida excepcional dentro del SGD del sector público.

	Normativas
13.	Circular N° 51 de 2009 del Archivo Nacional: Emitida por la Dirección de Bibliotecas, Archivos y Museos (DIBAM), establece disposiciones y recomendaciones técnicas para la conservación, transferencia y eliminación de documentos públicos, en el marco de la entrada en vigencia de la Ley N° 20.285 sobre Transparencia y Acceso a la Información Pública, y su propósito justamente es reforzar la correcta gestión documental como requisito habilitante para el acceso a la información pública, la probidad administrativa y la rendición de cuentas. Entre sus contenidos más relevantes, la circular define un glosario técnico especializado, con conceptos clave como archivo, custodia, documento público, documentos reservados y secretos, microformas, eliminación documental y transferencia, entre otros, fundado en normativas nacionales e internacionales, incluyendo ISAD(G) e ISO. Establece que la conservación de documentos debe realizarse conforme a instrucciones específicas, incluyendo la encuadernación física, la mantención de repositorios digitales, y el cumplimiento de las normas aplicables a microformas conforme a la Ley N° 18.845 de 1989. Asimismo, regula la transferencia obligatoria de documentos al Archivo Nacional, conforme al DFL N° 5200 de 1929, distinguiendo los plazos aplicables para distintos organismos del Estado. Además, detalla el tratamiento de documentos clasificados como reservados o secretos, estableciendo sus condiciones de acceso diferido. En lo relativo a la eliminación documental, describe en detalle el procedimiento y las condiciones que deben cumplirse, exigiendo la evaluación del valor histórico, jurídico, fiscal o administrativo de los antecedentes. Incluye requisitos diferenciados para documentos micrograbados, contables, fiscales, de personal, clínicos e indígenas, remitiéndose a las normativas específicas que rigen cada tipo documental. Esta circular exige contar con autorización formal para llevar a cabo la eliminación, la que debe realizarse mediante decreto o resolución según el tipo de entidad, e incluye la obligación de notificar previamente mediante publicación en el Diario Oficial y de permitir la oposición del Archivo Nacional. Finalmente, promueve buenas prácticas en los métodos de eliminación, privilegiando técnicas que impidan la recuperación de la información y fomenten la sustentabilidad ambiental. Sin lugar a duda, esta circular se configura, así como un instrumento normativo y técnico esencial para las instituciones públicas, al establecer estándares mínimos en materia de gestión documental, asegurar la legalidad de la disposición documental y garantizar la trazabilidad y protección de la información pública.

3.2 INSTRUCCIONES Y DICTÁMENES DE LA CGR

La CGR, en su rol de órgano superior de control y conforme a su potestad dictaminadora, ha emitido **instrucciones generales y circulares orientadas a regular el manejo documental en los organismos del Estado**, con especial énfasis en las materias de resguardo, conservación y eliminación de documentos oficiales. Estas directrices constituyen un marco normativo esencial y de especial observancia para las entidades sujetas a su fiscalización, puesto que son esenciales para asegurar la trazabilidad, legalidad y transparencia en la gestión documental de la información pública.

Ahora, **la aplicación sistemática de estas disposiciones no solo refuerza el control interno institucional, sino que también previene eventuales responsabilidades administrativas y asegura el cumplimiento de principios fundamentales** como la probidad, la eficiencia y el respeto a los derechos de los sujetos administrados.

Mediante esta potestad, la CGR ha sostenido de manera consistente y sistemática la supremacía de las disposiciones contenidas en su Ley Orgánica Constitucional, particularmente lo dispuesto en los artículos 14 y 21, como marco normativo rector en materia de eliminación documental. Por una parte, el artículo 14 faculta al Contralor (a) General para adoptar medidas específicas respecto de la destrucción de documentos relacionados con la deuda pública, especies valoradas y otros efectos, y por otra, el artículo 21 dispone que, la incineración de libros, documentos y cuentas aprobadas procede únicamente luego de transcurrido un plazo de tres años desde su revisión definitiva, salvo que por razones fundadas el(la) Contralor(a) determine su conservación. Solo en casos expresamente normados puede considerarse procedente la destrucción documental sin autorización del organismo de control.

A continuación, se presenta un **análisis sintético de las instrucciones y pronunciamientos normativos más relevantes en esta materia:**

	Normativa
1.	Circular N° 28.704 de 1981, de la Contraloría General de la República: Consolida disposiciones legales y recomendaciones aplicables a la eliminación de documentos en la Administración Pública. El texto establece lineamientos generales, modalidades especiales y recomendaciones específicas para distintos tipos documentales. En primer lugar, se dispone que la eliminación de documentos requiere autorización formal. En el caso de los servicios de la Administración Pública, esta debe ser otorgada por el Presidente de la República mediante decreto o resolución exenta. En los organismos autónomos, la autorización corresponde a su jefatura superior, cumpliendo las mismas formalidades. En segundo término, se detallan modalidades especiales para la eliminación de determinados documentos. Así, los antecedentes relacionados con deuda pública, especies valoradas u otros efectos solo pueden ser destruidos con la intervención del (de la) Contralor(a) General o un delegado especialmente designado, una vez transcurridos dos años desde su revisión. En cuanto a los libros, documentos y cuentas aprobadas, estos deben conservarse por un mínimo de tres años desde su revisión definitiva, salvo que exista instrucción en contrario. Respecto de los documentos ministeriales con más de cinco años de antigüedad, estos deben ser transferidos al Archivo Nacional conforme al DFL N°5.200 de 1929. En el caso de las Intendencias, Gobernaciones y libros de actas municipales, el plazo es de sesenta años. Por su parte, los documentos tributarios y previsionales se rigen por sus respectivas normativas sectoriales, como las instrucciones del Servicio de Impuestos Internos y de la Superintendencia de Seguridad Social. Otros documentos específicos (por ejemplo, universitarios o aduaneros) deben eliminarse según sus propias regulaciones, sin contradecir lo dispuesto por la CGR. En cuanto a las recomendaciones generales, se sugiere conservar indefinidamente los documentos de personal, salvo que toda la información se encuentre registrada en libros o tarjetas individuales. A su vez, los documentos operacionales deben mantenerse al menos por cinco años. Mientras aquellos que respalden obligaciones pendientes deben conservarse incluso una vez extinguida la obligación, hasta que los órganos de control realicen su revisión. En cuanto a la eliminación de documentos de Fiscalía debe contar con autorización de la unidad jurídica correspondiente. A su vez, los antecedentes de la Oficina de Partes deben conservarse por cinco años, mientras que las copias de resoluciones y oficios deben mantenerse de forma indefinida y debidamente empastadas. Respecto de los documentos no contemplados expresamente, se recomienda consultar a la unidad que los originó antes de proceder a su eliminación. Los plazos de conservación deben contarse desde la fecha de emisión del documento, salvo que exista norma expresa en contrario, como es el caso del artículo 21 de la Ley N°10.336, que computa el plazo desde la revisión definitiva del documento. Por otra parte, respecto del material de desecho, se establece que este debe sujetarse a lo dispuesto en el Decreto N°577 de 1978 del Ministerio de Bienes Nacionales (cuyo título específico en la actualidad se encuentra derogado). Por último, toda eliminación documental debe formalizarse mediante decreto o resolución exenta de toma de razón, y debe dejarse constancia del proceso en un acta.

	Normativas
2.	Dictamen N° E94973 de 2025: Este dictamen se pronuncia sobre la solicitud de un órgano público para implementar un repositorio digital que almacene carpetas electrónicas de procesos de contratación, incluyendo copias digitalizadas de documentos en papel y documentos electrónicos de origen. La CGR concluye que no se requiere autorización previa para adoptar esta modalidad, siempre que se cumpla con las normas que regulan los procedimientos administrativos respectivos, exista factibilidad técnica, y se aseguren medidas de resguardo que garanticen la veracidad e inviolabilidad de la información. Lo anterior se enmarca en la gradual implementación de la Ley N° 21.180 sobre Transformación Digital del Estado, que permite anticipar el uso de tecnologías de información antes de su entrada en vigencia plena en 2027. Se citan como fundamento los dictámenes N° E402560 de 2023 y N° E282779 de 2022.
3.	Dictamen N° E402560 de 2023: Este dictamen se pronuncia sobre la procedencia de eliminar antecedentes en soporte papel que respaldan pagos a proveedores una vez digitalizados, en el marco de la implementación gradual de la Ley N° 21.180 sobre transformación digital del Estado. La CGR concluye que dichos documentos no pueden eliminarse mientras no se acredite que han sido revisados de manera definitiva por este órgano de control, ya que están directamente relacionados con la administración de fondos públicos. Esta exigencia se fundamenta en el artículo 21 de la Ley N° 10.336, que impone la obligación de conservar libros y documentos por al menos tres años contados desde su revisión definitiva, y en el oficio circular N° 28.704 de 1981, que establece que solo pueden eliminarse los antecedentes contables cuando el(la) Contralor(a) lo autorice expresamente. Además, la jurisprudencia administrativa aplicable (dictámenes N°s 16.584 y 24.934 de 2019; 5.441 de 2014; y 36.583 de 2017) aclara que la revisión definitiva ocurre con la emisión del informe final de auditoría y que la eliminación de documentos requiere acreditar formalmente esa revisión. Dado que el organismo requirente no acompañó antecedentes que permitan verificar dicha circunstancia, la CGR desestima la solicitud y mantiene la obligación de conservar los documentos en soporte papel.
4.	Dictamen N° E368449 de 2023: Este dictamen se pronuncia sobre si la obligación de remitir documentos al Archivo Nacional por parte de las municipalidades comprende todo el fondo documental o solo la documentación oficial. La CGR reitera que, conforme al artículo 14 del DFL N° 5.200 de 1929 y su interpretación en los dictámenes N°s 34.050 de 2016 y E124197 de 2021, los municipios están comprendidos dentro del concepto de “Departamentos de Estado”, por lo que deben remitir al Archivo Nacional, en marzo de cada año, los documentos oficiales que hayan cumplido cinco años desde su emisión. Precisa además que esta obligación se refiere únicamente a documentación oficial y ordinaria, excluyéndose los documentos reservados o secretos. Además, recuerda que los antecedentes sujetos a revisión contable deben conservarse por tres años desde su revisión definitiva, de conformidad con los artículos 14 y 21 de la Ley N° 10.336, sin perjuicio de lo que él (la) Contralor(a) disponga expresamente.
5.	Dictamen N° E124197 de 2021: Este dictamen se pronuncia sobre la solicitud de reconsideración del dictamen N° 34.050 de 2016, que interpretó que la expresión “Departamentos de Estado”, contenida en el artículo 14 del DFL N° 5.200 de 1929, debe entenderse comprensiva de todos los organismos centralizados y descentralizados que integran la Administración del Estado, por lo que las Municipalidades deben remitir al Archivo Nacional todos sus documentos con más de cinco años de antigüedad, exceptuando sus libros de actas, que deben transferirse a los sesenta años. La CGR reitera que no existe una diferenciación normativa respecto del tipo de documentación sujeta a la regla general de cinco años, y que la letra c) del citado artículo constituye una excepción expresa y restringida aplicable solo a los libros de actas municipales. No habiéndose presentado nuevos antecedentes ni fundamentos que desvirtúen lo resuelto anteriormente, se desestima la reconsideración, sin perjuicio de que los órganos de la Administración del Estado, incluidas las Municipalidades, pueden adoptar sistemas electrónicos y digitales para la gestión documental, conforme a los principios establecidos en la Ley N° 18.575.

	Normativas
6.	Dictamen N° E282779 de 2022: Este dictamen se pronuncia sobre la procedencia de tramitar íntegramente en forma electrónica los procedimientos disciplinarios, registrando cada gestión en un sistema digital diseñado para ello. La CGR concluye que ello es jurídicamente posible, siempre que se respeten las normas que regulan dichos procedimientos, así como los principios de debido proceso y fidelidad de las actuaciones, y que el sistema asegure la veracidad e inviolabilidad de la información. Esta interpretación se fundamenta en las leyes N°s 18.575 y 19.880, además de los dictámenes N°s 42.473 de 2016, 47.858 de 2012, 78.962 de 2015 y 7.816 de 2020. Además, se indica, que el sistema deberá adecuarse gradualmente a lo dispuesto por la Ley N° 21.180 sobre transformación digital del Estado.
7.	Dictamen N° 24.934 de 2019: Este dictamen se pronuncia sobre la solicitud de autorización para eliminar documentos financieros y contables correspondientes al período 2006-2012, respecto de los cuales el organismo requirente señala que habrían sido revisados por la CGR mediante auditorías. Sin embargo, este órgano de control constata que las fiscalizaciones practicadas solo comprendieron los ejercicios 2014, 2015 y 2016, y que el listado de documentos acompañado carece de la especificidad necesaria para identificar los antecedentes y verificar que hayan sido efectivamente revisados de forma definitiva. En consecuencia, desestima la solicitud y ordena mantener los documentos para su consulta. La decisión se basa en el artículo 21 de la Ley N° 10.336, que exige conservar por al menos tres años los documentos contables relacionados con fondos públicos desde su revisión definitiva, salvo autorización del (de la) Contralor (a); en el artículo 14 de la misma ley, que faculta a la CGR para fiscalizar la destrucción documental; y en el oficio circular N° 28.704 de 1981, que regula los procedimientos para la eliminación de documentos. Asimismo, se aplican criterios ya recogidos por este órgano en los dictámenes N° 16.584 de 2019, que precisa qué documentos requieren autorización para su eliminación; N° 5.441 de 2014, que establece que la revisión definitiva se configura con la emisión del informe final de auditoría; y N° 36.583 de 2017, que exige acreditar dicha revisión como condición para autorizar la destrucción documental.
8.	Dictamen N° 16.584 de 2019: Este dictamen se pronuncia sobre la solicitud de reconsideración del oficio N° 3.953 de 2017, que había denegado a un organismo requirente la autorización para eliminar talonarios de licencias médicas, por considerarlos documentos vinculados a la administración de fondos públicos. Tras reevaluar el caso, la CGR concluye que dichos talonarios no corresponden a antecedentes sujetos a revisión contable en los términos del artículo 21 de la Ley N° 10.336, ni a documentos cuya destrucción esté sujeta a su autorización, conforme al dictamen N° 5.978 de 2012. Añade que estos formularios son administrados por las COMPIN y se encuentran regulados por el decreto N° 3 de 1984 del Ministerio de Salud, en virtud del cual su destrucción se rige por las instrucciones de la Superintendencia de Seguridad Social. En consecuencia, reconsidera el pronunciamiento anterior, señalando que no corresponde que la CGR se pronuncie sobre su eliminación, ya que dicha facultad recae en otra autoridad sectorial competente. Esta conclusión se funda en los artículos 14 y 21 de la Ley N° 10.336, el oficio circular N° 28.704 de 1981, y la normativa sectorial que regula específicamente la administración y control de los formularios de licencias médicas.
9.	Dictamen N° 36.583 de 2017: este dictamen se pronuncia sobre la solicitud de autorización de un requirente para incinerar documentación original vinculada a rendiciones por ingresos consulares desde 1979, mantenida en su archivo histórico. Sin embargo, al no individualizar los documentos ni acreditar que fueron revisados y aprobados por la CGR, esta rechazó la petición, recordando que solo pueden eliminarse aquellos antecedentes contables cuya revisión haya concluido con informe final, conforme al artículo 21 de la Ley N° 10.336 y a la Circular N° 28.704 de 1981. En consecuencia, el ministerio deberá conservar la documentación consultada.

	Normativas
10.	Dictamen N° 34.815 de 2017: Este dictamen se pronuncia sobre la procedencia de eliminar documentación almacenada en un archivo que colapsó tras el sismo del 16 de septiembre de 2015, situación que dificultó el acceso y generó riesgos para la salud del personal. Considerando los antecedentes técnicos aportados, se analiza la obligación de conservar los documentos conforme al artículo 21 de la Ley N° 10.336, que establece un plazo mínimo de tres años desde la revisión definitiva para la conservación de documentos relacionados con la administración de fondos públicos, salvo que el (la) Contralor(a) disponga otra cosa, y que se complementa con la Circular N° 28.704 de 1981, que amplía esta obligación en caso de observaciones pendientes. También se reconoce que esta conservación puede cumplirse mediante medios digitales, en línea con los principios de eficiencia y eficacia establecidos en la Ley N° 18.575 y las disposiciones de las leyes N° 18.845 y N° 19.799.
11.	Dictamen N° 84.160 de 2016: Este dictamen se pronuncia ante la consulta por la dificultad de conservar físicamente, incluso por más de diez años, la documentación relativa a créditos, subsidios y contabilidad, debido a su volumen y a la falta de espacio. En su análisis, la CGR recuerda que el artículo 21 de la Ley N° 10.336 obliga a conservar los documentos vinculados a la administración de recursos públicos por al menos tres años desde su revisión definitiva, y solo pueden ser incinerados si han sido previamente aprobados y no existe interés especial en conservarlos. Sin embargo, invocando los principios de eficiencia, eficacia e idónea administración de los medios públicos, establecidos en los artículos 3° y 5° de la Ley N° 18.575, la CGR articula este marco normativo con la posibilidad de utilizar tecnologías modernas para el cumplimiento de esta obligación, reconociendo como válidas alternativas legales como la microcopia, la digitalización y el uso de documentos electrónicos conforme a lo dispuesto en las leyes N° 18.845 y N° 19.799. A su vez, cita los dictámenes N°s 34.050 de 2016, 23.766 de 2008 y 81.069 de 2013, donde se ha validado que, siempre que se asegure la equivalencia técnica con el soporte papel, en cuanto a duración, fidelidad y legibilidad, la digitalización puede reemplazar válidamente los originales físicos. Así, se concluye que los órganos de la Administración del Estado pueden cumplir su obligación de conservación documental mediante medios electrónicos o digitales, siempre que estos garanticen la integridad de la información, permitiendo así enfrentar adecuadamente los problemas de espacio sin desatender la normativa.
12.	Dictamen N° 62.205 de 2016: Este dictamen se pronuncia sobre si basta con comunicar la destrucción de documentos afectados por un terremoto o si es necesaria autorización previa para su incineración. Pues se aclara que, conforme al artículo 21 de la Ley N° 10.336, los documentos solo pueden eliminarse luego de tres años desde su revisión definitiva y aprobación de las cuentas involucradas, salvo disposición contraria del (de la) Contralor(a). Además, el artículo 14 de la misma ley faculta al (a la) Contralor(a) para fiscalizar la destrucción documental. También se considera el oficio circular N° 28.704 de 1981, que regula la eliminación de documentos. Dado que no se acompañaron antecedentes que permitan verificar la naturaleza y estado de los documentos afectados por el siniestro, no se puede autorizar la incineración. En consecuencia, la CGR concluyó que, en ausencia de dichos antecedentes, no era posible pronunciarse sobre la procedencia de la incineración solicitada.
13.	Dictamen N° 56.331 de 2016: Este dictamen responde a una consulta sobre la posibilidad de emplear medios electrónicos y digitales para cumplir con la obligación legal de conservar documentación contable, conforme al artículo 21 de la Ley N° 10.336, que exige mantener los documentos por al menos tres años desde su revisión definitiva, salvo que el (la) Contralor(a) disponga lo contrario. Ante la acumulación de antecedentes no revisados y la falta de espacio, la CGR remite a su propia jurisprudencia, especialmente los dictámenes N°s 34.050 de 2016, 23.766 de 2008 y 81.069 de 2013, en los que se ha validado la adopción de tecnologías como la microcopia, la digitalización y el soporte electrónico, en tanto cumplan con estándares de fidelidad, legibilidad y durabilidad similares a los originales, según lo dispuesto en las leyes N° 18.845 y N° 19.799. La CGR articula estas normas a la luz de los principios de eficiencia y buena administración contenidos en la Ley N° 18.575, señalando que la conservación documental exigida por el artículo 21 y por el DFL N° 5.200, de 1929, puede ser cumplida mediante medios electrónicos, siempre que ello resulte procedente. Así, reconoce expresamente la equivalencia entre soportes digitales y papel, validando su uso en la gestión documental de los organismos públicos.

	Normativas
15.	Dictamen N° 34.050 de 2016: Este dictamen se pronuncia ante consulta efectuada por un requirente sobre el plazo que debe mantener el GORE su documentación antes de remitirla al Archivo Nacional, la CGR concluyó que, atendido el desarrollo del ordenamiento jurídico y conforme a los principios de la Ley N° 18.575, los Gobiernos Regionales deben sujetarse a la regla general del artículo 14 letra a) del DFL N° 5.200 de 1929, esto es, remitir anualmente al Archivo Nacional aquellos documentos que hayan cumplido cinco años desde su emisión. Se descartó que les aplicara el plazo excepcional de 60 años previsto para Intendencias y Gobernaciones. Por lo tanto, la remisión deberá comenzar a aplicarse a contar de la fecha del dictamen, reconsiderándose la jurisprudencia anterior que excluía a los GORE del concepto de "Departamentos de Estado". Además, se recomendó el uso de tecnologías como micrograbación o documentos electrónicos para facilitar el cumplimiento de esta obligación.
16.	Dictamen N° 5.441, de 2014: Este dictamen se pronuncia sobre la solicitud de autorización efectuada por un requirente para destruir documentos contables correspondientes al período 1996 - 2006, indicando que la petición carece de la especificidad necesaria para determinar con claridad los antecedentes que se desean eliminar, tales como comprobantes contables detallados, recibos de pagos, traspasos de obligaciones devengadas y documentos relacionados con ingresos y ajustes contables. Se fundamenta en el artículo 21, inciso segundo, de la Ley N° 10.336, que dispone que los libros, documentos y cuentas aprobados podrán ser incinerados únicamente después de transcurridos tres años desde su revisión definitiva, salvo que el Contralor disponga su conservación. Asimismo, el artículo 14 de la misma ley faculta además al (a la) Contralor(a) para fiscalizar la destrucción documental. Además, se toma en cuenta el oficio circular N° 28.704 de 1981, que establece la obligación de mantener la documentación contable gubernamental durante un plazo mínimo de tres años desde la revisión definitiva. También, se señala que la revisión definitiva corresponde al momento en que se emite el informe final de auditoría o fiscalización. En consecuencia, al no haberse aportado antecedentes que acrediten que los documentos solicitados para eliminación corresponden a cuentas revisadas y aprobadas por la CGR, se determina que la documentación debe mantenerse.
17.	Dictamen N° 100.175 de 2014: Este dictamen se pronuncia ante la consulta del Jefe de Auditoría de un Servicio sobre el plazo de conservación y procedimiento de destrucción de hojas de trabajo y antecedentes obtenidos en auditorías internas, tales como fotocopias de normativa, comprobantes contables, planillas e informes validados por el auditor, la CGR indica que estos documentos no corresponden a justificativos de ingresos y gastos ni a antecedentes vinculados al examen de cuentas, por lo que no se enmarcan en el ámbito de fiscalización que le asignan los artículos 14 y 21 de la Ley N° 10.336. En consecuencia, su eliminación no requiere autorización de este órgano de control, correspondiendo dicha facultad al Jefe del Servicio, quien debe determinar el tiempo de conservación y el procedimiento para su destrucción conforme al oficio circular N° 28.704, de 1981. Finalmente, se reitera que esta documentación no posee el carácter que justificaría intervención de la CGR.
18.	Dictamen N° 81.069 de 2013: Este dictamen, la CGR se pronuncia sobre la validez y requisitos para el uso exclusivo de documentos electrónicos con firma electrónica en actos administrativos, señalando que no existe impedimento para que los servicios públicos utilicen dichos documentos en reemplazo del soporte papel, siempre que se respeten las disposiciones de la Ley N° 19.799 y su reglamento. Sin embargo, se establece que debe mantenerse un sistema paralelo en papel para evitar restricciones injustificadas al acceso de los usuarios y garantizar la transparencia y no discriminación. Asimismo, se determina que los documentos electrónicos relacionados con la administración de fondos públicos deben conservarse durante un plazo mínimo de tres años desde su revisión definitiva, salvo que el (la) Contralor (a) General disponga su conservación por un periodo mayor o existan observaciones pendientes de resolución. Esta decisión armoniza la normativa sobre documentos electrónicos con las reglas tradicionales de conservación y eliminación de documentos públicos.

