

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



**“EVALUACIÓN DE BASES DE DATOS EN CONTEXTOS
SOCIALES CONVULSIONADOS: BUENAS PRÁCTICAS
PARA EL REGISTRO DE VÍCTIMAS DURANTE EL
ESTALLIDO SOCIAL EN CHILE BASADO EN NORMA
ISO/IEC 27001 Y 27002”**

ARIANE BELÉN CARVAJAL CANDIA

**MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA**

Profesor Guía: Mauricio Figueroa
Profesor Correferente: Pedro Godoy
Profesor Co-Guía: Andrés Tello

Mes Marzo - 2026

Esta investigación fue realizada en el marco del Programa Milenio de la Agencia Nacional de Investigación y Desarrollo (ANID) de Chile, a través del Núcleo Milenio de Investigación en Producción y Uso Estatal de Datos sobre Severas Violaciones a Derechos Humanos (DATA JUSTA).



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo:

Evaluación de Bases de Datos en Contextos Sociales Convulsionados: Buenas Prácticas para el Registro de Víctimas Durante el Estallido Social en Chile Basado en Norma ISO/IEC 27001 y 27002.

Nombre del candidato(a):

Ariane Belén Carvajal Candia

Carrera / Grado:

Ingeniero Civil Informático

Campus: Casa Central **Departamento:** Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, **Mauricio Figueroa Colarte**, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- ❖ He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- ❖ El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

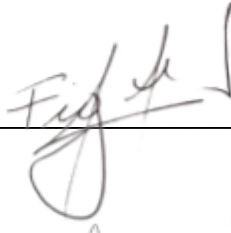
☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo): NA

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 15/06/20206

Firma: 

Estudiante o Candidato(a):

Fecha: 15/06/2026

Firma: 

DEDICATORIA

Hacia la biodiversidad que observé y acompaña mi espíritu. Estudio para protegerte.

AGRADECIMIENTOS

Cuando quise cambiar de rubro mi madre, hermano, tía y tío me supieron apoyar y acompañar. Su amor me dio fuerzas, alegrías y ganas de completar mi formación.

Mis queridas amistades también fueron fundamentales en mi camino. Me inspiraron en cada momento, me hicieron reír, me recordaron cariñosamente que cultivar el cuerpo es tan importante como cultivar la mente, y me dieron un hogar y una familia en una región que no me vio nacer.

Y por último mis amados gatos, Mako, Cati, Ruschka, Korra y Negrito. Cuidarlos, verlos envejecer y morir ha sido mi privilegio y honor.

Los llevaré siempre conmigo.

RESUMEN

Resumen—La presente memoria aborda el problema de la seguridad de la información en la gestión de antecedentes sensibles en la Comisión de Víctimas de Violencia Institucional (CVVI), dependiente del Ministerio de Justicia y Derechos Humanos de Chile. El objetivo del trabajo fue proponer una metodología de evaluación y mitigación de riesgos que permita robustecer el resguardo de activos físicos y digitales involucrados en el registro y manejo de información sensible. Para ello, se realizó un levantamiento del entorno de trabajo, identificando activos, vulnerabilidades y prácticas operativas asociadas a la gestión documental y al tratamiento de datos. Posteriormente, se aplicó un análisis de riesgos basado en una matriz de probabilidad e impacto, priorizando aquellos de severidad extrema. Sobre esta base, se propusieron controles de mitigación alineados con ISO/IEC 27002:2022, justificando su pertinencia según el contexto institucional. Como resultado principal, se obtuvo una propuesta de mitigación de riesgos extremos técnicamente fundamentada y trazable, junto con una priorización de controles donde destacan medidas de trazabilidad, monitoreo, procedimientos documentados, transferencia segura de información, clasificación, respaldo y cifrado.

Palabras Clave—*Seguridad de la información; Gestión de riesgos; ISO/IEC 27002:2022; Sector público; violencia institucional.*

ABSTRACT

Abstract—This thesis addresses the problem of information security in the management of sensitive records at the Commission for Victims of Institutional Violence (CVVI), under the Ministry of Justice and Human Rights of Chile. The objective of this work was to propose a risk assessment and mitigation methodology to strengthen the protection of physical and digital assets involved in the registration and handling of sensitive information. To this end, a survey of the work environment was conducted, identifying assets, vulnerabilities, and operational practices associated with document management and data processing. Subsequently, a risk analysis based on a probability and impact matrix was applied, prioritizing those of extreme severity. Based on this analysis, mitigation controls aligned with ISO/IEC 27002:2022 were proposed, justifying their relevance according to the institutional context. The main result was a technically sound and traceable proposal for mitigating extreme risks, along with a prioritization of controls that emphasize traceability measures, monitoring, documented procedures, secure information transfer, classification, backup, and encryption.