	Normativas
19.	Dictamen N° 25.634 de 2009: Este dictamen se pronuncia ante la solicitud de autorización para eliminar comprobantes contables y documentación sustentatoria de rendición de cuentas correspondientes al período 1997 - 2002, la CGR señaló que, conforme al artículo 21 de la Ley N° 10.336 y al oficio circular N° 28.704 de 1981, dicha documentación solo puede ser eliminada si han transcurrido al menos tres años desde su revisión definitiva y aprobación por parte de este órgano de control. En este caso, no se acompañaron antecedentes que acrediten que las cuentas fueron efectivamente revisadas y aprobadas, por lo que se instruyó mantener la documentación.
20.	Dictamen N° 37.995 de 2009: Este dictamen se pronuncia ante la solicitud de autorización para eliminar comprobantes contables y documentación sustentatoria de rendiciones de cuentas de los años 2003 y 2004, sin embargo, respecto del año 2003 no se acompañaron antecedentes que permitieran corroborar que las cuentas fueron revisadas y aprobadas por la CGR, condición necesaria según lo dispuesto en el artículo 21 de la Ley N° 10.336 y la circular N° 28.704 de 1981. En cuanto a la documentación del año 2004, si bien se presentó un oficio que da cuenta de cuentas examinadas en el Servicio, este no acredita la revisión y aprobación de los antecedentes de toda la región, por lo que tampoco se accedió a la eliminación solicitada.

3.3 ESTRATEGIAS NACIONALES PARA LA TRANSFORMACIÓN DIGITAL

La Transformación Digital del Estado se articula a través de un ecosistema normativo y estratégico que busca modernizar el funcionamiento de las instituciones públicas, promover la eficiencia administrativa y mejorar la calidad de los servicios prestados a la ciudadanía. En este contexto, diversas estrategias publicadas entre 2019 y 2025 orientan la acción del sector público hacia una gestión documental digital, interoperable, segura y centrada en las personas. Estas estrategias se alinean con principios de transparencia, trazabilidad, probidad y eficiencia, fundamentales para la función pública. A continuación, se resumen las principales estrategias vigentes:

● Estrategia de Gobierno Digital 2030

Publicada en junio de 2025 por la Secretaría de Gobierno Digital, esta estrategia define el marco que guiará la digitalización del Estado hacia el año 2030. Entre sus siete objetivos estratégicos destaca la necesidad de consolidar servicios digitales compartidos, potenciar la gobernanza institucional, fortalecer el uso estratégico de los datos y desarrollar talento digital en el aparato público.

Esta estrategia refuerza la obligación institucional de contar con sistemas de gestión documental digital interoperables, sustentados en estándares de calidad, seguridad y trazabilidad. Asimismo, promueve el uso de registros digitales confiables como base para servicios públicos eficientes y fiscalizables.

● Estrategia de Datos del Gobierno

Publicada en diciembre de 2024, esta hoja de ruta establece lineamientos para una gestión estatal de datos eficiente, segura y orientada a la generación de valor público, organizándose en tres ejes estratégicos: Ecosistema, Personas y Tecnología, y contempla medidas para fortalecer competencias digitales, infraestructura tecnológica y gobernanza del dato.

Esta estrategia refuerza el vínculo entre gestión documental y gestión de datos, promoviendo la apertura, estandarización y reutilización de los datos contenidos en documentos institucionales. Además, impulsa la calidad, integridad y trazabilidad de la información documental como insumo clave para la toma de decisiones basadas en evidencia.

● Estrategia de Identidad Digital

Emitida en diciembre de 2024, esta estrategia define los principios para desarrollar un sistema nacional de identidad digital robusto, interoperable y seguro, cuyo diseño se basa en la colaboración público-privada y está orientado a personas naturales, incluyendo figuras de representación jurídica.

Esta estrategia establece las condiciones de autenticación y verificación de identidad en entornos digitales, elementos esenciales para la validez de los actos administrativos firmados electrónicamente y el fortalecimiento del expediente electrónico, apoyando la trazabilidad, integridad y no repudio de los documentos públicos.

● Estrategia de Transformación Digital del Estado

Emitida en enero de 2019, esta estrategia transversal sentó las bases para la digitalización progresiva de los procesos y estructuras administrativas del Estado, definiendo principios, metas y proyectos estratégicos alineados con la Ley N°21.180. Esta estrategia refuerza la necesidad de implementar sistemas de expediente electrónico, mecanismos de interoperabilidad documental y estándares comunes para la gestión de registros, respaldando legal y operativamente la implementación de plataformas como DocDigital, PISEE y CPAT.

● **Agenda de Modernización del Estado**

Publicada en conjunto por la Presidencia, el Ministerio de Hacienda y la SEGPRES, esta agenda establece la arquitectura institucional y estratégica para una modernización continua del Estado, con énfasis en servicios públicos eficientes, participación ciudadana, institucionalidad y rendición de cuentas.

La agenda impulsa una gestión documental que garantice la transparencia, el acceso a la información, el cumplimiento normativo y la rendición de cuentas. Además, promueve una visión sistémica de los procesos documentales como parte del desempeño institucional.

Estas estrategias constituyen el marco programático que orienta la transformación digital del Estado chileno, sentando las bases para una gestión documental moderna, confiable y al servicio de los principios de legalidad, eficiencia, trazabilidad y transparencia. Por lo tanto, su implementación progresiva exige a los órganos públicos adaptar sus sistemas, fortalecer sus capacidades institucionales y avanzar hacia una cultura organizacional centrada en la gestión digital de la información como activo estratégico.

3.4 NORMAS INTERNACIONALES ISO

Las normas internacionales elaboradas por la Organización Internacional de Normalización (ISO) **constituyen un referente técnico fundamental para el desarrollo de políticas, procesos y sistemas de gestión documental en todo tipo de organizaciones**. Estas normas se agrupan en dos conjuntos complementarios. El primero está orientado a la implementación de procesos de gestión documental, y comprende marcos conceptuales, directrices técnicas y herramientas prácticas para asegurar la creación, captura, organización, trazabilidad y conservación de documentos en distintos formatos, tanto físicos como digitales. Entre ellas destacan la ISO 15489, ISO 16175, ISO 23081, y diversas normas técnicas aplicables a digitalización, migración de registros o análisis de procesos de trabajo. El segundo conjunto corresponde a las normas sobre sistemas de gestión documental (SGD), que establecen los principios, requisitos y lineamientos para diseñar, implementar, evaluar y mejorar sistemas institucionales alineados con la gobernanza organizacional, la gestión por procesos y el cumplimiento de objetivos estratégicos. Estas incluyen la serie ISO 30300 y sus adaptaciones nacionales, como la NCh-ISO 30301. En su conjunto, ambos grupos normativos ofrecen un marco integral para profesionalizar la gestión documental, promover la interoperabilidad tecnológica, resguardar la integridad de la información institucional y asegurar el cumplimiento de estándares internacionales en contextos públicos o privados, sin contradecir la normativa legal vigente de cada país.

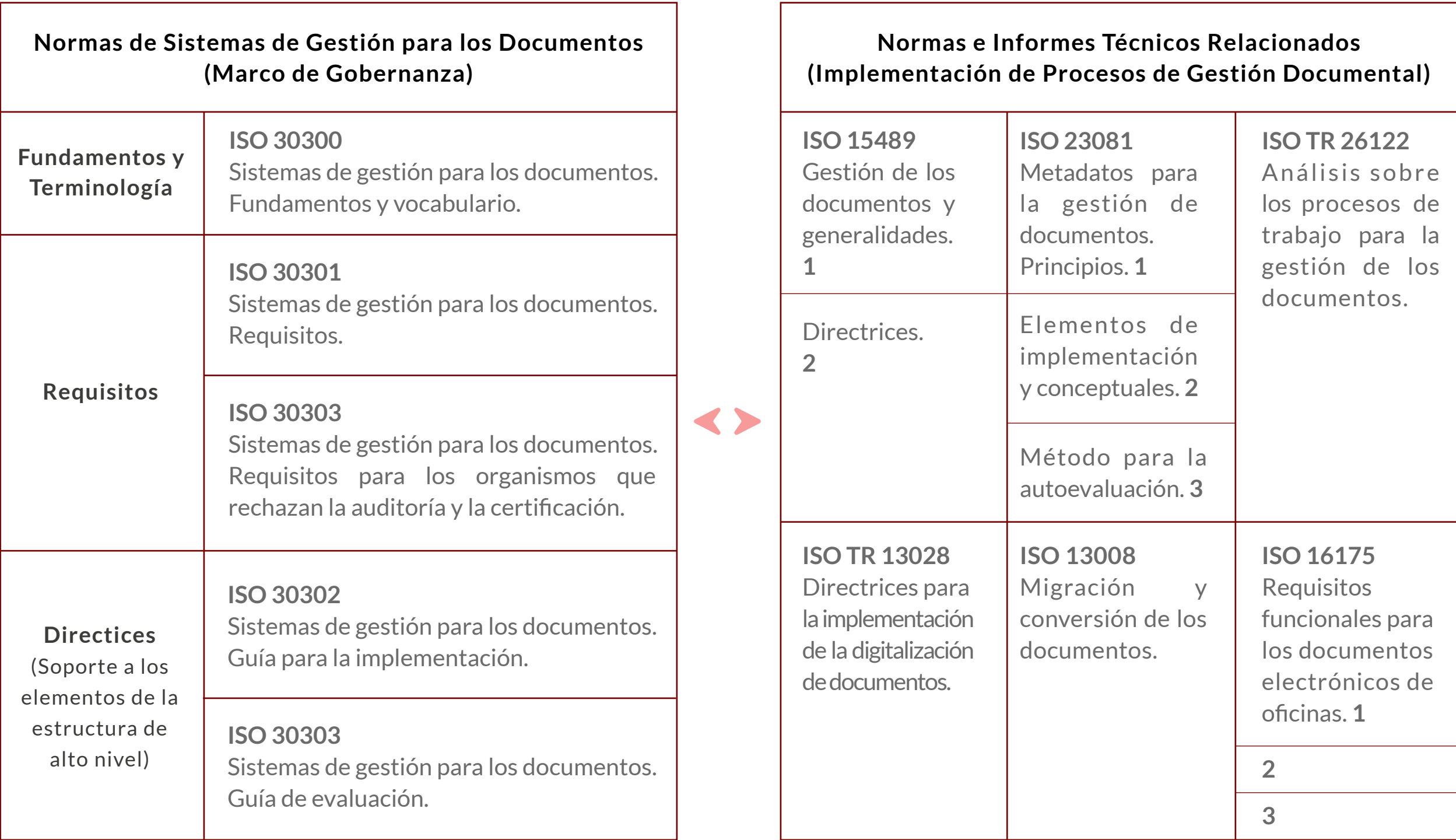


Figura N°4: Relación Normas ISO sobre Sistema de Gestión Documental. Fuente: Universidad de Jaén.

3.4.1 Normas e Informes Técnicos Relacionados con la Implementación de Procesos de Gestión Documental

	Normativas
1.	ISO 15489-1:2016 sobre Gestión de Documentos – Parte 1: Generalidades. Esta norma internacional establece los conceptos y principios fundamentales para la gestión documental en cualquier entorno organizacional o tecnológico. Define elementos clave como los registros, sus metadatos, y los sistemas que los gestionan; así como las políticas institucionales, responsabilidades asignadas, mecanismos de seguimiento y necesidades de capacitación asociadas. Además, promueve el análisis sistemático del contexto institucional para identificar requerimientos documentales, establecer controles efectivos y asegurar la adecuada creación, captura, preservación y gestión de los documentos a lo largo del tiempo, sin importar su forma o soporte. Ahora, su aplicación constituye una buena práctica internacional, especialmente útil como marco de referencia complementario en el sector público, siempre que no contravenga la normativa nacional vigente.
2.	ISO/TR 15489-2:2001 sobre Gestión de Documentos - Parte 2: Directrices. Esta norma proporcionaba directrices prácticas complementarias a la ISO 15489-1 para la implementación de procesos de gestión documental. Sin embargo, fue retirada oficialmente en 2017 y su contenido ha sido progresivamente reemplazado por nuevas normas específicas, tales como la ISO 16175 (funcionalidades para sistemas de gestión de documentos electrónicos), la ISO 21946 (gestión de documentos como evidencia), la ISO 21965 (metadatos para documentos) y la ISO 22428 (uso de tecnologías emergentes en gestión documental). En consecuencia, si bien la ISO/TR 15489-2 ya no se encuentra vigente, su enfoque fue base para el desarrollo de marcos técnicos posteriores que siguen siendo considerados buenas prácticas a nivel internacional.
3.	ISO/TR 26122:2008 sobre Análisis del Proceso de Trabajo para la Gestión de Documentos. La norma ISO/TR 26122:2008 entrega directrices para analizar procesos de trabajo desde la perspectiva de la creación, captura y control de documentos, estableciendo dos enfoques principales: el análisis funcional, que descompone funciones en procesos; y el análisis secuencial, que examina el flujo de transacciones dentro de la organización. Ambos enfoques requieren una revisión contextual previa, considerando el mandato institucional y el entorno normativo aplicable. Esta norma incluye guías prácticas en forma de listas de verificación para orientar el análisis de cada componente. Ahora, su aplicación es independiente del entorno tecnológico, aunque puede emplearse para evaluar herramientas que respalden los procesos documentales. Esta norma opera como una aplicación práctica de los conceptos definidos en la norma ISO 15489, enfocándose en procesos existentes y no en automatizaciones, lo que permite identificar mejoras en la gestión documental sin depender necesariamente de plataformas digitales.
4.	ISO/TR 13028:2010 sobre Directrices de Implementación para la Digitalización de Documentos. La norma ISO/TR 13028:2010 proporciona directrices para la digitalización responsable de documentos no digitales, con el objetivo de asegurar la fiabilidad, accesibilidad y valor probatorio de los registros generados. Está dirigida a organizaciones que digitalizan documentos en el marco de procesos de negocio o para la gestión documental posterior, conforme a los principios de la ISO 15489. Entre sus principales aportes, la norma entrega recomendaciones para: • Mantener registros únicamente digitales, cuando el documento original ha sido copiado mediante digitalización. • Asegurar la fiabilidad de los registros digitalizados, especialmente en lo que respecta a su admisibilidad legal. • Garantizar la accesibilidad de los registros durante el tiempo necesario para su uso institucional. • Establecer criterios para decidir la eventual eliminación de los documentos fuente en papel, una vez garantizada la integridad del registro digital. • Establecer estrategias para la conservación a largo plazo de registros digitalizados. Esta norma no aplica a la captura ni gestión de registros nativamente digitales, ni a especificaciones técnicas de escaneo o preservación digital, ni a la digitalización de archivos patrimoniales con fines exclusivamente históricos o de conservación.

	Normativas
5.	ISO 18829:2017 sobre Gestión Documental – Evaluación de Implementaciones de ECM/EDRM – Confiabilidad. La norma ISO 18829:2017 establece una metodología para evaluar si la información almacenada electrónicamente (ESI, por su sigla en inglés) en entornos digitales se mantiene en condiciones que garanticen su confiabilidad. Esta evaluación se orienta a sistemas de gestión de contenido empresarial (ECM, por su sigla en inglés) o de gestión electrónica de documentos y registros (EDRM, por su sigla en inglés), que implementan políticas institucionales y cronogramas de gestión documental. Complementando los lineamientos definidos por las normas ISO 15489 e ISO/TR 15801, la ISO 18829:2017 permite verificar el grado de cumplimiento de una organización en cuanto a la integridad, autenticidad y trazabilidad de los documentos electrónicos. Esta norma identifica actividades clave y áreas obligatorias que deben ser revisadas por profesionales con conocimiento técnico-operativo y experiencia en gestión de registros y tecnologías asociadas. Ahora bien, esta norma es aplicable tanto a sistemas ya implementados como a aquellos en fase de diseño, y constituye un marco de referencia para asegurar la fiabilidad de los documentos almacenados electrónicamente, especialmente en contextos donde se requiere respaldo normativo y control interno sobre la gestión documental digital.
6.	ISO/TR 21946:2018 sobre Valoración para la Gestión Documental. La norma ISO/TR 21946:2018 entrega directrices para la evaluación documental, entendida como el proceso mediante el cual se determina el valor de los documentos dentro de un contexto organizacional. Este documento complementa los principios de la ISO 15489-1 y permite su aplicación práctica mediante el análisis del contexto institucional, la identificación de funciones y procesos, y la evaluación de riesgos asociados a la gestión de información. Entre sus principales lineamientos, se destacan: la definición de los propósitos de la evaluación; la delimitación de su alcance; el análisis de funciones del negocio; la identificación de requerimientos documentales; el uso de evaluaciones de riesgo para apoyar decisiones sobre conservación o disposición; y las formas de documentar y revisar los resultados del proceso. La norma también señala que los productos de la evaluación pueden ser usados para estructurar instrumentos como cuadros de clasificación y tablas de retención, y que su revisión periódica es esencial para garantizar decisiones coherentes y ajustadas al contexto institucional. Ahora, este documento puede ser aplicado en organizaciones de cualquier tipo o tamaño, siendo especialmente útil para apoyar una gestión documental basada en riesgos, con criterios técnicos, normativos y funcionales.
7.	ISO 16175-1:2020 Procesos y requisitos funcionales del software de gestión de documentos. Parte 1: Requisitos Funcionales y Orientación Asociada para Aplicaciones que Gestionan Documentos Digitales. Esta norma establece un modelo conceptual y un conjunto de requisitos funcionales de alto nivel, junto con orientaciones asociadas, destinados a aplicaciones de software que gestionan registros digitales. Abarca tanto sistemas cuya función principal es la gestión de documentos como aplicaciones que, sin ser específicamente documentales, deben cumplir funciones de trazabilidad y registro conforme a principios archivísticos. Este documento se enfoca en registros en formato digital, incluidos aquellos generados por digitalización de documentos fuente analógicos. Sin embargo, no aborda requisitos funcionales específicos para la gestión de registros en soporte físico ni para entornos de preservación digital a largo plazo. Tampoco incluye aspectos relacionados con el diseño técnico general, como administración de sistemas o generación de reportes, aunque sí promueve prácticas que no obstaculicen la futura conservación de la información. Sin embargo, esta norma resulta particularmente útil como referencia técnica para asegurar que las soluciones digitales empleadas en la gestión documental institucional se ajusten a los principios de autenticidad, integridad, confiabilidad y disponibilidad, sirviendo como estándar complementario en contextos normativos nacionales.

	Normativas
8.	ISO/TS 16175-2:2020 sobre procesos y requisitos funcionales del software de gestión de documentos. Parte 2: Orientación para la selección, diseño, implementación y mantenimiento de software para la gestión de documentos. Esta norma técnica proporciona directrices para orientar la toma de decisiones y los procesos relacionados con la selección, diseño, implementación y mantenimiento de soluciones tecnológicas destinadas a la gestión de registros documentales. Está alineada con los principios de la norma ISO 15489-1 y es aplicable a cualquier tipo de SGD soportado por software, incluyendo aquellos que administran documentos físicos mediante plataformas digitales, con un enfoque especial en la gestión de registros electrónicos. Asimismo, está dirigida principalmente a profesionales de archivos y gestión documental que participen en procesos tecnológicos institucionales. También entrega lineamientos útiles para responsables de tecnologías de la información, diseñadores de soluciones, analistas de negocio, encargados de adquisiciones de software, desarrolladores y auditores de sistemas, que necesiten comprender los requisitos específicos que debe cumplir un sistema confiable de gestión documental. Cabe señalar, que esta norma establece buenas prácticas internacionales que permiten asegurar que los sistemas implementados respalden la integridad, autenticidad, fiabilidad y accesibilidad de los registros durante todo su ciclo de vida, siendo especialmente relevante como marco de referencia complementario en el sector público.
9.	ISO/TR 22428-1:2020 sobre gestión de registros en entornos de computación en la nube Parte 1: Problemas y preocupaciones. Esta norma técnica proporciona un marco conceptual para la gestión de documentos en entornos de computación en la nube, identificando los principales riesgos y consideraciones que deben tener en cuenta las organizaciones antes de adoptar este tipo de servicios. El modelo propuesto contempla elementos como actores involucrados, procesos, arquitectura, metadatos y casos de uso. Por su parte, los riesgos identificados se clasifican en internos, relacionados con los propios servicios, sistemas y partes interesadas de la nube, y externos, que derivan del entorno social, normativo y legal en el que operan dichos servicios. Ahora, esta norma está dirigida a profesionales de la gestión documental, arquitectos de servicios en la nube, desarrolladores de software documental, archivistas y proveedores de servicios de gestión documental basada en la nube, así como al personal de tecnologías de la información. Ahora, este documento resulta relevante como guía de referencia técnica para evaluar la adopción de soluciones en la nube en instituciones públicas, especialmente en lo referido a la trazabilidad, confidencialidad y conservación de documentos electrónicos, siempre que se respete la normativa nacional vigente.
10.	ISO/TR 21965:2019 sobre gestión de documentos en la arquitectura empresarial. Este documento técnico establece un lenguaje común que permite integrar las necesidades y requisitos de la gestión de documentos en la arquitectura empresarial, y su objetivo es generar consenso entre los gestores documentales, arquitectos empresariales y arquitectos de soluciones, promoviendo una comprensión compartida que permita posicionar la gestión de documentos como una capacidad organizacional clave, tanto a nivel estratégico como operativo. Esta norma proporciona lineamientos para que los arquitectos empresariales comprendan los principios, objetivos y preocupaciones de la gestión de documentos, reconociendo a los administradores documentales como actores fundamentales en los procesos de transformación institucional. Además, ofrece herramientas conceptuales para incorporar estos requisitos en el diseño de sistemas, procesos y estructuras organizacionales. Incluye perspectivas arquitectónicas, principios aplicables, modelos de colaboración, y orientaciones para facilitar consultas técnicas, promover el uso de herramientas existentes y mejorar la interoperabilidad entre los dominios de gestión documental, arquitectura empresarial y arquitectura de soluciones. Ahora, su aplicación es especialmente relevante para instituciones públicas que implementan procesos de modernización digital, al asegurar que los principios de trazabilidad, conservación y gobernanza documental sean considerados desde el diseño mismo de sus plataformas y sistemas.

	Normativas
11.	ISO/TR 15801:2017 sobre gestión documental - Información almacenada electrónicamente - Recomendaciones para la fiabilidad y la confianza. La norma ISO/TR 15801:2017 establece recomendaciones para la implementación y operación de sistemas de gestión de la información que almacenan información electrónicamente (ESI, por su sigla en inglés) de forma fiable, accesible y segura a lo largo del tiempo. Esta información puede abarcar documentos basados en texto, datos estructurados en bases de datos y registros multimedia. El enfoque se centra en garantizar que los sistemas utilizados incorporen políticas, procedimientos, controles tecnológicos y requisitos de auditoría (bajo norma ISO) que respalden la confiabilidad de la información almacenada. Aunque no aborda la validación de la fiabilidad de la ESI antes de su ingreso al sistema, esta norma permite demostrar que una vez almacenada, la información puede ser reproducida de forma precisa y auténtica. Actualmente, está en discusión el proyecto de norma ISO/DIS 15801.2 (en desarrollo), destinada a reemplazar la versión de 2017, que reforzará estos principios con mayores requisitos de fiabilidad y confianza para los entornos digitales modernos. Con todo, esta norma es especialmente relevante para organizaciones públicas que requieren garantizar la integridad de sus documentos electrónicos como parte de sus obligaciones de transparencia, legalidad y conservación.
12.	ISO 13008:2022 sobre información y documentación — Proceso de conversión y migración de registros digitales. Esta norma establece los requisitos y procedimientos para planificar y ejecutar procesos de conversión y/o migración de registros digitales, con el fin de preservar su autenticidad, fiabilidad, integridad y usabilidad como evidencia de funciones, actividades y transacciones institucionales. Está orientada a garantizar que, durante el cambio de formato o sistema, los registros digitales conserven sus propiedades esenciales y continúen siendo válidos como prueba documental. Cabe señalar que esta norma no aborda de manera exhaustiva aspectos como la creación de sistemas de respaldo, la preservación digital a largo plazo, la funcionalidad completa de repositorios digitales confiables ni la conversión entre formatos analógicos y digitales.
13.	ISO 23081-1:2017I sobre metadatos para la gestión de documentos. Parte 1: Principios. La norma ISO 23081-1:2017 establece los principios fundamentales que rigen el uso de metadatos en la gestión de documentos. Estos principios son aplicables a los documentos y sus respectivos metadatos, a todos los procesos que inciden sobre ellos, a cualquier sistema en el que residan, y a toda organización responsable de su administración. La norma proporciona un marco conceptual que permite asegurar la autenticidad, integridad, confiabilidad y usabilidad de los registros a lo largo del tiempo, facilitando su trazabilidad y control en contextos tanto físicos como digitales.
14.	ISO 23081-2:2021 sobre metadatos para la gestión de documentos. Parte 2: Cuestiones conceptuales y de implementación. Esta norma establece un marco para la definición e implementación de elementos de metadatos, en conformidad con los principios descritos en la norma ISO 23081-1, y su propósito es facilitar una descripción estandarizada de los registros y de las entidades contextuales relevantes, promover la interoperabilidad entre sistemas organizacionales, y permitir la reutilización y estandarización de metadatos en distintos entornos, y a lo largo del tiempo. Además, la norma identifica puntos críticos de decisión que deben ser abordados y documentados para una implementación efectiva. Incluye orientaciones sobre cómo identificar problemas clave, evaluar opciones disponibles y establecer caminos de decisión adecuados para gestionar metadatos de manera coherente y sostenible dentro de los sistemas documentales institucionales.

	Normativas
15.	ISO/TR 23081-3:2011 sobre metadatos para la gestión de documentos. Parte 3: Método de autoevaluación. Esta norma técnica entrega directrices para realizar una autoevaluación del estado de implementación y gestión de metadatos asociados a registros documentales, específicamente en lo que respecta a su creación, captura y control. Esta norma permite realizar una autoevaluación institucional para conocer el estado actual de los metadatos asociados a registros, establecer prioridades de mejora, verificar el cumplimiento de normas ISO previas, evaluar el progreso en la implementación de sistemas documentales y determinar si un sistema o proyecto está preparado para avanzar a nuevas fases, asegurando la integración de funcionalidades clave de metadatos. Ahora, esta herramienta es especialmente útil para apoyar decisiones estratégicas en proyectos de gestión documental, permitiendo detectar brechas, definir etapas de mejora y asegurar la trazabilidad de los registros a lo largo de su ciclo de vida.
16.	ISO/CD TR 23081-4 sobre metadatos para la gestión de documentos. Parte 4: Informe sobre conjuntos de elementos de metadatos. Actualmente en etapa de desarrollo la parte 4 de la serie ISO 23081 que busca consolidar un informe técnico sobre conjuntos de elementos de metadatos relevantes para la gestión de documentos, cuyo objetivo es facilitar la interoperabilidad entre sistemas, la coherencia terminológica y la estandarización de estructuras de metadatos en contextos organizacionales diversos. Dicha iniciativa se orienta a reforzar la implementación práctica de los principios establecidos en las partes anteriores de la norma.

3.4.2 Normas de Sistemas de Gestión Documental que Establecen el Marco de Gobernanza para los Documentos

	Normativas
1.	ISO 30300:2020 sobre Sistemas de Gestión Documental – Conceptos Básicos y Vocabulario. La serie ISO 30300 establece los términos y definiciones fundamentales utilizados en el ámbito de la gestión de documentos, y sirve como base común de entendimiento para las normas desarrolladas por el Comité Técnico ISO/TC 46/SC 11, sin limitar la incorporación de nuevos términos en normas futuras. Por lo tanto, su aplicación es útil como referencia conceptual para organismos que implementan sistemas de gestión documental (SGD), especialmente en contextos donde se requiere claridad terminológica estandarizada.
2.	NCh-ISO 30300:2016 sobre Sistemas de Gestión Documental - Fundamentos y Vocabulario Esta norma chilena oficial adapta los contenidos de la ISO 30300 al contexto nacional, y define los principios fundamentales, objetivos y vocabulario aplicable a los sistemas de gestión documental (SGD). A su vez, establece el enfoque por procesos, detalla los roles de la alta dirección y entrega orientaciones para implementar, mantener y mejorar un SGD. Dicha norma es aplicable a todo tipo de organización que busque apoyar sus actividades mediante un SGD eficaz, asegurar la conformidad con su política institucional en la materia y, eventualmente, demostrar dicha conformidad mediante una autodeclaración, verificación externa o certificación.
3.	ISO 30302:2022/Enmienda 1:2025 sobre sistemas de gestión documental - Directrices para la implementación - Enmienda 1: No conformidades, acciones correctivas y requisitos de cambio climático. Esta enmienda, publicada el 23 de febrero de 2024 por la Organización Internacional de Normalización (ISO), introduce ajustes transversales a todas las normas de sistemas de gestión, incluyendo la norma ISO 30302:2022 sobre implementación de sistemas de gestión documental (SGD). El objetivo de esta modificación es asegurar que las organizaciones consideren el cambio climático como una cuestión pertinente en el diseño, ejecución y mejora de sus sistemas de gestión. En concreto, se incorpora la exigencia de analizar si el cambio climático puede afectar el cumplimiento de los resultados previstos por el SGD, así como si existen requisitos vinculados al cambio climático por parte de las partes interesadas. Asimismo, la enmienda refuerza la necesidad de establecer mecanismos eficaces para identificar no conformidades, adoptar acciones correctivas y documentar adecuadamente los ajustes necesarios en el sistema, en coherencia con las nuevas preocupaciones ambientales y de sostenibilidad que afectan la gestión institucional. Esta incorporación promueve un enfoque más resiliente, adaptable y ambientalmente consciente en la gestión de registros, alineado con los compromisos globales de desarrollo sostenible y responsabilidad climática.
4.	ISO 30301:2019 sobre sistemas de gestión documental – Requisitos. La norma internacional ISO 30301:2019 especifica los requisitos que debe cumplir un SGD para apoyar a una organización en el cumplimiento de su misión, estrategia y objetivos institucionales. En este sentido, establece directrices para desarrollar e implementar una política de gestión documental, definir objetivos asociados y aplicar mecanismos de medición y seguimiento del desempeño del sistema. Ahora, esta norma puede aplicarse a una organización individual o a múltiples entidades que compartan funciones o actividades, y su adopción permite a las organizaciones: • Implementar y mejorar un SGD conforme a sus necesidades. • Verificar el cumplimiento de su política documental. • Demostrar conformidad mediante autoevaluación, validación externa o certificación por un tercero.

	Normativas
5.	NCh-ISO30301:2019 sobre sistema de gestión documental - Requisitos. Esta norma chilena adapta los lineamientos de la ISO 30301:2019 al contexto nacional, y define los requisitos esenciales para establecer, mantener y mejorar un SGD en organizaciones públicas o privadas. A su vez, establece las bases para una gestión documental alineada con la legislación chilena, promoviendo una administración eficiente, segura y trazable de la información institucional. Además, permite demostrar la conformidad del sistema mediante autoevaluación, revisión externa o certificación formal.
6.	ISO 30302:2022 sobre sistemas de gestión documental - Directrices para la implementación Esta norma internacional entrega orientaciones para la implementación efectiva de un SGD conforme a los requisitos establecidos en la norma ISO 30301, y está diseñada para acompañar y complementar dicha norma, describiendo las actividades necesarias para diseñar, ejecutar y supervisar un SGD dentro de cualquier tipo de organización. Ahora, su aplicación es transversal a organizaciones públicas, privadas o sin fines de lucro, sin importar su tamaño o estructura, y está dirigida especialmente a quienes lideran la implementación y mantenimiento del sistema, aunque también puede servir como guía para la alta dirección al momento de definir el alcance, las prioridades y los recursos del SGD en su institución.

Capítulo 4

ELEMENTOS TÉCNICOS

Capítulo 4

ELEMENTOS TÉCNICOS



A. Norma ISO 18128:2024 sobre riesgos de los documentos.

Evaluación de riesgos para la gestión de documentos.

La norma ISO 18128:2024, titulada “Evaluación de Riesgos para la Gestión de Documentos”, establece un **marco metodológico para identificar, analizar y evaluar los riesgos que pueden afectar los documentos, los sistemas que los gestionan y los controles que los resguardan**. Dicha norma se enmarca dentro de los estándares internacionales de buenas prácticas en gestión documental y resulta aplicable a cualquier tipo de organización, sin importar su tamaño, complejidad funcional o ámbito de operación, siendo especialmente útil en el contexto del sector público chileno.

Ahora, su **objetivo principal es ayudar a las organizaciones a garantizar que sus registros conserven las propiedades esenciales de autenticidad, confiabilidad, integridad y usabilidad durante todo su ciclo de vida**. Esto es clave para la trazabilidad de los actos administrativos, la rendición de cuentas y la prevención de riesgos legales o administrativos derivados de una gestión documental deficiente.

A su vez, la norma establece que la evaluación de riesgos documentales debe basarse en el enfoque de gestión de riesgos definido por la norma ISO 31000. Para ello, propone una metodología estructurada que comprende las siguientes etapas:

- Determinar el contexto organizacional, considerando factores internos y externos que afectan la gestión documental, como el marco normativo, estructura institucional, sistemas tecnológicos y obligaciones regulatorias.
- Identificación de riesgos, mediante el uso de listas de verificación u otras herramientas que permitan reconocer amenazas como pérdida, acceso no autorizado, obsolescencia tecnológica, alteración o destrucción de documentos.
- Análisis de riesgos, empleando técnicas como el análisis de impacto en el negocio (BIA), análisis de confiabilidad humana (HRA) y el enfoque “bow-tie”, que permiten evaluar causas, consecuencias y vulnerabilidades.
- Evaluación de riesgos, incorporando criterios de aceptabilidad, análisis costo-beneficio, priorización de amenazas y uso de indicadores, lo que permite tomar decisiones informadas respecto a medidas de control y mitigación.

Esta norma internacional resalta que **no aborda directamente la mitigación de riesgos, pero sí proporciona los fundamentos necesarios para planificar controles proporcionales y eficaces**. En este sentido, promueve la incorporación de la gestión de riesgos documentales dentro del sistema de control interno institucional, asegurando una integración efectiva con otras áreas críticas como tecnologías de la información, auditoría interna y cumplimiento normativo.

Asimismo, la ISO 18128:2024 se articula directamente con otras normas relevantes en el ámbito de la gestión documental, tales como la ISO 30300 (Conceptos y Vocabulario), la ISO 30301 (Requisitos de los SGD) y la ISO 15489 (Gestión de Registros), lo que permite su aplicación eficiente, coherente y complementaria.

Para los servicios públicos, esta norma representa una herramienta fundamental para fortalecer la gobernanza documental y asegurar que los documentos institucionales sean gestionados con los más altos estándares de integridad, trazabilidad y cumplimiento, en conformidad con los principios de probidad, eficiencia y transparencia que rigen la función pública.



B. Guía ARMA International: Evaluación y Mitigación de Riesgos Documentales. Association of Records Managers and Administrators.

La guía “Evaluating and Mitigating Records and Information Risks” (ARMA International, 2009), desarrollada por la Association of Records Managers and Administrators, constituye una referencia fundamental en la gestión documental y la gobernanza de la información.

Esta propone un modelo metodológico basado en un cuadrante de riesgos que clasifica las vulnerabilidades en cuatro categorías: riesgos administrativos, de control documental, legales/regulatorios y tecnológicos. Dicha estructura permite evaluar de forma sistemática el nivel de exposición organizacional.

Así, los riesgos administrativos se relacionan con deficiencias en la gobernanza de la información, la gestión del cambio y la preparación ante emergencias; los riesgos de control documental abarcan fallas en clasificación, retención, disposición y almacenamiento; los legales/regulatorios implican incumplimientos normativos, litigios o pérdidas de evidencia; y los tecnológicos consideran amenazas como la obsolescencia digital, brechas de seguridad o fallos en el respaldo de información.

Además, la guía incorpora una herramienta de evaluación estructurada en once áreas clave, que permite calcular un índice de riesgo por cuadrante. También entrega estrategias de mitigación como el perfilado de datos, la preservación digital conforme a normas ISO N°s 14721 y 16363, y la consolidación de una gobernanza colaborativa con el respaldo de la alta dirección.

Ahora, en contextos como el sector público, este enfoque se alinea con principios de trazabilidad, cumplimiento normativo y transparencia institucional, siendo especialmente útil para fortalecer sistemas de gestión documental y garantizar la rendición de cuentas.



C. Documento Técnico N° 70 de 2022, del CAIGG sobre Implantación, Mantención y Actualización del Proceso de Gestión de Riesgos en el Sector Público.

Este Documento Técnico (en actualización) tiene como principal objetivo **facilitar a las organizaciones gubernamentales, la implementación y cumplimiento del Proceso de Gestión de Riesgos, así como su mantención y mejora continua.** Su enfoque técnico está basado principalmente en la Norma Chilena NCh-ISO 31000:2018, Gestión del Riesgo - Principios y Orientaciones, y en menor medida en el Marco de Gestión de Riesgos Corporativos ERM – COSO II.

Dicho documento, establece en uno de sus anexos que la gestión de riesgos en los sistemas de información y gobierno electrónico es fundamental para garantizar la seguridad, integridad y disponibilidad de los datos. Por lo tanto, es esencial identificar y mitigar amenazas tanto internas como externas, incluyendo ciberataques, desastres naturales, errores humanos y fraudes. Entre los riesgos destacados se encuentran la pérdida de integridad de la información, el acceso no autorizado y las dificultades en la recuperación ante incidentes. Ahora, para abordar estos desafíos, se recomiendan controles específicos como mecanismos criptográficos (firmas digitales, certificados digitales, firewalls), políticas de acceso restringido, segregación de funciones, procedimientos de respaldo periódico, y planes de contingencia que aseguren la continuidad operativa.

En este contexto, los documentos electrónicos en las organizaciones representan una pieza fundamental para la exactitud, legalidad, y trazabilidad de las transacciones y procesos administrativos. Sin embargo, su manejo y protección conllevan diversos riesgos que deben ser cuidadosamente identificados y gestionados para garantizar su integridad, autenticidad, confidencialidad y disponibilidad.

A modo de ejemplo en el documento se consideran los siguientes:



C. Documento Técnico N° 70 de 2022, del CAIGG sobre Implantación, Mantenimiento y Actualización del Proceso de Gestión de Riesgos en el Sector Público.

● **Riesgos de Autorización:**

Este riesgo está asociado a que la creación, modificación, archivo, acceso, y eventual destrucción de los documentos electrónicos sean realizados únicamente por personas autorizadas y responsables. La falta de controles adecuados puede permitir que usuarios no autorizados accedan o manipulen información sensible, generando posibles fraudes o alteraciones ilícitas. La gestión de permisos, perfiles de usuario y controles de acceso basados en roles son esenciales para mitigar este riesgo.

● **Riesgos de Autenticación:**

Referido a la capacidad de verificar de manera fehaciente la identidad de quienes generan, modifican o acceden a los documentos electrónicos es crucial para evitar suplantaciones o accesos indebidos. La utilización de mecanismos de autenticación robustos, como certificados digitales, firma electrónica y tokens, ayuda a garantizar que solo las personas autorizadas puedan realizar acciones sobre los documentos, asegurando así la integridad y confianza en el sistema.

● **Riesgos de Integridad:**

Son aquellos que se relacionan con la exactitud, completitud y oportunidad de los datos, referidos a la modificación no autorizada o accidental de documentos electrónicos puede afectar la veracidad y confiabilidad de la información contenida. Esto puede ocurrir por errores en la manipulación, fallos en los sistemas, o ataques maliciosos que alteren el contenido. Controles como firmas electrónicas, hash y controles de versiones, así como mecanismos de auditoría y trazabilidad, son fundamentales para conservar la integridad de los documentos a lo largo del ciclo de vida.

● **Riesgo de Confidencialidad:**

Referido a la exposición no autorizada de documentos electrónicos puede llevar a la divulgación de información confidencial, con posibles impactos reputacionales, legales y económicos. La aplicación de controles de cifrado, protocolos seguros de transmisión y políticas de clasificación de documentos, junto con la segregación de acceso, son necesarios para mantener la confidencialidad según corresponda.

● **Riesgos de No Repudio:**

Relativo a la imposibilidad de probar de manera irrefutable que una transacción o documento fue enviado o recibido por las partes involucradas puede poner en riesgo la validez legal y la responsabilidad de las acciones. El uso de firmas digitales avanzadas, timestamping y registros de auditoría ayuda a garantizar que cada parte no pueda negar su participación en la generación o recepción del documento, fortaleciendo la confianza en los procesos digitales.

● **Riesgos de Accesibilidad:**

Corresponden a la posibilidad de que los datos o documentos no se encuentren disponibles de forma oportuna y continua para el cumplimiento de funciones institucionales, obligaciones legales, tributarias o requerimientos de auditoría.

Ahora bien, en el modelamiento de riesgos en la gestión documental, resulta crucial identificar estos riesgos específicos y definir controles efectivos que puedan prevenir, detectar y corregir incidentes relacionados. La integración de controles tecnológicos, políticas internas y capacitación constante de los usuarios conforma un marco integral que asegura la protección de los documentos electrónicos y la sostenibilidad de la gestión documental en el entorno digital.



C. Documento Técnico N° 70 de 2022, del CAIGG sobre Implantación, Mantención y Actualización del Proceso de Gestión de Riesgos en el Sector Público.

Por lo tanto, para la identificación de controles, es fundamental considerar la existencia de controles generales que operan de manera habitual en relación con los riesgos identificados en los procesos. Estos controles incluyen las políticas y procedimientos aprobados y difundidos respecto a la seguridad en accesos digitales y físicos, la segregación de funciones incompatibles, los controles de acceso, las políticas de retención, archivo o almacenamiento, así como la accesibilidad, distribución y destrucción de documentos electrónicos y otros datos. Igualmente, se deben tener en cuenta la administración de pistas o rastros de auditoría (Audit Trail), los contratos con proveedores de servicios tecnológicos, programas de capacitación y desarrollo de competencias, instrucciones sobre el uso seguro del correo electrónico, el monitoreo del cumplimiento de las políticas establecidas y la implementación de tecnologías de encriptación, firmas electrónicas y certificados digitales.

Adicionalmente, es necesario identificar y establecer controles específicos que respondan a los riesgos particulares asociados a cada proceso. Estos controles específicos permiten mitigar riesgos particulares, garantizando la protección, confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de las normativas y políticas de seguridad institucional.

- **Controles para Riesgos de Autenticación:**

Smart card o tokens, Password, Biometría, PKI Infraestructura de clave pública, certificados digitales, Firewalls, etc.

- **Controles para Riesgos de Integridad:**

Control de acceso a aplicaciones, funciones automáticas que permitan segregación de funciones, validación de datos, reportes de excepciones, controles de secuencia numérica y de coincidencia, control de rastros de correcciones, firma electrónica, firewalls entre otros.

- **Controles para Riesgos de No Repudio:**

Técnicas criptográficas, certificados digitales, firma electrónica avanzada, time stamping, entre otros.

- **Controles para Riesgos de Autorización:**

Controles de acceso, definición de perfiles de usuario en redes, aplicaciones y sistemas; firma electrónica, certificados digitales, etc.

- **Controles para Riesgos de Disponibilidad:**

Controles asociados a la adquisición, desarrollo y mantenimiento de sistemas, mecanismos de recuperación de pérdida de datos, planes de contingencia, políticas de respaldo periódico de la información, y otros.

- **Controles para Riesgos de Confiabilidad:**

Cifrado o encriptación, controles de acceso lógico y físicos a los sistemas y servidores, procedimientos de manipulación de copiado, almacenamiento, transmisión y destrucción, documentos reservados con niveles de acceso determinados, protocolos de seguridad sobre Internet (SSL), firewalls, entre otros.

4.1 DEFINICIÓN DE UNA TIPOLOGÍA GENERAL DE RIESGOS

En el marco del desarrollo de matrices de análisis de riesgos y controles aplicadas a los procesos de gestión documental, **resulta indispensable contar con una tipología orientada a clasificar y agrupar los riesgos operativos identificados, de acuerdo con su naturaleza, origen o impacto institucional.** Sin duda, esta categorización facilita una evaluación sistemática, permite asignar responsabilidades específicas, habilita el análisis comparado y orienta el diseño de controles proporcionales y pertinentes para cada tipo de amenaza.

Desde el punto de vista del origen de los riesgos, estos pueden clasificarse en dos grandes categorías: riesgos de fuente externa y riesgos de fuente interna.

- Riesgos de fuente externa:**
Corresponden a aquellos cuyo origen se encuentra fuera del ámbito de control directo de la institución pública. En materia de gestión documental, incluyen situaciones como cambios normativos que alteren los requisitos de conservación o acceso, fallos en servicios tecnológicos externalizados (como proveedores de almacenamiento en la nube), desastres naturales que afecten archivos físicos o incidentes de ciberseguridad que comprometan la integridad de plataformas externas.
- Riesgos de fuente interna:**
Tienen su origen al interior de la organización y están directamente relacionados con su estructura, procesos, recursos o decisiones. En la gestión documental, incluyen ejemplos como la ausencia de políticas claras de archivo, falta de capacitación del personal en normativa archivística, errores en la clasificación o custodia de documentos, deficiencias en la trazabilidad de actos administrativos, o la inexistencia de controles para la eliminación de documentos según plazo legal.