Keywords—*Information security; Risk management; ISO/IEC 27002:2022; Public sector; Sensitive information.*

INDICE DE CONTENIDOS

RESUMEN	3
ABSTRACT	4
INDICE DE CONTENIDOS	4
INDICE DE FIGURAS	7
INDICE DE TABLAS	7
INTRODUCCIÓN	10
CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA	11
1.1. CONTEXTO DEL ESTALLIDO SOCIAL DE 2019	11
1.2. PANORAMA Y LIMITACIONES EN LOS SISTEMAS DE REGISTRO DE VÍCTIMAS	11
1.3. ACTORES Y USUARIOS	14
1.4. IMPLICANCIAS DE NO ABORDAR EL PROBLEMA	16
1.5. MOTIVACIÓN Y ALCANCE DE LA MEMORIA	16
CAPÍTULO 2: MARCO CONCEPTUAL	18
2.1. INTRODUCCIÓN	18
2.2. INFRAESTRUCTURA DE INFORMACIÓN	18
2.3. ENFOQUE DE DERECHOS HUMANOS Y REGISTRO DE VÍCTIMAS	19
2.4. BASES DE DATOS, PRINCIPIOS Y BUENAS PRÁCTICAS	21
2.5. GOBERNANZA DE DATOS	23
2.6. GESTIÓN DE LA INFORMACIÓN Y BUENAS PRÁCTICAS	24
2.7. SEGURIDAD DE LA INFORMACIÓN Y BUENAS PRÁCTICAS EN BASES DE DATOS	28
2.8. MARCO DAMA Y BUENAS PRÁCTICAS EN LA GESTIÓN DE LA INFORMACIÓN	31
2.9. ESTÁNDARES ISO/IEC 27001 Y 27002:2022	36
2.10. MARCO NORMATIVO CHILENO APLICABLE A LA GESTIÓN DE BASES DE DATOS DE VÍCTIMAS	43
2.11. CASO DE ESTUDIO: COMISIÓN DE VÍCTIMAS DE VIOLENCIA INSTITUCIONAL (CVVI)	46
2.12. NATURALEZA SOCIOTÉCNICA DEL PROBLEMA	46
CAPÍTULO 3: PROPUESTA DE SOLUCIÓN	47
3.1. ALCANCE DE LA INVESTIGACIÓN	47
3.2. ACTIVIDADES DESARROLLADAS	47
3.3. DESCRIPCIÓN DEL PROCESO DE REGISTRO Y GESTIÓN DE INFORMACIÓN	48
3.4. INVENTARIO DE ACTIVOS DE INFORMACIÓN	51
3.5. IDENTIFICACIÓN DE RIESGOS POR ACTIVOS	55
3.6. ANÁLISIS DE RIESGO ACEPTABLE	63

3.7. SELECCIÓN DE CONTROLES DE MITIGACIÓN DE RIESGOS EXTREMOS	65
3.8. ANÁLISIS DEL PATRÓN DE CONTROLES PROPUESTOS	77
CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN	79
4.1. ALCANCE Y LIMITACIONES DE LA VALIDACIÓN	79
4.2. ESTRATEGIA DE VALIDACIÓN ADOPTADA	80
4.3. VALIDACIÓN DE IMPLEMENTACIÓN INCREMENTAL (MÍNIMO VIABLE DE SEGURIDAD)	81
4.4. DISCUSIÓN DE RESULTADOS DE VALIDACIÓN	83
CAPÍTULO 5: CONCLUSIONES	85
5.1. CONCLUSIÓN GENERAL Y CUMPLIMIENTO DE OBJETIVOS	85
5.2. PRINCIPALES RESULTADOS Y HALLAZGOS	86
5.3. APORTES E IMPACTO DEL TRABAJO	87
5.4. ALCANCES Y LIMITACIONES DE LA PROPUESTA	87
5.5. REFLEXIONES SOBRE CAPACIDADES ESTATALES Y FALTA DE PERFILES INFORMÁTICOS	87
5.6. RECOMENDACIONES Y TRABAJO FUTURO	88
5.7. CONCLUSIÓN FINAL	89
ANEXO A: PAUTA DE ENTREVISTA	92
ANEXO B: ENTREVISTAS Y CORPUS DOCUMENTAL	94
ANEXO C: TABLA DE CÁLCULO DE CRITICIDAD DE ACTIVOS	95
ANEXO D: TABLA DE CÁLCULO DE SEVERIDAD DEL RIESGO	96
ANEXO E: RÚBRICA DE EVALUACIÓN	97