A continuación, se presenta una tabla con ejemplos de categorías de riesgos documentales, adaptada del marco COSO ERM e incorporada en la metodología de gestión de riesgos institucionales promovida por el CAIGG:

<i>Tipo de Riesgo</i>	<i>Elementos que lo Caracterizan</i>	<i>Ejemplos Específicos</i>
Financiero	Uso inadecuado o ineficiente de los recursos públicos asignados a la gestión documental.	• Ejemplos de Riesgos Específicos en Gestión Documental. • Desvío de fondos de digitalización o conservación. • Gasto en insumos sin planificación documental. • Licitaciones de soluciones tecnológicas sin evaluación técnica.
Económico	Limitaciones o desequilibrios presupuestarios que afectan la planificación documental.	• Insuficiencia de recursos para migraciones digitales. • Cancelación de proyectos de digitalización clave. • Congelamiento de fondos que impiden mantener depósitos o servicios archivísticos.
Social	Factores socioculturales que afectan la percepción, uso o valorización de los documentos.	• Falta de cultura archivística en funcionarios/as. • Subvaloración del rol documental en la función pública. • Brechas de acceso ciudadano por baja alfabetización digital.
Tecnológico	Infraestructura tecnológica deficiente o desactualizada que afecta los procesos digitales.	• Fallas de respaldo en servidores documentales. • Pérdida de archivos digitales por formatos obsoletos. • Incompatibilidad entre plataformas documentales por falta de interoperabilidad.
Estratégico	Desalineación entre la gestión documental y la planificación estratégica institucional.	• No incorporación del archivo en la transformación digital. • Ausencia de un Plan Institucional de Gestión Documental. • Documentos no considerados en el diseño de procesos electrónicos.

<i>Tipo de Riesgo</i>	<i>Elementos que lo Caracterizan</i>	<i>Ejemplos Específicos</i>
Medioambiental	Amenazas físicas y ambientales que afectan la conservación de documentos.	• Daños por humedad, calor, polvo o plagas. • Almacenamiento en lugar inadecuado o sin monitoreo. • Vulnerabilidad de archivos físicos ante incendios o sismos.
Procesos	Fallas en el diseño o ejecución de los procedimientos técnicos del ciclo de vida documental.	• Eliminación de documentos sin autorización formal. • Clasificación errónea o no aplicable. • Ausencia de trazabilidad o cadena de custodia.
Legal y Regulatorio	Incumplimientos normativos respecto a conservación, acceso, eliminación y protección de datos personales.	• Destrucción sin autorización de Archivo Nacional. • Vulneración de plazos de retención establecidos por ley. • Incumplimiento de la Ley N°21.180 o Ley N°20.285 (Transparencia).
Personas	Capacidades insuficientes o actuaciones indebidas del personal responsable de los documentos.	• Manipulación indebida de archivos sensibles. • Personal sin formación en normativa archivística. • Desconocimiento de plataformas digitales oficiales (CPAT, DocDigital, etc.).
Imagen y Reputación	Daño a la confianza institucional por fallas en la gestión de la información y documentación.	• No incorporación del archivo en la transformación digital. • Ausencia de un Plan Institucional de Gestión Documental. • Documentos no considerados en el diseño de procesos electrónicos.
Sistemas	Fallas técnicas o deficiencias operativas en los sistemas informáticos documentales.	• Software documental sin controles de auditoría. • Errores en metadatos afectan búsqueda o recuperación. • Ausencia de integración con otras plataformas del Estado (PISEE, CPAT, etc.).
Bienes muebles e inmuebles	Infraestructura física insuficiente o en mal estado para el resguardo documental.	• Depósitos sin medidas de seguridad ni control ambiental. • Documentos extraviados por falta de custodia adecuada. • Carencia de mobiliario técnico normado (estanterías, cajas).

Esta tipología será utilizada como base para la clasificación de riesgos en las matrices correspondientes, vinculando cada etapa o subproceso técnico con los factores de exposición que pueden comprometer el cumplimiento normativo, la trazabilidad documental o la seguridad de la información institucional.

4.2 ESTRUCTURA DEL PROCESO DE GESTIÓN DOCUMENTAL

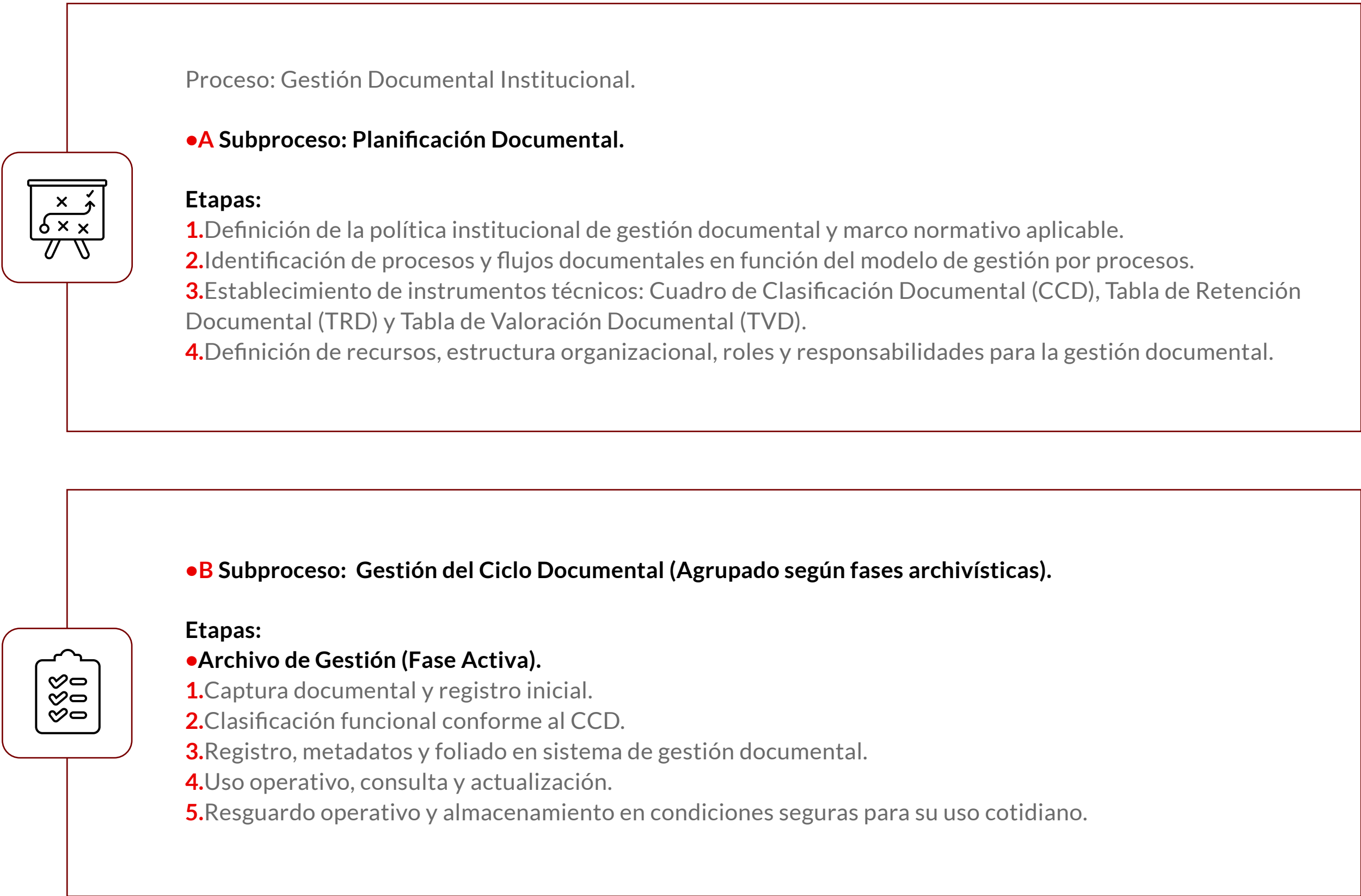
La gestión documental constituye un proceso estratégico dentro del funcionamiento institucional del sector público, cuya relevancia radica en su estrecha vinculación con la transparencia, el control interno y la toma de decisiones basada en evidencia. Esta perspectiva es coherente con los enfoques de gestión por procesos adoptados por diversos organismos públicos, y se alinea con modelos ampliamente utilizados en auditoría interna, control de gestión y gobernanza organizacional.

En términos técnicos, un proceso corresponde a un conjunto articulado de subprocesos y actividades interdependientes que contribuyen al logro de los objetivos estratégicos institucionales. Bajo esta lógica, la gestión documental integra múltiples subprocesos, como la planificación, captura, clasificación, archivo, eliminación y resguardo de la información, los cuales operan de manera continua y transversal a lo largo del ciclo de vida de la documentación pública.

Dada su naturaleza transversal, la gestión documental interactúa con otros procesos críticos institucionales, tales como la atención de usuarios, la rendición de cuentas, la respuesta a revisiones, la gestión de solicitudes de información (transparencia activa y pasiva), y la generación de insumos para la toma de decisiones. En consecuencia, su adecuada planificación, control y mejora continua es fundamental para asegurar el cumplimiento de los principios de legalidad, trazabilidad, eficiencia, responsabilidad administrativa y probidad pública.

Desde una perspectiva normativa y técnica, concebir la gestión documental como un proceso permite articularla coherentemente con los sistemas de control interno, las matrices de riesgos operacionales, los mapas de procesos institucionales y las revisiones orientadas a procesos. Este enfoque fortalece la gobernanza de la información pública y contribuye a la calidad, disponibilidad y seguridad del soporte documental que respalda la gestión administrativa y estratégica del Estado.

Ahora, con el fin de facilitar la comprensión técnica y didáctica de este proceso, en el presente documento se propone una estructura esquemática y funcional que organiza sus principales subprocesos y etapas, conforme a los estándares nacionales e internacionales aplicables, así como a las mejores prácticas de gestión documental adoptadas en el sector público chileno.





●**Archivo Intermedio (Fase Semiactiva):**

- 6.Transferencia documental desde unidades generadoras.
- 7.Revisión de plazos de conservación según TRD.
- 8.Almacenamiento temporal bajo condiciones de resguardo intermedio.
- 9.Control de acceso físico o digital.
- 10.Evaluación documental para disposición final o transferencia histórica.



●**Archivo Histórico (Fase Inactiva):**

- 11.Valoración patrimonial para su conservación permanente.
- 12.Transferencia definitiva al Archivo Nacional o repositorio institucional autorizado.
- 13.Conservación especializada bajo criterios archivísticos y normativos.
- 14.Regulación del acceso conforme a normativa de transparencia, reserva o secreto.
- 15.Disponibilización para fines de memoria institucional, investigación y control público.



●**C Subproceso: Eliminación Documental Regulada.**

Etapas:

- 1.Identificación documental sujeta a eliminación según TVD y normativa aplicable.
- 2.Revisión de requisitos legales y plazos de conservación.
- 3.Evaluación de valor secundario (histórico, legal, probatorio).
- 4.Análisis de formato o soporte (físico, digital, microforma).
- 5.Digitalización previa si procede, conforme a Ley N° 18.845.
- 6.Registro y respaldo digital y metadatos asociados.
- 7.Emisión de resolución administrativa de autorización (según jerarquía institucional).
- 8.Elaboración de acta de eliminación con firma responsable.
- 9.Eliminación física o digital bajo método seguro e irreversible.
- 10.Registro institucional permanente del procedimiento de eliminación.



●**D Subproceso: Resguardo de la Información.**

Etapas:

- 1.Identificación y clasificación de información crítica o sensible.
- 2.Diagnóstico de riesgos y planificación de medidas de protección documental.
- 3.Diseño e implementación de políticas institucionales de resguardo y acceso.
- 4.Implementación de medidas de continuidad operativa en soporte documental.
- 5.Monitoreo y revisión periódica de sistemas de protección.
- 6.Generación de reportes técnicos y acciones de mejora continua.
- 7.Verificación de cumplimiento normativo y respuesta ante revisiones o sanciones.

4.3 MATRICES DE ANÁLISIS DE RIESGO Y CONTROL

Las matrices de análisis de riesgo y control que se presentan a continuación tienen como propósito **identificar de forma sistemática los riesgos críticos asociados a la gestión documental institucional, así como proponer controles clave orientados a su mitigación**, conforme al principio de proporcionalidad, al marco normativo vigente y a las buenas prácticas en administración pública.

Cada matriz se estructura a partir de la **descomposición operativa del proceso de gestión documental**, considerando sus subprocesos esenciales desde una perspectiva funcional: planificación, ciclo de vida documental, eliminación regulada y resguardo de la información. Para cada uno se detallan riesgos específicos por etapa, controles orientadores (preventivos, detectivos o correctivos) y la documentación mínima requerida como evidencia de cumplimiento. Para cada subproceso o etapa se identifican tres elementos clave:

- **Riesgos asociados:** Situaciones de incertidumbre que pueden afectar la eficacia, legalidad o integridad del subproceso.
- **Controles teóricos mitigantes:** Acciones orientadoras que permiten prevenir, detectar o corregir los riesgos identificados.
- **Documentación requerida como evidencia:** Registros o respaldos necesarios para verificar el cumplimiento institucional, apoyar auditorías y fortalecer la trazabilidad y rendición de cuentas.

Estas matrices han sido diseñadas como herramientas de referencia técnica para alinear la gestión documental con los principios de control interno, legalidad, transparencia y mejora continua, conforme a las obligaciones normativas vigentes en el sector público chileno.

4.3.1 Matriz de Análisis de la Planificación Documental

La planificación documental constituye el punto de partida para una gestión documental eficiente, trazable y jurídicamente respaldada. Este subproceso **abarca la definición de políticas institucionales, normativa interna, instrumentos técnicos y estructuras organizacionales que deben sustentar todo el ciclo de vida de la documentación institucional**.

La matriz asociada identifica riesgos que pueden debilitar la planificación o generar inconsistencias normativas, funcionales u operativas desde el origen del sistema documental. **Los controles propuestos están orientados a prevenir omisiones, definir responsabilidades y asegurar la coherencia entre los instrumentos técnicos y los marcos regulatorios vigentes**.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
01 Definición de una política y una normativa institucional.	1. La inexistencia de una política formal para la gestión documental aprobada institucionalmente limita la estandarización de prácticas y genera incumplimientos normativos.	- Elaborar una política de gestión documental alineada con la normativa vigente, mediante revisión técnica y jurídica, durante la fase de planificación institucional, por la función encargada de la gestión normativa documental, con el propósito de establecer directrices claras y uniformes para todas las unidades. - Validar formalmente la política institucional mediante resolución aprobada por la autoridad competente, antes de su implementación, por el área responsable del marco normativo institucional, con el propósito de asegurar su legitimidad y obligatoriedad. - Difundir la política institucional aprobada mediante canales oficiales de comunicación interna, durante los días posteriores a su emisión, por quien tenga a cargo la difusión normativa, con el propósito de asegurar su conocimiento y aplicación transversal.	- Política institucional aprobada. - Resolución formal de validación. - Evidencia de difusión (un correo, una circular, una capacitación).

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
01 Definición de una política y una normativa institucional.	2. La ausencia de normativa interna sobre clasificación, conservación y acceso documental impide la aplicación consistente de criterios técnicos y afecta la trazabilidad documental.	- Elaborar normativa interna específica sobre clasificación, conservación y acceso documental, utilizando procedimientos participativos y referenciales técnicos, durante la planificación normativa, por la función encargada de la elaboración reglamentaria documental, con el propósito de estandarizar procesos institucionales. - Revisar y actualizar periódicamente (Ej. anual) la normativa interna sobre gestión documental mediante un proceso formal de evaluación, por quien tenga a cargo la actualización normativa, con el propósito de mantenerla alineada con los cambios institucionales o regulatorios. - Registrar y mantener disponible la normativa interna en los sistemas oficiales de la institución, inmediatamente después de su aprobación, por la unidad responsable del repositorio normativo, con el propósito de garantizar su acceso institucional.	- Reglamento o manual interno de gestión documental. - Registro de versiones y revisiones. - Publicación en sistema institucional (intranet, archivo normativo).
	3. La falta de validación jurídica y técnica de la política o reglamentos institucionales podría generar inconsistencias con el marco legal, exponiendo a la entidad a observaciones externas.	- Someter a revisión técnica y jurídica todo proyecto de política o normativa documental, antes de su promulgación, por la unidad encargada de la validación normativa, con el propósito de asegurar su conformidad con el marco legal vigente. - Aplicar un procedimiento institucional de revisión interfuncional de la normativa documental mediante mesas técnicas, durante el ciclo de aprobación normativa, por el equipo responsable del control normativo interno, con el propósito de validar integralmente sus contenidos. - Registrar las actas y observaciones derivadas del proceso de validación técnica y jurídica, inmediatamente después de cada sesión de revisión, por la unidad que coordina la elaboración normativa, con el propósito de asegurar trazabilidad y respaldo ante revisiones.	- Informes de revisión técnica y jurídica. - Procedimiento institucional de validación normativa. - Actas de validación y de las observaciones documentadas.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplo de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
02 Identificación de los procesos y de los flujos documentales.	1. La omisión en el levantamiento de procesos generadores de documentos puede generar vacíos en la cobertura del SGD, afectando su integridad y coherencia funcional.	- Realizar el levantamiento sistemático de procesos documentales mediante entrevistas, análisis de procedimientos y revisión de normativa, una vez por año o cuando existan reestructuraciones institucionales, por quien tenga a cargo la validación del proceso documental, con el propósito de asegurar una cobertura completa y actualizada. - Registrar todos los flujos documentales identificados en una matriz institucional que detalle tipo de documento, soporte, unidad generadora y responsables, durante la etapa de planificación documental, por la unidad responsable del diagnóstico de procesos, con el propósito de facilitar su trazabilidad y gestión. - Validar los procesos y flujos identificados con las unidades operativas mediante instancias formales de revisión, antes de consolidar los instrumentos técnicos, por el área encargada de coordinación documental, con el propósito de asegurar la precisión del levantamiento.	- Matriz de procesos y flujos documentales. - Registro de entrevistas, talleres o reuniones. - Validación formal con unidades operativas (actas o correos).
	2. La inexistencia de una caracterización clara de los flujos documentales puede dificultar la estructuración de series y subseries, comprometiendo la elaboración de instrumentos técnicos como el CCD o la TRD.	- Documentar cada flujo documental identificando etapas, soportes, responsables y puntos críticos, durante el proceso de mapeo, por la unidad que lidera la planificación documental, con el propósito de establecer insumos para la construcción del cuadro de clasificación y tablas de retención. - Utilizar herramientas visuales como diagramas o fichas estandarizadas para representar los flujos documentales, inmediatamente después de su levantamiento, por el área técnica responsable, con el propósito de facilitar su interpretación y validación. - Revisar periódicamente (Ej. anual) la coherencia entre los flujos documentales mapeados y los cambios en los procedimientos institucionales, por la función encargada de la actualización de instrumentos técnicos, con el propósito de mantener actualizados los insumos de clasificación.	- Fichas de flujo documental por unidad o proceso. - Diagramas o mapas de flujo validados. - Registro de revisión o actualización periódica de flujos.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
02 Identificación de los procesos y de los flujos documentales.	3. La falta de identificación de puntos críticos en los flujos documentales impide anticipar riesgos operacionales y debilita los controles de trazabilidad y conservación.	- Analizar los flujos documentales identificados para detectar puntos críticos de pérdida, duplicación o acceso no autorizado, durante el proceso de planificación, por quien tenga a cargo la revisión del riesgo documental, con el propósito de definir medidas de control preventivo. - Incorporar los puntos críticos identificados en los protocolos operativos de cada unidad mediante guías o instructivos internos, al finalizar el diagnóstico de procesos, por el área de gestión documental, con el propósito de fortalecer la trazabilidad y conservación. - Capacitar al personal involucrado en los procesos documentales sobre los riesgos asociados a los puntos críticos de sus flujos, una vez implementadas las mejoras, por la unidad de la responsable de la formación o de control interno, con el propósito de promover buenas prácticas de gestión documental.	- Informe de análisis de riesgos documentales por flujo. - Protocolos operativos con medidas aplicadas. - Registro de todas las capacitaciones realizadas.
03 Instrumentos técnicos que se establecieron	1. La inexistencia de instrumentos técnicos como el CCD, TRD y TVD impide organizar y controlar la documentación institucional según criterios funcionales y plazos legales, afectando la trazabilidad y cumplimiento normativo.	- Elaborar el Cuadro de Clasificación Documental (CCD), la Tabla de Retención Documental (TRD) y la Tabla de Valoración Documental (TVD), utilizando lineamientos del Archivo Nacional, durante el proceso de planificación, por quien tenga a cargo la implementación del SGD, con el propósito de organizar adecuadamente las series documentales institucionales. - Validar los instrumentos técnicos mediante resolución institucional aprobada por la autoridad competente, posterior a su revisión técnica, por la unidad responsable del marco normativo documental, con el propósito de asegurar su aplicación obligatoria. - Registrar y publicar los instrumentos técnicos aprobados en el sistema institucional de gestión documental, inmediatamente después de su validación, por la unidad encargada del archivo institucional, con el propósito de facilitar su uso transversal.	- CCD, TRD y TVD elaborados y aprobados. - Resolución institucional de validación. - Publicación en intranet o repositorio oficial.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
03 Instrumentos técnicos que se establecieron.	2. La desactualización de los instrumentos técnicos documentales frente a cambios institucionales o normativos puede generar discrepancias en la aplicación de plazos y series, afectando la gestión operativa y la legalidad de la eliminación.	- Evaluar periódicamente (Ej. anual) la vigencia y adecuación del CCD, TRD y TVD mediante revisión técnica y normativa, durante el primer trimestre del año, por la unidad responsable de la actualización documental, con el propósito de mantenerlos alineados con la estructura y funciones institucionales. - Aplicar un procedimiento institucional para la revisión y modificación de instrumentos técnicos que contemple participación de las unidades responsables, por la función encargada de la gestión normativa documental, con el propósito de asegurar la validez técnica y operativa de los cambios. - Registrar todas las versiones históricas y vigentes de los instrumentos técnicos con sus respectivas fechas de aprobación, por la unidad que gestiona el archivo normativo documental, con el propósito de garantizar trazabilidad ante revisiones o fiscalizaciones.	- Registro de versiones y revisiones del CCD, TRD, TVD. - El Procedimiento institucional usado para la actualización. - Actas o informes de revisión participativa.
	3. La falta de alineación entre los instrumentos técnicos y los flujos reales de trabajo documental puede generar aplicaciones erróneas que comprometan la eficiencia y el cumplimiento legal.	- Vincular el diseño de los instrumentos técnicos a los flujos y series documentales previamente mapeados, durante el proceso de construcción, por quien tenga a cargo la articulación entre procesos y clasificación documental, con el propósito de asegurar su coherencia operativa. - Verificar la aplicabilidad de los instrumentos técnicos mediante pilotos o pruebas controladas en unidades seleccionadas, antes de su implementación total, por la unidad de archivo institucional, con el propósito de ajustar contenidos y mejorar la funcionalidad. - Capacitar a los funcionarios responsables del uso de CCD, TRD y TVD en cada unidad administrativa, antes de la entrada en vigor de los instrumentos, por quien tenga a cargo la formación documental, con el propósito de garantizar su correcta aplicación.	- La matriz de correspondencia entre flujos documentales y series clasificadas. - Informe de validación de pruebas piloto. - Registro de todas las capacitaciones aplicadas.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
4. Definición de los recursos, de estructura organizacional y roles.	1. La falta de asignación de recursos humanos y tecnológicos específicos para la gestión documental dificulta su implementación efectiva, generando sobrecarga operativa y riesgos de incumplimiento.	- Identificar los recursos necesarios para la implementación del SGD mediante un diagnóstico institucional, durante la fase de planificación anual, por quien tenga a cargo la planificación operativa institucional, con el propósito de asegurar su viabilidad técnica y funcional. - Asignar funciones formales en gestión documental a través de perfiles de cargo, descripciones de rol o resoluciones internas, antes de la implementación del modelo, por la función encargada de la organización administrativa, con el propósito de garantizar claridad de responsabilidades. - Incorporar en el presupuesto institucional los recursos necesarios para infraestructura documental, plataformas tecnológicas y capacitación, durante el ciclo presupuestario anual, por la unidad responsable de la planificación financiera, con el propósito de asegurar sostenibilidad operativa.	- Diagnóstico de las necesidades para gestión documental. - Resoluciones o perfiles de cargo asignando funciones documentales. - Presupuesto institucional con las asignaciones específicas para gestión documental.
	2. La ausencia de una estructura organizacional definida para la gestión documental genera dispersión de funciones, debilita la coordinación institucional y afecta la trazabilidad de decisiones.	- Establecer una estructura organizacional formal para la gestión documental mediante la designación de unidades, comités o encargados responsables, antes de la ejecución operativa, por la unidad de gestión organizacional, con el propósito de consolidar el sistema documental como función institucional. - Formalizar los mecanismos de articulación entre la unidad de archivo y las unidades operativas mediante procedimientos internos, durante el diseño del modelo de gestión documental, por quien tenga a cargo la implementación del sistema, con el propósito de asegurar la coordinación funcional. - Mantener actualizado un organigrama funcional vinculado al modelo de gestión documental institucional, revisado periódicamente (Ej. anual), por la unidad responsable de estructura organizacional, con el propósito de reflejar los roles vigentes y facilitar la supervisión.	- Organigrama funcional actualizado. - Actas de constitución de comités o designación de responsables. - Los procedimientos internos de coordinación entre unidades.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
4. Definición de los recursos, de la estructura organizacional y roles.	3. La inexistencia de perfiles y competencias definidos para los encargados de gestión documental limita la capacidad técnica para aplicar instrumentos y protocolos, afectando su cumplimiento.	- Diseñar perfiles de cargo específicos para funciones de gestión documental, incluyendo competencias técnicas y conocimientos normativos, durante la planificación de recursos humanos, por la unidad de desarrollo organizacional, con el propósito de asegurar una implementación competente y conforme a estándares. - Capacitar al personal con funciones documentales en normativa, herramientas e instrumentos técnicos, durante la etapa de implementación y cada vez que existan actualizaciones relevantes, por quien tenga a cargo la formación interna, con el propósito de asegurar un desempeño adecuado. - Evaluar periódicamente las competencias del personal asignado a funciones documentales mediante instrumentos de evaluación institucional, al menos una vez al año, por la unidad de control de gestión o supervisión interna, con el propósito de identificar brechas y oportunidades de mejora.	- Perfiles de cargo formalizados. - Registros de la capacitación técnica documental. - Instrumentos de evaluación de las competencias y los resultados.

4.4.2 Matriz de Análisis de la Gestión del Ciclo de Vida Documental

El ciclo de vida documental comprende el conjunto de fases sucesivas que transita la documentación institucional desde su creación o recepción hasta su disposición final (conservación permanente o eliminación). Este enfoque se estructura en tres grandes fases archivísticas: archivo de gestión (fase activa), archivo intermedio (semiactiva) y archivo histórico (fase inactiva), cada una con requerimientos específicos en materia de conservación, acceso y control.

La matriz identifica riesgos en cada fase del ciclo, abordando amenazas como errores en el registro o clasificación, fallas en el control de acceso, omisiones en la evaluación de valor documental y condiciones deficientes de almacenamiento.

Los controles definidos buscan reforzar la trazabilidad, integridad, seguridad y disponibilidad de la documentación pública, facilitando la toma de decisiones, el cumplimiento normativo y el resguardo de evidencia institucional.

• Archivo de Gestión (fase activa).

<i>Etapa o Subproceso</i>	<i>Riesgos Asociados</i>	<i>Ejemplo de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
1A. Captura del Documento y del Registro Inicial.	1. La omisión en la incorporación formal de documentos recibidos o generados internamente debilita la trazabilidad institucional y puede generar pérdida o desconocimiento de antecedentes relevantes para la gestión administrativa.	- Registrar todos los documentos recibidos o generados internamente mediante su incorporación obligatoria en el SGD institucional, de forma inmediata tras su creación o recepción, por quien tenga a cargo la validación del proceso documental, con el propósito de asegurar trazabilidad desde el origen. - Evaluar periódicamente el cumplimiento del registro de documentos mediante revisiones sistemáticas de correspondencia entre los documentos físicos o digitales y los registros en el sistema, al menos una vez al mes, por la función encargada de la custodia documental. - Emitir reportes automáticos de ingresos pendientes, documentos no clasificados o registros incompletos, generados por el SGD, con revisión periódica (Ej. semanal) por el área que administra el archivo institucional, con el propósito de activar medidas correctivas oportunas.	- Registro del ingreso documental institucional. - Bitácora de control de recepción. - Informe de revisión documental periódica. - Reporte del sistema con alertas de registro incompleto.
	2. La ausencia de procedimientos estandarizados para el ingreso de documentos físicos o digitales incrementa el riesgo de registros incompletos o duplicados, afectando la organización y control de la información institucional.	- Aplicar un procedimiento institucional estandarizado para la captura documental, aprobado conforme a la normativa interna, que defina pasos, formatos y sistemas a utilizar, por el personal autorizado según el procedimiento correspondiente. - Revisar periódicamente (Ej. semestral) la aplicación del procedimiento mediante revisiones internas o supervisiones documentadas, por la función encargada del control de procesos documentales. - Incluir actividades de verificación del ingreso documental en las listas de control operativo que utilizan las unidades que generan o reciben documentación, con el propósito de reforzar la aplicación uniforme del procedimiento.	- Procedimiento institucional aprobado. - Instructivo operativo. - Informe de revisiones o supervisiones - Lista de control de ingreso aplicada por unidades.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
1A. Captura del Documento y del Registro Inicial.	3. La recepción de documentos sin asignación de responsable ni validación de su procedencia dificulta su seguimiento, clasificación y resguardo, comprometiendo la calidad y fiabilidad de los archivos institucionales.	- Verificar la procedencia y completitud de cada documento antes de su incorporación al sistema institucional, mediante cotejo de remitente, firma, fecha y anexos, al momento de recepción, por quien tenga a cargo la validación del proceso documental. - Registrar de forma obligatoria la unidad receptora y el responsable designado para cada documento capturado, utilizando los campos predefinidos del sistema institucional de gestión documental. - Aplicar un protocolo de recepción documental que contemple revisión cruzada con registros de ingreso oficial (correspondencia, derivación, canal digital), para cada documento recibido, como medida preventiva de errores o duplicaciones.	- Registro de recepción con campos completos. - Formulario de validación de ingreso. - Protocolo de control de procedencia. - Registro de derivación o trazabilidad de origen.
1B. Clasificación Funcional conforme a CCD.	1. La omisión en la asignación de códigos de clasificación a los documentos capturados dificulta su identificación, afecta la organización del archivo institucional y compromete la trazabilidad documental.	- Asignar un código de clasificación documental a cada documento capturado, conforme al Cuadro de Clasificación Documental (CCD) vigente, en el momento de su registro inicial, por quien tenga a cargo la validación del proceso documental. - Implementar validaciones automáticas en el SGD que impidan finalizar el registro sin incluir un código de clasificación válido, configuradas por la unidad que administra la plataforma documental. - Realizar revisiones periódicas (E. trimestrales) sobre documentos ingresados sin clasificación o con código erróneo, mediante reportes del sistema y revisión cruzada.	- Registro de ingreso con código de clasificación. - Cuadro de Clasificación Documental vigente. - Reporte del sistema de validación de campos obligatorios. - Informe de revisión de clasificación aplicada.
	2. La clasificación incorrecta o inconsistente de documentos según su función o tipo puede generar desalineación con los procesos administrativos y dificultar su recuperación posterior.	- Aplicar matrices funcionales y tablas de apoyo con criterios de clasificación para cada tipo documental, disponibles para consulta permanente en los sistemas. - Incorporar la revisión de clasificación en las actividades regulares de supervisión documental, utilizando listas de cotejo que comparen clasificación aplicada versus proceso institucional de origen. - Capacitar al personal responsable sobre el uso correcto del CCD y la lógica de clasificación funcional, al menos una vez al año o cuando se actualicen los instrumentos técnicos, por la unidad responsable de formación documental.	- Matrices de clasificación funcional. - Lista de cotejo de revisión. - Registro de capacitación técnica en clasificación documental.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
1B. Clasificación Funcional conforme a CCD.	3. La inexistencia de controles sobre la calidad del registro clasificatorio limita la capacidad de verificar que los antecedentes estén correctamente categorizados y disponibles cuando se requieran.	- Establecer controles de revisión cruzada entre documentos clasificados y las series documentales registradas en el CCD, con frecuencia semestral, por la unidad responsable de la gestión documental institucional. - Documentar las observaciones y correcciones aplicadas a clasificaciones erróneas, dejando trazabilidad en informes periódicos o bitácoras internas. - Realizar muestreos aleatorios de expedientes para verificar coherencia entre el contenido documental y su clasificación funcional, como parte de las actividades de mejora continua.	- Informe de revisión cruzada CCD-documentos. - Registro de observaciones o correcciones aplicadas. - Bitácora de control o revisión documental.
1C. Registro y Foliado en el Sistema de la Gestión Documental.	1. La omisión en el registro formal de documentos en los sistemas institucionales afecta la trazabilidad, dificulta su localización y compromete la integridad del archivo.	- Registrar todos los documentos en el sistema institucional de gestión documental, incluyendo metadatos mínimos obligatorios (fecha, unidad, tipo documental, clasificación), de forma inmediata posterior a su recepción o generación, por quien tenga a cargo la validación del proceso documental. - Configurar reglas automáticas en el sistema documental que impidan cerrar el registro sin campos obligatorios completos, según lo definido en el procedimiento institucional. - Ejecutar revisiones periódicas (Ej. mensual) sobre registros incompletos o inconsistentes mediante reportes del sistema y revisión cruzada, por la función encargada del control documental.	- Registro electrónico institucional. - Parámetros de validación del sistema. - Informes de revisión de registros y evaluaciones internas.
	2. El registro incompleto o con errores en los metadatos debilita la identificación del documento, afecta su recuperación y puede generar inconsistencias en los procesos administrativos.	- Aplicar una plantilla estandarizada de metadatos en el SGD con campos obligatorios definidos por normativa interna. - Establecer un procedimiento de revisión y validación de metadatos posterior al ingreso, a cargo de quien administra la plataforma documental, con periodicidad mensual. - Capacitar a los equipos responsables en el correcto uso de metadatos y criterios de calidad para su registro, al menos una vez al año o cuando se actualicen los formatos.	- Plantilla de metadatos institucional. - Informe de revisión de calidad de registros. - Registro de todas las capacitaciones impartidas.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
1C. Registro y Foliado en el Sistema de la Gestión Documental.	3. La inexistencia de foliado o numeración secuencial en documentos en soporte físico dificulta su control, debilita la trazabilidad y puede permitir omisiones o manipulaciones no detectadas.	- Aplicar foliado manual o automatizado a los documentos físicos mediante numeración correlativa al momento de su incorporación al expediente, utilizando sellos, timbres o formatos oficiales definidos por la institución. - Incluir una hoja de control de foliado en cada expediente físico, donde se registre el rango numérico de documentos que contiene. - Verificar periódicamente (Ej. semestral) la secuencia del foliado en expedientes seleccionados mediante muestreos aleatorios, por la función encargada del resguardo documental.	- Registro de foliado aplicado. - Hoja de control de folios por expediente. - Informe de revisión o muestreo archivístico.
1D. Uso Activo, Consulta y Actualización.	1. La falta de disponibilidad oportuna de los documentos en uso activo puede generar retrasos en la toma de decisiones, afectando el cumplimiento de funciones administrativas y legales.	- Mantener los documentos activos disponibles en espacios físicos habilitados o sistemas digitales institucionales con acceso autorizado, durante toda su vigencia operativa, conforme a las directrices internas. - Verificar periódicamente (Ej. mensual) la disponibilidad y localización de documentos en uso activo mediante controles de acceso o inspecciones en terreno, por quien tenga a cargo la gestión documental. - Establecer mecanismos de reemplazo documental (copia de trabajo o respaldo temporal) ante eventos que afecten la disponibilidad inmediata, definidos por protocolo institucional.	- Registro de la disponibilidad, ya sea por ubicación física o digital. - Informe de revisión de accesibilidad. - Protocolo de reemplazo temporal de documentos en uso.
	2. La incorporación de antecedentes complementarios sin registro o control puede afectar la integridad del documento y dificultar su trazabilidad.	- Registrar toda modificación o agregado de antecedentes en bitácoras de cambios, sistemas de control de versiones o campos de seguimiento habilitados en el sistema documental, al momento de realizar el cambio. - Implementar alertas o restricciones para modificaciones a documentos clasificados como definitivos o cerrados, conforme a la política institucional. - Realizar revisiones periódicas (Ej. bimensuales) sobre la trazabilidad de documentos activos con múltiples antecedentes anexados, por quien tenga a cargo la supervisión documental.	- Bitácora de cambios o registro de versiones. - Parámetros de edición restringida. - Informe de revisión de integridad documental.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplo de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
1D. Uso Activo, Consulta y Actualización.	3. La ausencia de controles sobre el uso y consulta de documentos vigentes puede facilitar su extravío, alteración no autorizada o uso indebido.	- Registrar toda solicitud, consulta o préstamo de documentos en una bitácora institucional, indicando fecha, unidad solicitante y medio de consulta. - Aplicar perfiles diferenciados de acceso a sistemas documentales según las funciones y autorizaciones asignadas, conforme a las políticas de seguridad de la información. - Revisar periódicamente (Ej. trimestral) los registros de uso y acceso, comparándolos con la política de perfiles y la bitácora de préstamos, para detectar inconsistencias o accesos indebidos.	- Bitácora de uso, préstamo o consulta. - Parámetros de perfil en el sistema documental. - Informe de revisión de accesos documentales.
1E. El Resguardo Operativo y almacenaje en condiciones seguras.	1. La ausencia de condiciones adecuadas de resguardo durante la vigencia activa del documento puede exponer la información a deterioro, pérdida o acceso no autorizado, afectando la continuidad operativa.	- Mantener los documentos activos en espacios físicos cerrados o plataformas digitales institucionales con medidas de seguridad, acceso restringido y respaldo, durante toda su vigencia operativa. - Verificar periódicamente las condiciones de resguardo mediante inspecciones físicas o revisiones en plataformas, con frecuencia trimestral, por la función encargada de la custodia documental. - Aplicar protocolos de contingencia ante los riesgos de deterioro o pérdida documental de la política de continuidad operativa.	- Registro de condiciones de almacenamiento. - Informe de revisión física o digital. - Protocolo de contingencia para resguardo operativo.
	2. La existencia de múltiples copias no controladas de documentos activos puede generar versiones contradictorias, dificultando la verificación de información válida.	- Establecer un procedimiento institucional para la emisión, resguardo y control de copias documentales, incluyendo distinción visual obligatoria (sello o marca de agua). - Registrar la emisión de copias mediante un formulario o módulo en el sistema institucional, indicando el motivo y destino. - Verificar periódicamente (Ej. mensual) la consistencia entre documentos originales y copias, especialmente en procesos sensibles o con alta circulación interna.	- Procedimiento de control de copias. - Registro de emisión de copias. - Informe de revisión de consistencia documental.
	3. La falta de respaldo sistemático de documentos digitales activos incrementa el riesgo de pérdida de información frente a fallas técnicas o eventos imprevistos.	- Realizar respaldos periódicos de los documentos digitales activos, con frecuencia diaria o semanal, conforme a la política institucional de respaldo. - Establecer una programación técnica de verificación de respaldos mediante restauraciones de prueba, al menos una vez al mes, por la unidad responsable de tecnología y seguridad documental. - Mantener una bitácora institucional con trazabilidad de los respaldos realizados, errores detectados y acciones correctivas aplicadas.	- Registro de respaldos documentales. - Log de pruebas de restauración. - Bitácora institucional de respaldo digital.

● Archivo Intermedio (fase semiactiva):

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
2A. Transferencia documental desde Unidades Operativas.	1. La inexistencia de procedimientos definidos para la transferencia de documentos puede generar acumulación innecesaria en unidades operativas, afectando la organización y saturando los espacios de trabajo.	- Aplicar un procedimiento institucional estandarizado para la transferencia de documentos al archivo intermedio, ejecutado conforme a un calendario definido, por quien tenga a cargo la coordinación documental. - Programar la transferencia de documentos mediante un cronograma institucional que indique plazos, volúmenes y unidades responsables, elaborado por la función encargada de la planificación archivística, con el propósito de mantener el flujo regular de descarga documental. - Supervisar cada proceso de transferencia mediante el uso de actas, formularios y registros de entrega-recepción, validados por ambas partes involucradas, con el propósito de asegurar trazabilidad y cumplimiento del procedimiento.	- El procedimiento institucional para las transferencias. - Cronograma de las transferencias. - Actas o formularios de entrega y recepción documental.
	2. La falta de registro formal de los documentos trasladados al archivo intermedio puede dificultar su localización posterior y debilitar la trazabilidad institucional.	- Elaborar un inventario detallado de documentos trasladados, incluyendo datos mínimos como número de documentos, fecha, tipo documental, unidad de origen y volumen, completado por quien tenga a cargo el proceso de transferencia. - Incorporar validación formal del inventario mediante firma de conformidad o verificación por parte de las funciones responsables del envío y la recepción documental, dejando respaldo del acto. - Registrar los antecedentes de la transferencia en un sistema institucional, planilla electrónica o base de datos habilitada para dicho fin, administrada por el área que gestiona el archivo intermedio, con el propósito de facilitar su localización.	- Inventario de todos los documentos transferidos. - Registro de ingreso al archivo intermedio. - Soporte digital o físico del acto de transferencia.
	3. La omisión de criterios técnicos de admisibilidad o condiciones mínimas del material transferido puede implicar el ingreso de documentación incompleta, ilegible o fuera de norma.	- Aplicar una lista de verificación técnica antes de aceptar los documentos en el archivo intermedio, completada por quien tenga a cargo la revisión documental, con el propósito de asegurar que los antecedentes cumplan las condiciones. - Rechazar o devolver formalmente los documentos que no cumplan con los requisitos, dejando constancia escrita para su regularización por la unidad remitente. - Incorporar una etapa de revisión cruzada de los registros de origen, a fin de validar que la documentación coincida con el inventario.	- Lista de verificación documental. - Registro de las observaciones y/o devoluciones. - Informe de revisión técnica o control de admisibilidad.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
2B. Revisión de los Plazos de Conservación.	1. La inexistencia de revisión sistemática de los plazos de conservación establecidos en la TRD puede derivar en la custodia indefinida de documentos sin valor vigente, afectando la eficiencia del archivo institucional.	- Realizar revisiones periódicas de los plazos de conservación conforme a la Tabla de Retención Documental institucional, aplicadas por ejemplo semestral o anualmente, por quien tenga a cargo la gestión del archivo intermedio, con el propósito de identificar documentos que hayan cumplido su vigencia. - Elaborar un listado de documentos susceptibles de disposición final al término de cada período de revisión, con base en las fechas consignadas en el inventario y los criterios definidos en la normativa archivística. - Registrar formalmente los resultados de cada revisión mediante actas, informes técnicos u otro instrumento institucional, resguardado por la unidad responsable del control documental.	- TRD institucional vigente. - Listado de documentos con vencimiento de plazo. - Informe de revisión de plazos de conservación.
	2. La aplicación inconsistente de los plazos definidos en las tablas de retención puede generar decisiones dispares, afectando la coherencia en la disposición final de los documentos.	- Aplicar un protocolo interno que estandarice la revisión de plazos documentales, incluyendo criterios para documentos con fechas irregulares o series sin definición explícita. - Incorporar doble validación de los documentos evaluados, mediante revisión cruzada entre el inventario y la TRD, por funciones distintas dentro del mismo proceso, con el propósito de asegurar coherencia técnica. - Capacitar periódicamente (Ej. anual) al personal involucrado en la revisión de plazos respecto del uso correcto de la TRD y sus actualizaciones, con trazabilidad institucional del cumplimiento.	- Protocolo de revisión de plazos. - Registro de doble validación. - Registro de capacitación técnica aplicada.
	3. La falta de evidencia documentada del proceso de revisión impide acreditar la decisión sobre la permanencia, eliminación o transferencia de los documentos.	- Documentar cada proceso de revisión de plazos mediante informes técnicos que indiquen criterios aplicados, fecha de análisis, unidades afectadas y responsables de la ejecución. - Conservar los antecedentes de revisión junto con el expediente de disposición final, como respaldo en caso de revisiones u observaciones externas. - Incluir la etapa de revisión de plazos como parte del procedimiento institucional de eliminación o transferencia, debidamente formalizado y difundido.	- Informe técnico de revisión de plazos. - Expediente de la disposición final. - Procedimiento institucional validado y vigente.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
2C. Almacenamiento Transitorio.	1. La ausencia de condiciones físicas o digitales adecuadas para la conservación de documentos puede provocar su deterioro, pérdida o daño, comprometiendo su integridad institucional.	- Almacenar los documentos del archivo intermedio en espacios acondicionados según estándares técnicos de conservación (temperatura, humedad, ventilación, mobiliario apropiado), conforme a lo definido por la unidad responsable de custodia documental. - Aplicar medidas de conservación preventiva mediante inspecciones periódicas y registros de mantenimiento, con frecuencia definida en el protocolo institucional. - Utilizar soportes o contenedores adecuados para el resguardo físico (cajas, carpetas, fundas libres de ácido) o respaldos en entornos digitales con sistemas de seguridad activados, definidos por el procedimiento institucional correspondiente.	- Registro de condiciones físicas o ambientales. - Protocolo de conservación preventiva. - Informe de inspección o mantenimiento archivística.
	2. La falta de mecanismos de localización puede dificultar la recuperación eficiente de los documentos bajo custodia, afectando su uso administrativo o fiscalización posterior.	- Registrar la ubicación exacta de los documentos almacenados en inventarios que incluyan datos de caja, estante, sala o carpeta, actualizados por la función encargada del archivo intermedio. - Implementar sistemas de codificación o señalética interna que permitan identificar fácilmente la documentación según series, fechas o unidades de origen. - Revisar periódicamente la consistencia entre el inventario y la ubicación física o digital, mediante cotejo aleatorio, con trazabilidad del control realizado.	- Inventario físico o digital actualizado. - Sistema de codificación de ubicación. - Informe de revisión de consistencia de las ubicaciones.
	3. El acceso no autorizado a documentos en almacenamiento transitorio puede generar filtraciones, manipulación indebida o pérdida de información.	- Restringir el acceso a los espacios de archivo intermedio mediante controles físicos (llaves, cerraduras, registro de ingreso) o digitales (perfiles, claves, roles asignados), definidos por la política de seguridad institucional. - Registrar cada ingreso o consulta en bitácoras oficiales, indicando persona, fecha, motivo y unidad solicitante, conforme a los lineamientos internos. - Revisar periódicamente (Ej. semestral) los registros de acceso para detectar ingresos no autorizados o anomalías, por la función encargada del resguardo documental.	- Registro de ingreso o consulta. - Política de acceso restringido. - Informe de revisión de acceso.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
2D. Control del Acceso Físico o Digital.	1. La ausencia de restricciones formales de acceso a documentos almacenados en archivo intermedio puede exponer información sensible o institucional a usos indebidos o no autorizados.	- Establecer niveles de acceso diferenciados a la documentación almacenada en función de su nivel de confidencialidad o sensibilidad, conforme a lo definido en la política institucional de gestión documental. - Asignar credenciales de ingreso o permisos de consulta únicamente al personal autorizado, conforme a los perfiles establecidos y validados por la función encargada de la custodia documental. - Implementar mecanismos físicos y/o digitales de restricción (cerraduras, claves, permisos de lectura) que se actualicen de forma periódica y mantengan registro de modificaciones.	- Política de niveles de acceso. - Registro de asignación de permisos. - Bitácora de controles físicos y digitales aplicados.
	2. La inexistencia de registro de acceso a la documentación puede impedir verificar responsabilidades en caso de pérdida, filtración o uso inapropiado.	- Registrar cada solicitud de acceso, consulta o préstamo mediante bitácoras institucionales, físicas o digitales, incluyendo usuario, fecha, unidad solicitante y motivo. - Validar todas las solicitudes de acceso mediante autorización expresa, de acuerdo con el procedimiento interno vigente. - Revisar periódicamente (Ej. trimestral) los registros de acceso para verificar su consistencia y detectar anomalías, dejando constancia escrita de las observaciones y medidas adoptadas.	- Bitácora de acceso y préstamo. - Formulario de autorización de consulta. - Informe de revisión de registros de acceso.
	3. La falta de control sobre accesos remotos a documentos digitalizados en archivo intermedio puede facilitar vulneraciones de seguridad o filtraciones de información institucional.	- Configurar perfiles de usuario diferenciados en las plataformas de almacenamiento digital, limitando accesos según criterios definidos en el protocolo institucional de resguardo documental. - Activar sistemas de registro de actividad (log) que permitan revisar accesos remotos por usuario, documento y fecha. - Revisar periódicamente (Ej. mensual) los logs de acceso para detectar patrones anómalos o intentos no autorizados, y activar alertas o bloqueos preventivos conforme a las políticas de seguridad de la información.	- Registro de perfiles habilitados. - Log de actividad en plataforma digital. - Informe de monitoreo de accesos remotos.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
2E. Evaluación Documental para la Disposición Final.	1. La inexistencia de procedimientos para evaluar el destino final de los documentos puede generar demoras innecesarias en su eliminación o conservación, afectando la eficiencia del archivo institucional.	- Aplicar un procedimiento formal que establezca las etapas, responsables y criterios técnicos para la evaluación del destino final de los documentos en archivo intermedio, conforme a lo dispuesto en la normativa interna y las orientaciones del Archivo Nacional. - Programar evaluaciones documentales por ejemplo con frecuencia semestral o anual, priorizando las series que han cumplido su plazo de conservación, por la función encargada de la gestión archivística. - Registrar sistemáticamente cada proceso de evaluación mediante actas, formularios o informes técnicos que den cuenta del análisis realizado.	- Procedimiento de evaluación documental institucional. - Cronograma de las evaluaciones programadas. - Informe técnico o acta de evaluación documental.
	2. La ausencia de criterios claros para determinar la eliminación o transferencia definitiva puede dar lugar a decisiones erróneas o arbitrarias, afectando la trazabilidad institucional.	- Aplicar matrices de valoración documental previamente validadas por la unidad competente, que contemplen criterios legales, administrativos, fiscales e históricos. - Validar las decisiones de disposición final mediante revisión técnica conjunta entre quienes gestionan el archivo intermedio y quienes definen la política institucional de resguardo. - Documentar los criterios aplicados a cada caso en los expedientes de eliminación o transferencia, resguardando trazabilidad normativa y técnica.	- Matriz de valoración documental aplicada. - Acta de validación técnica. - Expediente de disposición final con criterios de respaldo.
	3. La evaluación de documentos sin verificar su vinculación con procesos activos o requerimientos legales puede derivar en eliminaciones indebidas o pérdida de evidencia institucional.	- Cruzar los documentos evaluados con registros administrativos vigentes, sistemas transaccionales o bases de datos institucionales, para verificar que no estén involucrados en procesos activos o trámites pendientes. - Solicitar validación formal a las unidades generadoras antes de incorporar documentos a listados de disposición final, dejando constancia escrita del pronunciamiento. - Suspender del proceso de disposición aquellos documentos que presenten dudas razonables sobre su vigencia o relevancia, a la espera de confirmación técnica o jurídica.	- Registro de validación cruzada con sistemas administrativos. - Oficio de validación emitido por unidad generadora. - Lista de documentos excluidos por dudas de vigencia.