INDICE DE FIGURAS

Figura 1: Actores de instituciones estatales y organizaciones de la sociedad civil.	14
Figura 2: Proceso de registro y generación de productos CVVI.	48
Figura 3: Top 10 Cantidad de veces que un Control fue recomendado	77

INDICE DE TABLAS

Tabla 1: Entradas del proceso de registro y gestión de información de CVVI.	49
Tabla 2: Salidas del proceso de registro y gestión de información de CVVI.	50
Tabla 3: Activos del proceso de registro y gestión de información de CVVI.	51
Tabla 4: Riesgos del proceso de registro y gestión de información de CVVI.	54
Tabla 5: Riesgos del activo Planilla Maestra de Casos.	56
Tabla 6: Riesgos del activo Planillas Externas Recibidas.	58
Tabla 7: Riesgos del activo Carpetas Documentales por Caso.	58
Tabla 8: Riesgos del activo Documentos Probatorios.	59
Tabla 9: Riesgos del activo Digitalizaciones y Escaneos.	59
Tabla 10: Riesgos del activo Base Estadística Consolidada.	59
Tabla 11: Riesgos del activo Minutas Internas y Actas.	60
Tabla 12: Riesgos del activo Correos Institucionales.	60
Tabla 13: Riesgos del activo Repositorio Institucional.	60
Tabla 14: Riesgos del activo Equipos Computacionales.	61
Tabla 15: Riesgos del activo Soportes Físicos de Transferencia.	61
Tabla 16: Riesgos del activo Personal del Equipo.	62
Tabla 17: Riesgos del activo Oficina del Equipo.	62
Tabla 18: Riesgos del activo Sala de Reunión.	63
Tabla 19: Nivel de Riesgo Aceptable.	63
Tabla 20: Riesgo Acceso no autorizado.	65
Tabla 21: Medidas de control para Riesgo Acceso no Autorizado.	65
Tabla 22: Riesgo Modificación inadvertida.	66
Tabla 23: Medidas de control para Riesgo Modificación inadvertida	66
Tabla 24: Riesgo Uso indebido del archivo.	66
Tabla 25: Medidas de control para Riesgo Uso indebido del archivo.	67
Tabla 26: Riesgo Exposición masiva de datos sensibles.	67
Tabla 27: Medidas de control para Riesgo Exposición masiva de datos sensibles.	67
Tabla 28: Riesgo Fuga de datos por reenvío.	68
Tabla 29: Medidas de control para Riesgo Fuga de datos por reenvío.	68
Tabla 30: Riesgo Alteración no detectada.	68
Tabla 31: Medidas de control para Riesgo.	69
Tabla 32: Riesgo Pérdida física.	69
Tabla 33: Medidas de control para Riesgo Pérdida física.	69
Tabla 34: Riesgo Inexistencia de respaldo sistemático.	70
Tabla 35: Medidas de control para Riesgo Inexistencia de respaldo sistemático.	70
Tabla 36: Riesgo Pérdida u omisión documental.	70
Tabla 37: Medidas de control para Riesgo Pérdida u omisión documental	70

Tabla 38: Riesgo Exposición indebida.	71
Tabla 39: Medidas de control para Riesgo Exposición indebida.	71
Tabla 40: Riesgo Error en consolidación.	72
Tabla 41: Medidas de control para Riesgo Error en consolidación.	72
Tabla 42: Riesgo Pérdida o corrupción.	72
Tabla 43: Medidas de control para Riesgo Pérdida o corrupción.	73
Tabla 44: Riesgo Falta de catálogo completo.	73
Tabla 45: Medidas de control para Riesgo Falta de catálogo completo.	73
Tabla 46: Riesgo Pérdida o traspaso no controlado.	74
Tabla 47: Medidas de control para Riesgo Pérdida o traspaso no controlado.	74
Tabla 48: Riesgo Uso indebido.	74
Tabla 49: Medidas de control para Riesgo Uso indebido.	75
Tabla 50: Riesgo Phishing / Ingeniería Social.	75
Tabla 51: Medidas de control para Riesgo Phishing / Ingeniería Social.	75
Tabla 52: Riesgo Acceso físico indebido a dependencias institucionales.	76
Tabla 53: Medidas de control para Riesgo Acceso físico indebido a dependencias institucionales.	76
Tabla 54: Gantt de alto nivel para aplicación de controles.	81