● Archivo Histórico (fase inactiva):

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
3A. Valoración Patrimonial.	1. La ausencia de criterios técnicos para determinar el valor patrimonial de los documentos puede derivar en la eliminación de antecedentes con valor histórico o institucional.	- Aplicar pautas de valoración documental aprobadas institucionalmente, mediante la revisión técnica de criterios históricos, jurídicos y administrativos, por la función encargada de la gestión archivística, cada vez que se planifique un proceso de disposición final, con el propósito de asegurar la conservación de documentos con valor patrimonial. - Validar las decisiones de conservación permanente mediante la elaboración de informes técnicos que incluyan justificación normativa y fundamentos archivísticos, por quien tenga a cargo la evaluación patrimonial, antes de autorizar cualquier eliminación. - Registrar formalmente cada documento valorado como patrimonial en un inventario institucional permanente, con identificación de origen, fecha y criterio aplicado, para asegurar trazabilidad y control posterior.	- Pauta institucional de valoración documental. - Informe técnico de valoración. - Inventario de los documentos patrimoniales.
	2. La falta de trazabilidad en las decisiones sobre conservación permanente puede afectar la legitimidad del proceso y dificultar revisiones o consultas posteriores.	- Incorporar en cada expediente de disposición final una ficha de valoración patrimonial que registre el análisis efectuado, los participantes del proceso y la decisión adoptada, elaborada por la unidad responsable de la custodia histórica. - Consolidar los antecedentes de valoración en un expediente archivístico institucional, organizado cronológicamente y con respaldo físico o digital, para asegurar su disponibilidad ante fiscalizaciones. - Revisar periódicamente (Ej. semestral) la consistencia entre los documentos conservados y sus respectivos respaldos de valoración mediante un cotejo cruzado, por la función encargada del archivo histórico, con el propósito de validar el cumplimiento de criterios técnicos.	- Ficha de valoración documental por expediente. - Expediente institucional del archivo histórico. - Informe de revisión de consistencia documental.
	3. La omisión de participación técnica especializada en el proceso de valoración puede conducir a decisiones erróneas o no fundamentadas.	- Designar formalmente a los participantes del proceso de valoración patrimonial, con acto administrativo o resolución interna. - Realizar sesiones de valoración con participación colegiada de distintas funciones técnicas, documentadas, para fortalecer la objetividad del proceso. - Capacitar periódicamente (Ej. anual) al personal involucrado en valoración patrimonial sobre normativa vigente, criterios de conservación y orientaciones del Archivo Nacional, dejando constancia.	- Resolución de designación técnica. - Actas de sesiones de valoración. - Registro de las capacitaciones técnicas archivísticas.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
3.B Transferencia Definitiva.	1. La inexistencia de un procedimiento formal de transferencia puede generar pérdida de documentos patrimoniales o debilitar la trazabilidad del proceso.	- Aplicar un procedimiento institucional formalizado para la transferencia definitiva de documentos patrimoniales, ejecutado por la función encargada del archivo histórico, cada vez que se concluya un proceso de valoración, con el propósito de asegurar trazabilidad, resguardo y legalidad. - Registrar cada transferencia mediante actas, listados y formularios normalizados que incluyan detalle de los documentos, volúmenes, fechas, unidades de origen y destino, firmados por las partes intervinientes. - Verificar la consistencia entre los documentos transferidos y el inventario institucional antes de autorizar el traslado, mediante revisión cruzada realizada por quien tenga a cargo la custodia histórica.	- Procedimiento de transferencia definitiva. - Acta de entrega y recepción. - Inventario validado de documentos transferidos.
	2. La falta de respaldo documental sobre la transferencia puede dificultar la acreditación del acto ante evaluaciones, revisiones, observaciones externas o requerimientos judiciales.	- Conservar copias físicas y/o digitales de todas las actas de transferencia firmadas, en el expediente institucional del archivo histórico, con el propósito de asegurar trazabilidad del proceso. - Incorporar un registro centralizado de transferencias realizadas, actualizado periódicamente (Ej. semestral) por el área que administra el archivo histórico, para consulta interna y control documental. - Adjuntar copia del inventario de transferencia y de la resolución o acto administrativo que aprueba la operación en los sistemas oficiales de gestión documental institucional.	- Expediente consolidado de todas las transferencias. - Registro centralizado de los actos de transferencia. - Resolución de aprobación con anexos.
	3. El traslado físico o digital de documentos sin condiciones técnicas adecuadas puede generar daños, pérdida de información o comprometer su integridad.	- Embalar los documentos que serán transferidos utilizando materiales de conservación archivística y según protocolos establecidos por la función técnica responsable, previo al traslado. - Documentar cualquier alteración, deterioro o inconsistencia detectada durante el proceso de traslado mediante acta de observaciones firmada al momento de la recepción. - Ejecutar el proceso de transferencia en horarios programados y mediante medios físicos o digitales controlados, bajo supervisión de la función que administra el archivo histórico, con el propósito de garantizar la integridad del material.	- Protocolo de embalaje y traslado. - Acta de observaciones del proceso de entrega. - Registro de ejecución del traslado con validación institucional.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
3.C Conservación Especializada	1. La falta de condiciones técnicas de preservación puede provocar deterioro físico, pérdida o ilegibilidad de los documentos conservados de forma permanente.	- Mantener los documentos en espacios acondicionados con control ambiental (temperatura, humedad y luz), verificado periódicamente (Ej. trimestral) por quien tenga a cargo la custodia del archivo histórico, con el propósito de asegurar su integridad física. - Aplicar inspecciones periódicas a los documentos patrimoniales para detectar signos de deterioro o riesgo, registradas mediante listas de verificación archivística. - Implementar planes de mantenimiento preventivo de estanterías, mobiliario y materiales de resguardo, con frecuencia anual, bajo supervisión técnica.	- Informe de inspección ambiental. - Lista de verificación de condiciones físicas. - Plan anual de mantenimiento de los archivos.
	2. La inexistencia de acciones de digitalización preventiva puede dificultar la preservación de contenidos ante deterioro natural o emergencias.	- Digitalizar progresivamente los documentos patrimoniales más expuestos a deterioro o manipulación, conforme a estándares definidos por el Archivo Nacional y bajo la supervisión de la función responsable del archivo histórico. - Registrar cada proceso de digitalización mediante bitácoras que incluyan fecha, tipo documental, parámetros técnicos aplicados y responsable del procedimiento. - Revisar periódicamente (Ej. anual) el avance del plan de digitalización preventiva y actualizar prioridades en función de estado físico, demanda de acceso o antigüedad del soporte.	- Registro de documentos digitalizados. - Bitácora técnica del proceso. - Plan anual de digitalización preventiva.
	3. La falta de tratamiento especializado para documentos frágiles o en riesgo puede ocasionar su pérdida total o inutilización como evidencia histórica.	- Evaluar el estado de conservación de los documentos frágiles mediante diagnósticos técnicos elaborados por personal capacitado, cada vez que se detecte un caso crítico. - Ejecutar acciones de restauración o estabilización documental según prioridad técnica y disponibilidad presupuestaria, con registro del procedimiento aplicado. - Establecer protocolos de manejo y consulta restringida para documentos en condición crítica, supervisados por la función técnica correspondiente, con el propósito de prevenir su deterioro adicional.	- Informe de diagnóstico de estado físico. - Registro de restauración documental. - Protocolo de manejo de documentos frágiles.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
3.D Regulación del Acceso.	1. La ausencia de políticas claras sobre acceso a documentos históricos puede generar uso indebido de información o conflictos con normas de transparencia o protección de datos.	- Establecer una política institucional de acceso al archivo histórico que distinga entre documentos públicos, reservados o confidenciales, conforme a la Ley N° 20.285 y la Ley N° 19.628, revisada anualmente por la función responsable del resguardo documental. - Publicar en medios oficiales (sitio web o intranet) las condiciones, procedimientos y restricciones aplicables al acceso de documentos históricos, asegurando transparencia institucional. - Actualizar la clasificación de los documentos conforme a nuevas disposiciones legales o vencimiento de plazos de reserva, bajo responsabilidad de quien tenga a cargo el control de acceso archivístico.	- Política institucional de acceso a archivos. - Registro de difusión normativa. - Listado actualizado de documentos con reserva o confidencialidad.
	2. El acceso no controlado a documentación histórica puede derivar en pérdida, manipulación indebida o uso no autorizado de antecedentes.	- Registrar cada solicitud de acceso a documentos históricos mediante formularios normalizados que incluyan identidad, propósito y material consultado, bajo custodia de la función que administra el archivo. - Supervisar presencialmente o de forma remota las consultas realizadas a documentos en soporte físico o digital, cuando el nivel de sensibilidad lo requiera, según protocolo institucional. - Autorizar el acceso únicamente a través de validación previa por parte de la función que administra el archivo, conforme a los criterios establecidos en la política de acceso institucional.	- Formulario de solicitud de acceso. - Registro de supervisión de consulta. - Acta o validación de autorización de acceso.
	3. La inexistencia de procedimientos para atender solicitudes ciudadanas o académicas puede afectar la transparencia activa y debilitar la función pública del archivo.	- Establecer un procedimiento interno para atención de solicitudes externas de acceso a documentos históricos, que contemple plazos, medios de respuesta y validación jurídica si corresponde. - Registrar todas las solicitudes y respuestas emitidas en una bitácora institucional de acceso público o controlado, administrada por la unidad responsable. - Coordinar con el área jurídica o de transparencia el tratamiento de solicitudes complejas, asegurando el cumplimiento normativo antes de emitir respuesta.	- Procedimiento de atención de solicitudes de acceso. - Bitácora de ingresos y respuestas. - Registro de consultas derivadas a asesoría jurídica.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
3.E Uso para fines de Memoria Institucional.	1. La falta de difusión del patrimonio documental puede limitar su uso en investigaciones, rendición de cuentas o fortalecimiento de la identidad institucional.	- Promover periódicamente (Ej. anual) la utilización del archivo histórico mediante actividades de difusión institucional como exposiciones, jornadas temáticas o publicaciones, organizadas por la función encargada del resguardo patrimonial. - Identificar series documentales de alto valor histórico o testimonial que puedan ser publicadas, resguardando los criterios de transparencia, protección de datos y legalidad. - Generar productos de divulgación como boletines, cápsulas digitales o informes temáticos sobre el contenido y relevancia de los fondos históricos conservados.	- Plan anual de difusión del archivo histórico. - Registro de actividades de memoria institucional. - Materiales de divulgación (boletines, catálogos, exposiciones).
	2. El uso no orientado o no autorizado de documentos históricos puede desvirtuar su contenido o afectar su valor como evidencia institucional.	- Elaborar directrices para el uso responsable de documentos históricos por parte de unidades internas o externas, validadas por el área jurídica o técnica correspondiente. - Solicitar declaración de uso académico, institucional o investigativo a quienes accedan a documentos para reproducción o difusión, con trazabilidad documental. - Registrar y archivar cada producto derivado del uso del archivo histórico institucional, indicando propósito, responsable y fecha de utilización.	- Instructivo para uso responsable de documentos patrimoniales. - Formulario de declaración de uso. - Registro de productos generados desde el archivo histórico.
	3. La ausencia de articulación entre el archivo histórico y otras funciones institucionales puede debilitar su contribución al control interno, transparencia y mejora de procesos.	- Incorporar el uso del archivo histórico en instancias de capacitación, inducción o formación institucional sobre identidad, funciones públicas y transparencia, con actividades organizadas por la unidad competente. - Coordinar con unidades de planificación, control de gestión o comunicaciones el uso del fondo histórico como insumo para evaluaciones o revisiones, memoria institucional o conmemoraciones oficiales. - Evaluar periódicamente (Ej. anual) el impacto de las acciones de uso del archivo histórico mediante informes de actividad, retroalimentación de usuarios y registro de solicitudes recibidas.	- Registro de actividades de formación con uso de archivo histórico. - Actas de coordinación entre las diferentes unidades. - Informe periódico del impacto del uso del archivo como memoria institucional.

4.4.3 Matriz de Análisis de la Eliminación de Documentos

Esta matriz sistematiza los riesgos, controles y documentación de respaldo asociados al proceso de eliminación documental regulada, el cual debe ejecutarse conforme a procedimientos formalizados, criterios técnicos y normativa vigente. La finalidad es asegurar que los documentos eliminados hayan perdido su valor legal, administrativo o patrimonial, sin afectar la trazabilidad ni el cumplimiento de las obligaciones institucionales.

El análisis se organiza en torno a diez etapas operativas, desde la identificación de documentos hasta el resguardo de los antecedentes que respaldan su eliminación. Se identifican riesgos como eliminaciones indebidas, deficiencias en la valoración documental, fallas en la digitalización y ausencia de respaldo legal.

Los controles propuestos buscan garantizar que cada decisión esté jurídicamente fundada, técnicamente validada y adecuadamente documentada, de forma que pueda ser auditada y verificada conforme a los principios de legalidad, probidad y transparencia.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C1. Identificación Documental Sujeta a Eliminación.	1. La falta de revisión sistemática de archivos por parte de las unidades responsables puede generar omisiones en la identificación de documentos eliminables, manteniendo en custodia información que ha perdido su valor administrativo o legal.	- Revisar periódicamente los archivos gestionados por cada unidad para identificar documentos que hayan cumplido su ciclo de vida útil, conforme a lo establecido en la TRD institucional, por la función encargada de la administración documental, con el propósito de optimizar el volumen documental en custodia. - Aplicar listados de verificación de plazos de conservación y estado del documento en cada revisión programada, elaborados por quien tenga a cargo la coordinación archivística, a fin de facilitar la identificación oportuna. - Consolidar los resultados de cada revisión en un listado preliminar de documentos a evaluar, validado por la unidad generadora correspondiente, para asegurar su trazabilidad y análisis posterior.	- Registro de revisión periódica de archivos. - Listado preliminar de documentos identificados. - Instructivo institucional de descarte documental.
	2. La inexistencia de criterios técnicos claros para determinar la antigüedad y relevancia de los documentos incrementa el riesgo de decisiones erradas sobre su eliminación o conservación.	- Aplicar criterios de análisis documental previamente definidos por la unidad de archivo institucional, con base en normativa del Archivo Nacional, cada vez que se identifique un grupo documental susceptible de descarte, con el propósito de asegurar una decisión fundamentada. - Capacitar al personal responsable de la identificación documental sobre los criterios de evaluación y aplicación de la TRD, al menos una vez al año, para asegurar comprensión técnica uniforme. - Supervisar de forma aleatoria los procesos de identificación realizados por las unidades operativas mediante revisión técnica efectuada por la función encargada del resguardo documental, con el propósito de prevenir errores críticos.	- Manual de criterios técnicos de descarte. - Registro de la capacitación archivística aplicada. - Informe de supervisión técnica de identificación documental.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C1. Identificación Documental Sujeta a Eliminación.	3. La inclusión de documentos aún vigentes o con trámites activos en los listados preliminares de descarte podría derivar en eliminaciones indebidas que comprometan la gestión institucional o la atención de requerimientos legales.	- Verificar que los documentos incluidos en los listados preliminares no estén vinculados a trámites activos, mediante revisión cruzada con los sistemas administrativos o registros institucionales, realizada por la unidad generadora y validada por la función archivística. - Excluir de forma preventiva cualquier documento cuya vigencia legal o administrativa no haya sido confirmada con certeza, dejando constancia en el expediente respectivo. - Requerir pronunciamiento formal de las unidades operativas antes de consolidar los listados finales de descarte documental, como condición previa de valoración o eliminación.	- Acta de validación de vigencia documental. - Registro de exclusión por trámites activos. - El oficio del pronunciamiento de la unidad generadora.
C2. Revisión de Requisitos de Conservación.	1. El desconocimiento de normativas sectoriales o disposiciones específicas de organismos fiscalizadores podría derivar en el descarte de documentos relevantes para revisiones, fiscalizaciones o procesos judiciales.	- Contrastar cada listado de documentos identificados para descarte con la normativa sectorial vigente y con las exigencias definidas por órganos fiscalizadores, mediante revisión documental efectuada por la función responsable del análisis normativo, antes de autorizar su eliminación, con el propósito de asegurar su legalidad. - Incorporar como parte obligatoria del proceso de eliminación una revisión cruzada con leyes especiales, decretos o reglamentos institucionales que definan plazos mínimos de conservación, según orientación de la unidad jurídica o de cumplimiento normativo. - Registrar formalmente el resultado de la revisión legal en informes técnicos o matrices de cumplimiento, anexadas al expediente de eliminación documental, para resguardar la trazabilidad del análisis.	- Informe jurídico o normativo de respaldo. - Matriz de revisión de las normativas aplicadas. - Registro consolidado de disposiciones especiales de conservación.
	2. La falta de documentación que respalde la revisión de requisitos de conservación limita la trazabilidad del proceso y dificulta la defensa institucional ante eventuales observaciones o requerimientos.	- Documentar cada proceso de revisión de requisitos normativos mediante actas, informes técnicos o formularios, firmados por quien tenga a cargo la validación archivística. - Archivar todos los documentos de respaldo utilizados en el análisis normativo (copias de leyes, circulares, dictámenes), en conjunto con los expedientes de eliminación, para asegurar disponibilidad ante fiscalización posterior. - Incluir una lista de verificación documental específica sobre requisitos de conservación legal como parte obligatoria del expediente de descarte, supervisada por la unidad de archivo.	- Acta de revisión de requisitos legales. - Lista de verificación de conservación normativa. - Expediente de respaldo normativo consolidado.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C2. Revisión de Requisitos de Conservación.	3. La ausencia de evaluación ante dudas razonables sobre requisitos legales o de conservación incrementa el riesgo de eliminar documentos que posteriormente sean requeridos como evidencia administrativa o legal.	- Suspender del proceso de eliminación aquellos documentos que presenten dudas razonables sobre su vigencia legal o valor institucional, dejando constancia en acta de observación, elaborada por quien administre el archivo institucional. - Requerir evaluación jurídica o pronunciamiento formal de la unidad de cumplimiento antes de proceder con la eliminación de documentos cuya condición normativa no esté claramente resuelta. - Establecer en el procedimiento institucional el principio de precaución como criterio obligatorio ante dudas técnicas o legales sobre la eliminación, con validación de la unidad correspondiente.	- Acta de observaciones por dudas normativas. - Oficio del pronunciamiento legal solicitado. - Un procedimiento institucional con una cláusula de precaución documental.
C3. Valoración Documental.	1. La aplicación inconsistente de los criterios técnicos definidos para la valoración documental puede generar decisiones dispares sobre la eliminación o conservación, afectando la coherencia en la gestión de archivos institucionales.	- Aplicar criterios técnicos homogéneos establecidos en una pauta de valoración institucional validada por la unidad de archivo, cada vez que se realice un proceso de eliminación documental, con el propósito de asegurar decisiones coherentes y fundadas. - Revisar los criterios aplicados en procesos anteriores mediante informes de valoración previamente registrados, como insumo para asegurar consistencia de manera regular, bajo responsabilidad de quien gestiona el archivo intermedio. - Validar cada decisión de eliminación mediante una sesión técnica documentada con participación de las funciones responsables del archivo, valoración y cumplimiento normativo.	- Pauta técnica para la valoración documental vigente. - Registro de sesiones de validación. - Informe de criterios aplicados por serie documental.
	2. La inexistencia de registros formales que respalden el proceso de valoración dificulta la trazabilidad y justificación de las decisiones adoptadas ante instancias de fiscalización o revisión.	- Elaborar un expediente de valoración por cada proceso de eliminación, que contenga actas, formularios y matriz de decisión aplicada, bajo custodia de la unidad responsable de la conservación o disposición documental. - Registrar formalmente a los participantes y sus respectivos roles en el proceso de valoración, dejando constancia mediante firma en el acta o instrumento equivalente. - Digitalizar todos los registros de valoración documental y vincularlos al expediente de eliminación correspondiente, para asegurar su disponibilidad en plataformas institucionales.	- Expediente de valoración documental consolidado. - Acta firmada de valoración técnica. - Registro digital de respaldo archivístico.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C3. Valoración Documental.	3. La falta de articulación entre los criterios institucionales y las orientaciones del Archivo Nacional incrementa el riesgo de incumplimientos normativos o discrepancias en la aplicación de políticas archivísticas.	- Revisar periódicamente (Ej. anual) la coherencia entre la pauta institucional de valoración documental y las directrices vigentes del Archivo Nacional, bajo responsabilidad de la unidad de archivo o función especializada. - Incorporar en cada proceso de valoración una cláusula de conformidad técnica con la normativa externa aplicable, documentada mediante referencia explícita en el informe final. - Solicitar acompañamiento técnico al Archivo Nacional en casos de duda sobre la aplicabilidad de criterios específicos, dejando constancia formal del intercambio.	- Informe de revisión normativa periódica. - Matriz de valoración con cláusulas de conformidad. - Registro de consultas al Archivo Nacional.
C4. Revisión del Formato o Soporte.	1. La falta de distinción entre documentos físicos, digitalizados y nativos digitales incrementa el riesgo de aplicar procedimientos inadecuados de eliminación, lo que puede generar incumplimientos normativos.	- Clasificar los documentos según su soporte, físico, digitalizado o digital nativo, mediante una ficha técnica elaborada por la función encargada de la gestión documental, antes de iniciar cualquier procedimiento de eliminación, con el propósito de aplicar medidas diferenciadas según tipo de respaldo. - Incorporar una etapa obligatoria de revisión de formato en cada proceso de eliminación documental, registrada en acta y validada por la unidad técnica correspondiente, para asegurar su trazabilidad. - Actualizar periódicamente (Ej. anual) el protocolo institucional de revisión de soportes documentales, incluyendo orientaciones técnicas y legales conforme a normativa vigente.	- Ficha de soporte documental por serie. - Acta de revisión de los formatos. - Protocolo institucional de clasificación por tipo de soporte.
	2. La eliminación de documentos digitales nativos sin respaldo normativo puede generar observaciones por parte de órganos de control o pérdida de información institucional.	- Verificar que los documentos digitales nativos no sean eliminados sin contar con una autorización expresa o respaldo normativo específico, mediante revisión documental por parte de quien tenga a cargo la función de resguardo digital. - Registrar formalmente las resoluciones u orientaciones legales que habilitan o restringen la eliminación de documentos electrónicos, vinculándolas al expediente de eliminación. - Suspender cualquier procedimiento de eliminación de documentos digitales nativos en caso de ausencia de respaldo legal claro, aplicando el principio de precaución documental.	- Registro de las autorizaciones legales aplicables. - Informe técnico-jurídico de habilitación. - Acta de suspensión por falta de respaldo normativo.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C4. Revisión del Formato o Soporte.	3. La utilización de procedimientos homogéneos para soportes con exigencias técnicas distintas puede comprometer la integridad de los documentos o su valor probatorio.	- Aplicar protocolos diferenciados de eliminación para cada tipo de soporte documental, validados por la función técnica correspondiente, con base en estándares institucionales y recomendaciones del Archivo Nacional. - Realizar capacitación técnica periódicamente (Ej. anual) para el personal involucrado en eliminación documental sobre procedimientos específicos por tipo de soporte. - Supervisar cada ejecución de eliminación conforme al tipo de formato involucrado, dejando constancia del método aplicado y soporte tratado, en acta firmada por personal autorizado.	- Protocolo de eliminación por tipo de soporte. - Registro de las capacitaciones técnicas aplicadas. - Acta de ejecución diferenciada del procedimiento.
C5. Digitalización.	1. La ejecución del proceso de digitalización sin cumplir con los estándares técnicos establecidos puede comprometer la fidelidad del contenido y afectar la validez del documento digital como respaldo legal o administrativo.	- Ejecutar cada proceso de digitalización conforme a los estándares técnicos definidos por la Ley N° 18.845 y las orientaciones del Archivo Nacional, mediante la utilización de equipos certificados y parámetros de calidad controlada, bajo responsabilidad de la función técnica correspondiente. - Verificar la calidad de la imagen digital obtenida mediante revisión aleatoria por muestreo, dejando constancia del resultado y de las medidas correctivas aplicadas, cuando corresponda. - Documentar en bitácora técnica cada digitalización realizada, indicando tipo documental, parámetros utilizados, fecha y responsable, con el propósito de asegurar trazabilidad del respaldo.	- Protocolo técnico de digitalización. - Registro de revisión de calidad. - Bitácora institucional del proceso digital.
	2. La omisión en el registro de información clave del proceso de digitalización (como fecha, formato o responsable) limita la trazabilidad del procedimiento y dificulta su verificación posterior ante revisiones o fiscalizaciones.	- Registrar sistemáticamente los datos esenciales de cada proceso de digitalización en una planilla o módulo del sistema institucional, incluyendo fecha, tipo documental, formato de salida, software utilizado y responsable directo del escaneo. - Conservar en expediente digital o físico los reportes técnicos generados por el software de digitalización, incluyendo metadatos de origen y certificados de integridad si correspondiere - Verificar que cada documento digitalizado se encuentre correctamente identificado y vinculado al expediente de eliminación respectivo, antes de autorizar el procedimiento de destrucción física.	- Planilla de digitalización completa. - Registro técnico de parámetros aplicados. - Acta de verificación de correspondencia entre copia digital y documento original.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C5. Digitalización.	3. La utilización de equipos o formatos no adecuados para la digitalización puede generar copias de baja calidad o ilegibles, afectando la integridad del documento y su valor como evidencia institucional.	- Mantener actualizada una lista de equipos y software autorizados para la digitalización institucional, controlada por la unidad responsable de gestión documental o tecnología - Ejecutar pruebas técnicas periódicas de calibración y mantenimiento a los dispositivos de escaneo, dejando constancia en bitácoras de servicio o fichas de mantenimiento. - Excluir del proceso de digitalización aquellos documentos que por su condición física o complejidad técnica requieran tratamiento especial, hasta que cuenten con condiciones adecuadas de reproducción segura.	- Registro de equipos autorizados. - Bitácora de mantenimiento técnico. - Informe de exclusión de documentos críticos o deteriorados.
C6. Registro y Respaldo del Documento Digital.	1. La ausencia de respaldos periódicos del archivo digital puede derivar en la pérdida total o parcial de la información en caso de fallas técnicas o eventos críticos.	- Ejecutar respaldos periódicos de los documentos digitalizados mediante rutinas programadas y sistemas automatizados, configurados por la función responsable de tecnologías de la información, con el propósito de asegurar la recuperación de los archivos ante contingencias. - Verificar periódicamente (Ej. semestral) el correcto funcionamiento de los sistemas de respaldo, mediante revisión de logs, alertas y reportes automáticos, bajo supervisión de la función encargada del soporte documental digital. - Almacenar los respaldos en ubicaciones seguras, separadas del entorno principal de operación, conforme a lo definido en la política institucional de continuidad operativa.	- Registro de respaldo programado. - Bitácora de monitoreo de respaldo. - Plan de continuidad tecnológica institucional.
	2. El almacenamiento de documentos digitales sin controles de acceso adecuados expone la información a vulneraciones de seguridad y posibles filtraciones.	- Configurar perfiles de usuario diferenciados en los sistemas de gestión documental, asignando privilegios de acceso según funciones y niveles de responsabilidad, por la función encargada del sistema de resguardo digital. - Registrar automáticamente cada ingreso, modificación o descarga de documentos mediante logs de revisión que permitan trazabilidad en tiempo real. - Revisar periódicamente (Ej. mensual) los perfiles de acceso vigentes y eliminar cuentas inactivas o innecesarias, con validación por la unidad responsable de la custodia documental digital.	- Reporte de configuración de perfiles de usuario. - Log de acceso a los documentos digitales. - Acta de revisión periódica de los permisos activos.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C6. Registro y Respaldo del Documento Digital.	3. La falta de trazabilidad respecto de los documentos incorporados a sistemas digitales limita la capacidad institucional para auditar procesos o responder a requerimientos de información.	- Registrar en cada carga de documento digital metadatos obligatorios como fecha de incorporación, nombre del responsable, unidad de origen, tipo documental y código de serie, conforme a protocolo institucional definido por la unidad de archivo. - Vincular digitalmente cada documento escaneado al expediente electrónico al que pertenece, asegurando su correcta localización y contexto dentro del sistema. - Validar periódicamente (Ej. mensual) una muestra aleatoria de documentos digitalizados para una verificación la correspondencia entre el archivo, los metadatos y el expediente institucional.	- Registro de carga documental con metadatos. - Protocolo de vinculación de documentos al expediente. - Informe de revisión cruzada entre metadatos y archivo.
C7. Resolución de Autorización para la Eliminación.	1. La omisión en la emisión de una resolución formal que autorice la eliminación de documentos puede invalidar el procedimiento y generar observaciones por parte de organismos fiscalizadores.	- Emitir una resolución administrativa formal y numerada que autorice la eliminación de documentos, elaborada por la función responsable de la gestión documental, previa validación jurídica y técnica, con el propósito de garantizar el respaldo institucional del acto. - Revisar que la resolución cuente con los antecedentes técnicos necesarios, incluyendo informe de valoración, listado de documentos y criterios normativos aplicados, antes de ser firmada por la autoridad competente. - Registrar digitalmente cada resolución emitida en el sistema institucional oficial, bajo resguardo de la unidad de archivo, asegurando su trazabilidad futura.	- Resolución formal de autorización. - Informe técnico de respaldo. - Registro digital de resoluciones emitidas.
	2. La falta de fundamentos o detalle en el contenido de la resolución dificulta la identificación precisa de los documentos eliminados y limita la trazabilidad del proceso.	- Incluir en la resolución el detalle técnico que identifique con precisión los documentos a eliminar, especificando serie documental, rango temporal, volumen, unidad de origen y tipo de soporte. - Validar el contenido de la resolución mediante cotejo con el inventario de documentos propuestos para eliminación, efectuado por quien tenga a cargo la coordinación archivística. - Adjuntar como anexo obligatorio a la resolución el listado completo de documentos eliminables, firmado por la unidad técnica responsable.	- Resolución con anexo detallado. - Inventario validado de documentos - Acta de validación técnica del contenido.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C7. Resolución de Autorización para la Eliminación.	3. La ausencia de firma o validación por parte de la autoridad competente puede dejar sin efecto el acto administrativo y comprometer la legalidad del procedimiento de eliminación.	- Verificar que la resolución de autorización cuente con firma de la autoridad institucional facultada conforme al reglamento interno, mediante control previo de legalidad efectuado por la función de apoyo jurídico o administrativo. - Establecer como parte del procedimiento formal de eliminación un punto de control de firmas válidas, antes de ejecutar cualquier acción sobre los documentos. - Conservar copia firmada de la resolución en el expediente físico y digital de eliminación, bajo resguardo de la unidad de archivo o quien ejerza dicha función.	- Resolución firmada por autoridad competente - Registro de validación de firmas. - Copia archivada en expediente documental.
C8. Acta para la Eliminación.	1. La omisión de algún aspecto en el acta formal que dé cuenta de la eliminación de documentos puede dificultar la acreditación del procedimiento ante evaluaciones o revisiones posteriores.	- Elaborar el acta de eliminación utilizando un formato institucional estandarizado que asegure la inclusión de todos los elementos requeridos, inmediatamente después de ejecutada la destrucción, por la función responsable del proceso documental, con el propósito de asegurar trazabilidad y respaldo. - Completar el acta en el mismo lugar donde se realizó la eliminación, incluyendo los datos esenciales del procedimiento (fecha, volumen, método y documentos intervenidos), validado por los participantes designados. - Incorporar copia del acta en el expediente digital y físico del proceso de eliminación, bajo custodia de quien tenga a cargo el archivo institucional.	- Acta institucional de eliminación - Formulario oficial con campos obligatorios. - Expediente completo con copia del acta.
	2. La ausencia de información esencial en el acta (como fecha, método, volumen o responsables) limita la trazabilidad del proceso y debilita la validez del registro institucional.	- Verificar que el acta contenga todos los campos requeridos antes de su validación final, mediante revisión realizada por la función de gestión documental al cierre del procedimiento. - Establecer como requisito obligatorio la presencia y firma de al menos dos testigos institucionales durante el proceso de eliminación, quienes deberán consignarse en el acta. - Incorporar una sección específica en el acta para observaciones o eventualidades ocurridas durante la ejecución, con validación inmediata por los participantes.	- Formulario institucional con campos críticos. - Registro de la participación de testigos. - Acta firmada con observaciones que han sido documentadas.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C8. Acta para la Eliminación.	3. La falta de firma de los funcionarios participantes en el acto de eliminación podría afectar la validez administrativa del procedimiento y dificultar la verificación de responsabilidades.	- Recolectar las firmas de todos los funcionarios que participaron en el acto de eliminación inmediatamente después de la ejecución, utilizando el formato establecido por la unidad de archivo. - Validar las identidades de los participantes mediante registro de asistencia previo al inicio del procedimiento, verificado por la unidad que coordina la eliminación documental. - Registrar digitalmente la versión escaneada del acta firmada en el expediente oficial del proceso, resguardada en el sistema institucional.	- Acta de eliminación firmada. - Registro de asistencia de participantes. - Copia digital del acta archivada.
C9. Eliminación Física Segura.	1. La utilización de métodos de destrucción que no aseguren la eliminación irreversible del soporte puede permitir la recuperación no autorizada de información, comprometiendo la confidencialidad institucional.	- Aplicar métodos de destrucción que aseguren la eliminación total e irreversible del soporte físico o digital, como trituración, incineración o borrado seguro de datos, conforme al procedimiento institucional, bajo ejecución directa o supervisión de la función responsable del resguardo documental. - Verificar que el método seleccionado sea compatible con la naturaleza del soporte y el nivel de sensibilidad de la información, antes de su ejecución, por quien coordina el proceso de eliminación - Registrar evidencia del método utilizado mediante acta técnica, certificado externo o documentación audiovisual, inmediatamente después del procedimiento.	- Protocolo institucional de eliminación segura. - Acta técnica con descripción del método. - Registro fotográfico o audiovisual (si aplica) del procedimiento.
	2. La ausencia de supervisión durante la ejecución del proceso de destrucción incrementa el riesgo de fallas en la operación o de desviaciones respecto del procedimiento autorizado.	- Supervisar en tiempo real la ejecución del proceso de destrucción documental por un representante institucional designado, quien debe verificar el cumplimiento del método aprobado y registrar el acto en la bitácora correspondiente. - Requerir la presencia de al menos un testigo adicional durante todo el procedimiento, especialmente en actos realizados por proveedores externos - Completar y firmar inmediatamente el informe de supervisión, indicando fecha, responsables, método aplicado y observaciones, por la función encargada del control documental.	- Bitácora de supervisión de destrucción. - Registro de asistencia de funcionarios testigos - Informe de supervisión firmado.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C9. Eliminación Física Segura.	3. La ejecución del proceso por proveedores externos sin verificación institucional podría generar incumplimientos de contrato, pérdidas de trazabilidad o compromisos legales.	- Exigir al proveedor externo la emisión de un certificado de destrucción que describa el método utilizado, fecha, volumen intervenido y medios aplicados, como condición para validar la conformidad del servicio. - Verificar in situ la ejecución del procedimiento por parte de un funcionario institucional, quien debe contrastar lo observado con el contenido del certificado emitido. - Incorporar en el contrato o acuerdo de servicios una cláusula específica sobre responsabilidad, confidencialidad y estándares mínimos exigibles para la eliminación documental.	- Certificado de destrucción emitido por proveedor. - Registro de verificación institucional. - Cláusula contractual sobre eliminación segura.
C10. El Registro Institucional de Eliminación	1. La inexistencia de lineamientos institucionales sobre el resguardo de los registros de eliminación incrementa el riesgo de prácticas no estandarizadas, dificultando la entrega de antecedentes y la verificación posterior.	- Establecer lineamientos institucionales sobre conservación, acceso y custodia del expediente de eliminación, mediante instructivo formal emitido por la función encargada del archivo, inmediatamente después de finalizado cada procedimiento, con el propósito de garantizar trazabilidad y control. - Mantener en un repositorio único y centralizado toda la documentación asociada al proceso de eliminación, en formato físico y digital, bajo responsabilidad de la unidad que administre el SGD. - Verificar periódicamente (Ej. anual) la integridad del expediente documental de eliminación, mediante revisión cruzada entre registros físicos y digitales, realizada por la función encargada del control documental.	- Instructivo institucional de archivo del proceso. - Registro digital del expediente de eliminación. - Acta de revisión periódica del respaldo documental.
	2. La exclusión de documentos clave, como certificados de destrucción o actas firmadas, debilita el respaldo formal del procedimiento y puede dar lugar a observaciones de órganos de control.	- Incorporar como parte obligatoria del expediente de eliminación todos los documentos clave (resolución, acta, certificado, informes técnicos), antes de su archivo definitivo, por la función que coordina el proceso documental. - Establecer una lista de verificación documental obligatoria, utilizada como checklist previo al cierre del expediente, validada por la unidad encargada del archivo. - Registrar digitalmente los documentos clave en orden cronológico y con metadatos asociados, vinculándolos al expediente general del procedimiento.	- Checklist de documentos requeridos. - Expediente con los documentos clave que fueron escaneados. - Registro digital con metadatos institucionales.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
C10. El Registro Institucional de Eliminación.	3. La falta de trazabilidad documental respecto de procesos anteriores limita la posibilidad de acreditar el cumplimiento normativo ante evaluaciones, revisiones internas, solicitudes ciudadanas o fiscalizaciones.	- Numerar y clasificar cada expediente de eliminación con un código único institucional, asignado por quien administre el sistema de archivo, inmediatamente después del cierre del procedimiento. - Registrar en sistema digital el historial completo de procesos de eliminación realizados, con acceso restringido y respaldo automático, bajo control de la unidad técnica correspondiente - Generar informes periódicos (Ej. anual) de consolidación y análisis de procesos de eliminación realizados, elaborados por la función encargada del resguardo documental, con fines de revisión y mejora continua.	- Registro institucional de procesos finalizados. - Código único por expediente de eliminación. - Informe periódico de consolidación y de trazabilidad.

4.4.4 Matriz de Análisis del Resguardo de la información

El resguardo de la información es una función transversal que recorre todo el ciclo de vida documental. Su finalidad es proteger los antecedentes institucionales frente a riesgos de acceso no autorizado, pérdida, deterioro o uso indebido, mediante la aplicación de medidas técnicas, organizacionales y normativas.

La matriz permite identificar, evaluar y mitigar los riesgos asociados a este subproceso, organizados en etapas específicas como clasificación de información sensible, planificación de medidas de protección, continuidad operativa, cumplimiento normativo y prevención de sanciones.