INTRODUCCIÓN

En los últimos años, la transformación digital del Estado (Ley N° 21.180 de Transformación Digital del Estado, publicada el 11 de noviembre de 2019, modifica las bases de los procedimientos administrativos para su digitalización) ha incrementado el uso de sistemas, planillas, repositorios y flujos documentales para registrar, gestionar y analizar información en múltiples instituciones públicas. Este proceso ha permitido mejorar la disponibilidad de antecedentes y apoyar la coordinación entre unidades, pero también ha expuesto una dificultad persistente: el fortalecimiento de la seguridad de la información no siempre avanza al mismo ritmo que la digitalización de los procesos. Esta brecha se vuelve especialmente crítica en organismos que trabajan con antecedentes sensibles, donde la pérdida, alteración o exposición indebida de la información puede comprometer los derechos de las personas, la trazabilidad institucional y afectar la capacidad de respuesta del Estado.

Este escenario resulta particularmente relevante en unidades que gestionan información asociada a víctimas, donde conviven documentos físicos, planillas de trabajo, repositorios digitales, transferencias de archivos y prácticas operativas heterogéneas. En estos contextos, la seguridad de la información no depende únicamente de infraestructura tecnológica, sino también de la forma en que se organizan los procesos, se asignan responsabilidades, se controla el acceso a los antecedentes y se resguardan los activos físicos y digitales involucrados en la operación cotidiana.

La presente memoria se desarrolla en este marco, tomando como caso de estudio a la Comisión de Víctimas de Violencia Institucional (CVVI), dependiente del Ministerio de Justicia y Derechos Humanos de Chile. La CVVI trabaja con antecedentes sensibles en un entorno donde coexisten soportes físicos y digitales, procesos manuales y semiestructurados, y restricciones institucionales de recursos que dificultan la implementación de medidas de seguridad de manera integral.

Frente a esta situación se propone una metodología de trabajo para robustecer la seguridad de la información, orientada a la identificación, priorización y mitigación de riesgos en activos físicos y digitales relevantes para la operación de la CVVI. Para ello se realizó un levantamiento del entorno de gestión de información, identificando activos, vulnerabilidades y prácticas operativas. Posteriormente, se desarrolló un análisis de riesgos mediante una matriz de probabilidad e impacto, con el fin de priorizar aquellos riesgos de mayor severidad. A partir de dicha priorización, se propusieron controles de mitigación para los riesgos extremos, justificando su pertinencia en función del contexto institucional. Finalmente, la propuesta se valida a nivel de factibilidad y pertinencia, sin ejecutar una implementación operativa completa, tomando en cuenta la pertinencia contextual e implementabilidad incremental, considerando las restricciones reales de presupuesto, capacidades técnicas y horas-hombre existentes en la institución.

CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA

1.1. CONTEXTO DEL ESTALLIDO SOCIAL DE 2019

El 18 de octubre de 2019 se inició en Chile un ciclo de protestas sociales sin precedentes desde el retorno a la democracia en 1990. Lo que comenzó como una reacción al alza en la tarifa del transporte público se transformó rápidamente en un movimiento nacional que exigía reformas estructurales en pensiones, salud, educación y reducción de la desigualdad (Jiménez-Yañez, 2020).

Durante esos meses, el Estado respondió con medidas de control que incluyeron el despliegue de Fuerzas Armadas en las calles y un uso intensivo de la fuerza policial. Como consecuencia, se produjeron violaciones masivas a los derechos humanos, documentadas tanto por organismos chilenos como internacionales. El Instituto Nacional de Derechos Humanos (INDH) presentó 3.023 querellas judiciales, de las cuales 460 fueron por lesiones oculares causadas por disparos de proyectiles (INDH, 2020). El Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH, 2019) y Human Rights Watch (2020) señalaron que las violaciones tuvieron un carácter generalizado y sistemático, abarcando detenciones arbitrarias, malos tratos, torturas, violencia sexual y muertes en contexto de protesta.

Este escenario tensionó las infraestructuras de información. La magnitud de los hechos superó la capacidad de los sistemas estatales de registro, las instituciones encargadas de registrar denuncias y víctimas (como INDH, Ministerio Público, Fiscalía, Defensoría de la Niñez y organizaciones de la sociedad civil), debieron procesar volúmenes de datos muy superiores a los habituales, en un entorno de alta presión social y política. Así surgió el problema de la fragmentación y precariedad en el registro de víctimas, que aún hoy es objeto de análisis académico y político.