Los controles orientadores propuestos fortalecen la seguridad documental, consolidan el control interno y refuerzan una cultura organizacional basada en la legalidad, la responsabilidad institucional y la protección de la información pública.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D1. Levantamiento y clasificación de información sensible.	1. La falta de criterios estandarizados para la clasificación de la información dificulta la diferenciación entre datos públicos, personales y sensibles, lo que podría generar errores en su protección y tratamiento.	- Aplicar criterios de clasificación definidos institucionalmente para categorizar la información como pública, personal o sensible, cada vez que se registre o revise un documento, por la función encargada de la gestión documental, con el propósito de asegurar un tratamiento adecuado y conforme a la normativa vigente. - Difundir lineamientos de clasificación mediante instructivos operativos validados y capacitar periódicamente al personal involucrado, por la función responsable de resguardo de la información, para reducir errores en el tratamiento. - Verificar periódicamente (Ej. mensual) el cumplimiento de los criterios de clasificación mediante revisión aleatoria de registros, por la unidad encargada de control documental, con el fin de detectar desviaciones y aplicar medidas correctivas.	- Política institucional de clasificación. - Un instructivo técnico validado. - El registro de las capacitaciones realizadas. - Informe de revisión periódica de clasificación.
	2. La inexistencia de un inventario actualizado de los datos almacenados impide conocer el volumen y tipo de información existente, aumentando el riesgo de omisiones en su resguardo y acceso indebido.	- Mantener un inventario actualizado de la información institucional que identifique el tipo de dato, unidad responsable, ubicación y nivel de sensibilidad, actualizado periódicamente (Ej. semestral) por la función que administre el sistema de información institucional, con el propósito de garantizar trazabilidad. - Revisar periódicamente (Ej. anual) la consistencia del inventario mediante evaluaciones internas sobre los registros de información crítica, por la función encargada del control de activos documentales. - Registrar formalmente cada nuevo ingreso de datos institucionales en el inventario, al momento de su incorporación al sistema, por la función que gestiona el ingreso documental.	- Inventario de los datos institucionales clasificados. - Actas de revisión y actualización. - Registro digital de ingresos documentales.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D1. Levantamiento y clasificación de información sensible.	3. El acceso no controlado a información aún no clasificada incrementa el riesgo de exposición o uso indebido de datos sensibles antes de que se implementen las medidas de seguridad correspondientes.	- Restringir el acceso a documentos no clasificados mediante perfiles temporales de acceso o aislamiento digital, por la unidad responsable del sistema de información, desde el momento de la captura documental hasta su categorización definitiva. - Registrar cada intento de acceso a documentación no clasificada mediante bitácoras de actividad digital supervisadas por la función encargada de seguridad de la información. - Evaluar periódicamente (Ej. semanal) los niveles de acceso asignados a usuarios con privilegios administrativos, a fin de prevenir accesos indebidos, bajo responsabilidad de la unidad que administra los sistemas documentales.	- Protocolo de restricción transitoria de acceso. - Bitácora de la trazabilidad de accesos. - Informe de revisión periódica.
D2. Diagnóstico y planificación.	1. La falta de un diagnóstico integral sobre los riesgos en el tratamiento de datos podría impedir la identificación temprana de vulnerabilidades, exponiendo la información a accesos no autorizados o pérdidas.	- Realizar diagnósticos de riesgo sobre el tratamiento de datos institucionales mediante herramientas de análisis técnico, al menos una vez al año o ante la incorporación de nuevos sistemas, por la función encargada de seguridad de la información, con el propósito de identificar vulnerabilidades y establecer acciones preventivas. - Aplicar evaluaciones de impacto en protección de datos personales (EIPDP) conforme a la Ley N° 21.180, durante la fase de diseño o rediseño de procesos, por la función responsable de cumplimiento normativo documental. - Mantener actualizado un registro institucional de los riesgos identificados y sus respectivas medidas de mitigación, bajo resguardo de la unidad que administre la planificación estratégica documental.	- Informe de diagnóstico de seguridad documental. - Evaluación de impacto en protección de datos. - Matriz institucional de riesgos y mitigaciones.
	2. La ausencia de criterios claros para la evaluación y monitoreo de riesgos impide establecer controles efectivos, reduciendo la capacidad de la organización para gestionar incidentes de seguridad.	- Definir y documentar criterios técnicos de evaluación de riesgos para el tratamiento de información institucional, por la función encargada del diseño de políticas de seguridad, con el fin de establecer una línea base de control. - Evaluar periódicamente el cumplimiento de los criterios definidos mediante revisiones internas programadas, ejecutadas por la función encargada del seguimiento de planes de acción. - Incorporar los criterios de evaluación como anexo obligatorio de cada plan de gestión de riesgos institucional, para asegurar coherencia entre diagnóstico, planificación y monitoreo.	- Documento con criterios de evaluación definidos. - Informes de revisión y seguimiento periódico. - Planes de gestión de riesgos que cuenten con anexos normativos.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D2. Diagnóstico y planificación.	3. La falta de procedimientos documentados para la revisión y mejora del diagnóstico de riesgos reduce la posibilidad de generar aprendizajes organizacionales, afectando la evolución de las estrategias de seguridad de la información.	- Documentar el procedimiento institucional para la revisión y actualización del diagnóstico de riesgos de información, con periodicidad anual o posterior a incidentes críticos, por la unidad encargada de gobernanza documental. - Registrar los aprendizajes derivados de cada revisión en informes técnicos consolidados, disponibles para los responsables de la planificación documental institucional. - Incorporar un sistema de retroalimentación continua que permita ajustar las medidas preventivas según los resultados obtenidos en revisiones anteriores, bajo responsabilidad de la función que gestiona los planes de mejora institucional.	- Procedimiento de revisión de diagnósticos. - Informes técnicos de lecciones aprendidas. - Sistema de retroalimentación institucional.
D3. Diseño e implementación de políticas.	1. La falta de un marco normativo claro y actualizado en las políticas de seguridad de la información genera confusión en su aplicación, aumentando el riesgo de incumplimiento normativo y exposición a sanciones.	- Revisar y actualizar las políticas institucionales de seguridad de la información cada vez que existan cambios normativos relevantes o anualmente, por la función encargada de cumplimiento documental, con el propósito de asegurar alineación con la legislación vigente. - Formalizar las políticas mediante resolución institucional y difundirlas al personal mediante canales internos oficiales, por la función responsable de gobernanza de la información. - Verificar periódicamente (Ej. semestral) el cumplimiento de lo dispuesto en las políticas a través de revisiones internas documentadas, por la unidad encargada del control normativo.	- Política institucional vigente firmada por autoridad competente. - Resolución de validación jurídica. - Registro de difusión y capacitación institucional.
	2. Deficiencias en la definición de procedimientos de acceso y almacenamiento de datos pueden permitir accesos indebidos, filtraciones de información o pérdida de datos críticos.	- Definir procedimientos operativos normalizados para el acceso y almacenamiento de datos institucionales, por la función responsable del sistema de resguardo documental, incorporando restricciones por perfil de usuario. - Registrar cada modificación a los procedimientos mediante versiones controladas, bajo custodia de la unidad que administra la documentación normativa interna. - Capacitar periódicamente al personal sobre los procedimientos definidos, especialmente al asumir nuevas funciones, por la función encargada de formación en gestión documental.	- Manuales y/o procedimientos operativos firmados. - Historial de versiones normativas. - Registro de las capacitaciones específicas por unidad.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D3. Diseño e implementación de políticas.	3. La inexistencia de procesos de validación y actualización periódica de las políticas de seguridad puede hacer que las estrategias queden obsoletas frente a nuevas amenazas tecnológicas o regulatorias.	- Establecer un calendario institucional de revisión y actualización de políticas de seguridad, a ser ejecutado periódicamente (Ej. anual) por la función encargada del gobierno de la información. - Validar cada nueva versión de política mediante acta técnica que fundamente los cambios normativos o tecnológicos incorporados, bajo responsabilidad de la unidad técnica correspondiente. - Mantener disponible un repositorio único y actualizado de políticas institucionales vigentes, con acceso restringido según perfil, por quien tenga a cargo la custodia normativa interna.	- Calendario de actualización institucional. - Actas de validación de nuevas versiones. - Repositorio institucional de políticas vigentes de privilegios.
D4. Implementación de medidas de seguridad y continuidad operativa.	1. El no contar con herramientas efectivas de monitoreo en tiempo real limita la capacidad de detección temprana de amenazas, facilitando la materialización de ataques cibernéticos y accesos no autorizados.	- Implementar sistemas de monitoreo en tiempo real para identificar eventos anómalos o accesos indebidos en plataformas institucionales, bajo operación continua de la función encargada de seguridad de la información, con el propósito de anticipar incidentes. - Configurar alertas automáticas ante eventos críticos que comprometan la integridad de los sistemas, activadas por el sistema documental o herramientas asociadas, y gestionadas por la unidad responsable del soporte tecnológico. - Evaluar periódicamente (Ej. semanal) los registros generados por las herramientas de monitoreo, identificando patrones de riesgo, bajo supervisión de la función encargada del análisis de ciberseguridad institucional.	- Reportes de monitoreo automatizado. - Logs de las alertas generadas. - Actas de revisión técnica periódica.
	2. Las deficiencias en la implementación de mecanismos de detección y mitigación de amenazas pueden generar respuestas tardías ante incidentes, permitiendo la propagación de riesgos en la infraestructura tecnológica.	- Activar mecanismos de contención inmediata ante la detección de incidentes críticos mediante protocolos predefinidos, ejecutados por la unidad que administra los sistemas documentales institucionales. - Registrar formalmente cada incidente y su tratamiento en una bitácora técnica, bajo responsabilidad de la función encargada del control de seguridad, para su análisis posterior. - Revisar y actualizar periódicamente (Ej. mensual) los protocolos de mitigación y contención, considerando incidentes recientes y nuevas vulnerabilidades, por la función que gestiona la continuidad operativa institucional.	- Protocolo institucional de respuesta ante incidentes. - Bitácora de incidentes registrados. - Registro de actualización de protocolos.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D4. Implementación de medidas de seguridad y continuidad operativa.	3. La ausencia de una planificación clara para la continuidad operativa expone a la institución a pérdidas de información y tiempos de inactividad prolongados en caso de incidentes críticos.	- Diseñar y mantener actualizado un plan institucional de continuidad operativa que incluya procedimientos de respaldo y recuperación documental, elaborado por la función encargada de gestión de riesgos. - Realizar pruebas de recuperación de información al menos una vez por semestre, en coordinación con las unidades críticas de la institución, para verificar la eficacia del plan. - Documentar los resultados de cada simulacro o ejercicio de recuperación, con identificación de brechas detectadas y acciones correctivas, bajo supervisión de la unidad que coordina la seguridad documental.	- Plan de continuidad operativa validado. - Registro de simulacros y resultados. - Informes técnicos con medidas correctivas.
D5. Monitoreo, revisiones y evaluación de impacto.	1. La falta de indicadores de cumplimiento y monitoreo continuo de la seguridad de la información dificulta la identificación de brechas y debilita la capacidad de respuesta ante vulnerabilidades que se presenten o emergentes.	- Definir y aplicar indicadores de cumplimiento asociados a la seguridad de la información, actualizados periódicamente (Ej. mensual) por la función encargada del monitoreo documental, con el propósito de detectar desviaciones y prevenir riesgos. - Consolidar los resultados de los indicadores en reportes periódicos y remitirlos a la instancia directiva correspondiente, por la unidad responsable del análisis de gestión. - Ajustar los umbrales de alerta de los indicadores al menos una vez al año, considerando hallazgos de revisiones internas o cambios normativos, por la función encargada del control institucional.	- Ficha técnica de indicadores definidos. - Reporte periódico de cumplimiento. - Registro de ajustes y validaciones periódicas.
	2. La ausencia de revisiones internas y externas con una periodicidad establecida impide detectar fallas en los controles de seguridad, aumentando el riesgo de exposición de información sensible.	- Programar revisiones periódicas por ejemplo internas semestrales y externas anuales de los sistemas de seguridad de la información, coordinadas por la unidad encargada de evaluaciones internas o control institucional. - Documentar formalmente los resultados de las revisiones realizadas, incluyendo hallazgos, recomendaciones y fechas de seguimiento, por la función responsable de resguardo documental. - Registrar la ejecución de las medidas correctivas derivadas de los hallazgos en un sistema de seguimiento institucional, con actualización periódica por la unidad que gestiona el plan de mejora.	- Programa anual de revisiones. - Informes técnicos de revisiones. - Registro de cumplimiento de medidas correctivas.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D5. Monitoreo, revisiones y evaluación de impacto.	3. La falta de automatización en los procesos de monitoreo y reportes relativos a incidentes puede generar retrasos en la detección de vulnerabilidades y en la implementación de medidas correctivas oportunas.	- Implementar herramientas tecnológicas que permitan el monitoreo automatizado de eventos de seguridad y generación de alertas inmediatas, bajo gestión de la unidad responsable del sistema documental institucional. - Configurar reportes automáticos con frecuencia diaria o semanal según criticidad, y distribuirlos a las funciones responsables de respuesta ante incidentes. - Revisar la configuración de las herramientas automatizadas al menos una vez cada trimestre, asegurando su adecuación a las necesidades actuales de la institución.	- Plataforma de monitoreo automatizado configurada. - Reportes generados automáticamente. - Bitácora de ajustes técnicos periódicos.
D6. Generaciones de Reportes y aplicar mejora continua.	1. La inexistencia de reportes periódicos sobre incidentes y hallazgos documentales impide el seguimiento institucional y debilita la capacidad para tomar decisiones informadas.	- Generar reportes técnicos periódicos (Ej. mensual) sobre incidentes de seguridad documental, elaborados por la unidad responsable del resguardo institucional, con el fin de informar a las jefaturas pertinentes y facilitar decisiones preventivas. - Consolidar periódicamente (Ej. semestral) los hallazgos y tendencias relevantes en materia de protección documental, por la función encargada del monitoreo de riesgos, a fin de orientar mejoras sistémicas. - Incorporar los reportes generados al expediente institucional de gestión de riesgos documentales, resguardado por la unidad responsable, para asegurar trazabilidad y respaldo ante revisiones.	- Reportes periódicos de incidentes. - Informes periódicos de tendencias. - Registro archivístico de reportes consolidados.
	2. La ausencia de mecanismos sistemáticos de mejora continua genera estancamiento en los procedimientos, dificultando la adaptación institucional a nuevas amenazas o requerimientos regulatorios.	- Diseñar y mantener un plan de mejora continua en materia de resguardo documental, actualizado periódicamente (Ej. anual) por la función encargada de seguridad de la información, a partir de evaluaciones previas y cambios normativos. - Registrar formalmente las acciones de mejora ejecutadas, especificando fecha, responsable y resultados, en un sistema institucional de seguimiento, a cargo del área técnica competente. - Revisar el cumplimiento del plan de mejora continua cada semestre mediante una matriz de verificación, elaborada por la unidad responsable del control documental.	- Plan anual de mejora continua. - Registro institucional de acciones correctivas. - Matriz de verificación periódica.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D6. Generaciones de Reportes y aplicar mejora continua.	3. La falta de articulación entre los reportes generados y la toma de decisiones institucionales limita el impacto del análisis de datos en la gestión de riesgos documentales.	- Socializar los reportes técnicos relevantes con las instancias directivas mediante presentaciones periódicamente (Ej. trimestral) coordinadas por la unidad responsable del resguardo documental, con el fin de facilitar la incorporación de medidas correctivas. Incorporar las observaciones derivadas de los reportes técnicos en el plan institucional de gestión documental, por la función encargada de la planificación estratégica, garantizando su trazabilidad. - Evaluar el uso efectivo de los reportes en la toma de decisiones mediante un análisis periódico (Ej. anual) de impacto, liderado por el área de control de gestión.	- Actas o presentaciones de reuniones de reporte. - Plan institucional con observaciones integradas. - Informe periódico de impacto en la toma de decisiones.
D7. Gestión del cumplimiento y sanciones.	1. La inexistencia de mecanismos internos de supervisión sobre el cumplimiento normativo en materia de resguardo documental incrementa el riesgo de infracciones legales o sanciones externas.	- Verificar periódicamente (Ej. trimestral) el cumplimiento de las políticas internas de protección documental mediante revisiones internas programadas, por la función encargada del control de gestión documental, con el objetivo de prevenir incumplimientos normativos y fortalecer el control institucional. - Documentar los hallazgos y desviaciones detectadas en cada revisión, en informes técnicos elaborados por la unidad responsable del monitoreo, para su posterior análisis y corrección. - Establecer alertas automatizadas en el SGD, configuradas por el área técnica correspondiente, para advertir sobre posibles incumplimientos o brechas operativas.	- Informes de revisiones internas. - Registro de hallazgos documentales. - Alertas configuradas en el SGD.
	2. La ausencia de un régimen interno de sanciones proporcionales limita la efectividad de las medidas de control y reduce la responsabilidad funcional sobre el resguardo de la información.	- Incorporar en el reglamento interno institucional un régimen de sanciones específicas por incumplimientos en la gestión de documentos, diseñado por la unidad jurídica y validado por la autoridad competente. - Comunicar de forma formal y periódica los lineamientos de sanciones a todo el personal, mediante inducciones, cápsulas o sesiones informativas, coordinadas por la unidad encargada de la gestión documental. - Registrar y archivar todas las sanciones aplicadas en un expediente de cumplimiento normativo, gestionado por el área correspondiente, como respaldo para evaluaciones o revisiones.	- Reglamento interno con sanciones. - Materiales de difusión y registro de capacitaciones. - Expediente de sanciones institucionales.

<i>Etapas o Subprocesos</i>	<i>Riesgos Asociados</i>	<i>Ejemplos de Controles Teóricos Mitigantes</i>	<i>Documentación Requerida</i>
D7. Gestión del cumplimiento y sanciones.	3. La inexistencia de un plan de prevención de riesgos legales en materia de protección documental aumenta la exposición institucional frente a eventuales multas, denuncias o cuestionamientos públicos.	- Diseñar y actualizar periódicamente (Ej. anual) un plan institucional de prevención de riesgos legales relacionados con el resguardo de información, elaborado por el área jurídica en coordinación con el área de gestión documental, para reducir la exposición institucional. - Evaluar periódicamente (Ej. semestral) los riesgos jurídicos emergentes mediante matrices de análisis actualizadas por la función encargada del cumplimiento normativo. - Revisar e incorporar las observaciones de órganos fiscalizadores al plan de prevención, mediante actas técnicas elaboradas por el área responsable de cumplimiento, para evidenciar trazabilidad y mejora continua.	- Plan anual de prevención de riesgos legales. - Matriz de evaluación periódica de riesgos. - Actas de revisión y posibles mejoras del plan institucional.

Capítulo 5

CONCLUSIONES Y RECOMENDACIONES FINALES

I 5.1 RECOMENDACIONES FINALES

En atención al análisis efectuado sobre los riesgos, controles y disposiciones normativas vinculadas a la gestión del ciclo de vida documental, la eliminación regulada de documentos y el resguardo de la información institucional, se presentan las siguientes recomendaciones finales. Estas orientaciones buscan fortalecer el cumplimiento normativo, mejorar la capacidad preventiva y de control de las instituciones públicas, y consolidar una cultura organizacional orientada a la gestión responsable de la información y la protección de los datos personales.

Su implementación debe adaptarse a la realidad operativa y nivel de madurez de cada entidad, considerando un enfoque progresivo, sostenible y verificable, en coherencia con los principios de legalidad, trazabilidad, transparencia y eficiencia que rigen el actuar de la Administración del Estado.

- **Desarrollar mecanismos institucionales de información a titulares de datos personales:**

Las instituciones deben implementar sistemas claros y accesibles para informar a los titulares sobre el tratamiento de sus datos personales, indicando finalidades, base legal y canales de contacto. Esto incluye cláusulas informativas en formularios, políticas de privacidad institucionales, plataformas web actualizadas y procedimientos de atención ciudadana, en cumplimiento del principio de transparencia activa.

- **Fomentar una cultura organizacional basada en la seguridad y trazabilidad documental:**

Es indispensable incorporar la seguridad de la información y la gestión documental como ejes transversales de la gestión institucional, integrándolos en los planes estratégicos, políticas internas y evaluaciones de desempeño. Esta cultura debe reflejarse en el comportamiento de los equipos, en el cumplimiento de procedimientos y en la atención a auditorías o requerimientos externos.

- **Establecer gobernanza institucional para la gestión documental y de datos:**

La participación activa de los distintos niveles jerárquicos es clave para asegurar la sostenibilidad de las medidas implementadas. Se recomienda formalizar estructuras de gobernanza (comités, responsables institucionales, coordinadores técnicos), con funciones específicas relacionadas con la gestión de documentos, protección de datos personales y seguridad de la información.

- **Implementar programas periódicos de formación para el personal:**

Se debe establecer un programa continuo de capacitación técnica dirigido a los funcionarios que intervienen en la creación, conservación, eliminación o tratamiento de documentos y datos. Los contenidos deben abordar aspectos normativos (como la Ley N°21.180 y la Ley N°21.719), operativos (gestión del ciclo de vida documental) y tecnológicos (seguridad, digitalización e interoperabilidad), asegurando su actualización periódica.

- **Realizar auditorías internas y revisiones sistemáticas de cumplimiento normativo:**

La identificación temprana de desviaciones o incumplimientos permite prevenir consecuencias mayores. Para ello, deben establecerse procedimientos de revisión regular, con apoyo de auditoría interna, que evalúen la aplicación efectiva de los controles y el cumplimiento de los marcos legales vigentes. Las brechas identificadas deben derivar en planes de mejora con responsables, plazos e indicadores de avance.

- **Fortalecer la coordinación con organismos reguladores y entidades de control:**

Las instituciones deben establecer canales formales de comunicación con la Contraloría General de la República, el Consejo para la Transparencia y la futura Agencia de Protección de Datos Personales. Esta relación permite el intercambio de buenas prácticas, la participación en instancias colaborativas y el cumplimiento oportuno de oficios, fiscalizaciones o requerimientos.

- **Transparentar las políticas de tratamiento de datos y gestión documental:**

La publicación proactiva de políticas, protocolos y procedimientos relacionados con el tratamiento de datos personales, la eliminación documental y la conservación de información fortalece la confianza ciudadana, permite el control social y reduce los riesgos reputacionales. Estas publicaciones deben estar disponibles en canales accesibles y actualizados.

- **Habilitar mecanismos para el ejercicio de los derechos de los titulares de datos:**

Las instituciones deben contar con canales electrónicos y físicos que permitan a la ciudadanía ejercer sus derechos de acceso, rectificación, supresión y oposición al tratamiento de datos personales. Estos mecanismos deben operar con procedimientos formales, plazos definidos, registro de solicitudes y trazabilidad, asegurando su atención efectiva conforme a la legislación vigente.

BIBLIOGRAFÍA

- **Constitución Política de la Republica: Capítulo III, De los Derechos y Deberes Constitucionales. Artículo 19 N°4.**
Garantiza el respeto y protección a la vida privada y a la honra de la persona y su familia.
- **Decreto N° 721 de 1980 del Ministerio de Educación.**
Crea la Comisión de Selección de Documentación de Descarte.
- **Ley N° 18.845 de 1989.**
Establece Sistemas de Microcopia o Micrograbación de Documentos.
- **Ley N°1 9.628 de 1999, Protección de la Vida Privada y su Reforma.**
Regula el tratamiento de datos personales y establece derechos y obligaciones en el manejo de la información.
- **Ley N° 19.880 de 2003.**
Establece bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado.
- **Ley N°20.285 de 2008.**
Sobre Acceso a la Información Pública, regula la transparencia y acceso a la información pública, con excepciones relacionadas con datos personales.
- **Ley N°21.180 de 2019, Transformación Digital del Estado.**
Introduce la digitalización de los procesos estatales, garantizando la protección de datos personales y la seguridad de los sistemas.
- **DFL N° 1 de 2021 (SEGPRES).**
Reglamenta la implementación de la Ley 21.180.
- **Decreto Fuerza Ley N° 5.200 de 1929 (Última versión 09.06.2022)**
Norma base sobre archivo de documentos del Estado.
- **Ley N°21.719 de 2024.**
Regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales.
- **Resolución Exenta N°1962 de 2022 de la CGR.**
Normas de control interno.
- **Normativa de la CGR.**
Establece instrucciones específicas para el manejo y resguardo de la información en el sector público, incluyendo auditorías de sistemas y cumplimiento.
- **Boletín Jurídico de 2024, CAIGG.**
Informa Reforma a la Ley 19.628 sobre Vida Privada.
- **Dictámenes relevantes de la CGR sobre protección de datos y resguardo de la información:**
 - Dictamen CGR N° E402560N23 de 2023.
 - Dictamen CGR N° 005414N14 de 2014.
 - Dictamen CGR N° 062205N16 de 2016.
 - Dictamen CGR N° 100175N14 de 2014.
 - Dictamen CGR N° 036407N05 de 2005.

CAIGG

CONSEJO DE AUDITORÍA INTERNA
GENERAL DE GOBIERNO



Ministerio Secretaría General de la Presidencia

A cerca de los Documentos Técnicos del CAIGG (DT)

Los Documentos Técnicos del CAIGG constituyen orientaciones especializadas destinadas a fortalecer y apoyar el ejercicio de la auditoría interna en el sector público. Abordan un conjunto amplio y estratégico de materias, entre ellas la gestión de riesgos, la prevención de la corrupción, la probidad administrativa, la auditoría interna, el gobierno corporativo, el control interno y la gestión de riesgos financieros, contribuyendo a la mejora continua y a la alineación con buenas prácticas nacionales e internacionales.

Propiedad Intelectual

El contenido de este documento es de propiedad del Consejo de Auditoría Interna General de Gobierno (CAIGG). Se permite la reproducción parcial de este documento únicamente con fines no comerciales, siempre que se cite adecuadamente la fuente, el título completo y la autoría correspondiente.