1.2. PANORAMA Y LIMITACIONES EN LOS SISTEMAS DE REGISTRO DE VÍCTIMAS

En el contexto del estallido social, la producción de datos sobre violaciones de derechos humanos se intensificó de manera abrupta. Hoy existe una multiplicidad de bases de datos, repositorios y registros que buscan documentar lo ocurrido entre 2019 y 2020. Estas iniciativas provienen tanto de organismos estatales (INDH, Ministerio Público, Subsecretaría de Derechos Humanos, Defensoría de la Niñez) como de organizaciones de la sociedad civil (ONG, colectivos de víctimas, observatorios). Sin embargo, la infraestructura de información resultante presenta problemas estructurales que dificultan su uso coordinado y eficiente.

1.2.1. FRAGMENTACIÓN INSTITUCIONAL

La información se encuentra dispersa en múltiples instituciones, cada una con su propio mandato y lógica de recolección de datos.

- **Organismos estatales** registran hechos según su competencia legal o médica: el Instituto Nacional de Derechos Humanos (INDH) documenta violaciones a los derechos humanos y presenta querellas cuando corresponde; el Ministerio Público investiga los delitos asociados y mantiene bases de datos de causas penales; el Poder Judicial administra el estado procesal de las causas y resoluciones; Carabineros y la Policía de Investigaciones (PDI) levantan partes policiales, detenciones y antecedentes; y el Servicio Médico Legal (SML) registra peritajes forenses, autopsias y constatación de lesiones en el marco de investigaciones judiciales y de derechos humanos.
- **Organizaciones civiles** mantienen listados de víctimas, catálogos de casos y documentación médica, a menudo con el objetivo de incidir en políticas públicas o prestar apoyo psicosocial y legal.

Esta fragmentación hace que muchas víctimas aparezcan en múltiples registros, sin un identificador único o sistema que enlace los diferentes datos, lo cual dificulta reconstruir trayectorias completas de casos, verificar su estado legal o su tratamiento médico y social (Sasse, 2021).

1.2.2. FALTA DE ESTANDARIZACIÓN DE DATOS

Cada institución define sus propios campos y categorías para describir los eventos. Por ejemplo, una base de datos clasifica de manera explícita las “lesiones oculares”, otra las agrupa bajo la categoría más amplia de “lesiones físicas graves”; también sucede que el agente perpetrador puede ser registrado simplemente como “policía” u “otro”, o bien desagregado en subcategorías como “Carabineros”, “PDI”, “militar” o “actor externo”. Esta diversidad se replica en el formato de los datos: fechas registradas como texto (“18 de octubre de 2019”), como campos tipo *timestamp* o en diferentes estándares de fecha; identificadores personales (RUT, pasaporte) escritos con o sin guiones; e incluso ubicaciones geográficas que pueden incluir comuna y región, solo región o coordenadas. A esto se suman las diferencias semánticas entre instituciones en conceptos clave como “víctima directa”, “víctima secundaria” o “hecho de violencia”, que en algunos casos abarcan desde la jornada completa de manifestaciones hasta incidentes específicos de represión.

Esto complica la interoperabilidad pues no existen esquemas compatibles que permitan consolidar o comparar datos entre instituciones (Lindeberg & Henkel, 2024). Cuando se

intenta un análisis agregado, se deben realizar limpiezas manuales, reconciliaciones semánticas, lo que consume muchos recursos y puede introducir errores.

1.2.3. PROCESOS MANUALES Y SISTEMAS HEREDADOS

La recolección, consolidación y actualización de datos en el contexto de las violaciones de derechos humanos durante el estallido social depende en gran medida de herramientas manuales o semimanuales. Muchas instituciones continúan utilizando hojas de cálculo (Excel u hojas similares), documentos de texto y formularios en papel que luego deben digitalizarse, lo que genera flujos de trabajo tediosos y propensos a error. A esto se suma la existencia de sistemas antiguos (*“legacy systems”*) que no cuentan con interfaces modernas ni mecanismos de integración automatizada, lo que limita la capacidad de interoperar con otras plataformas o de incorporar nuevos datos en tiempo real (The Engine Room & HURIDOCS, n.d.).

Este escenario tiene consecuencias directas sobre la calidad y oportunidad de la información. Los casos pueden tardar días o incluso semanas en ser incorporados a las bases de datos o en actualizar su estado, lo que ralentiza la generación de estadísticas y retrasa las acciones de seguimiento. Estas condiciones dificultan la trazabilidad de cada caso, ya que no siempre es posible saber qué institución lo registró primero, qué acciones legales se han tomado ni cuál es su situación actual, comprometiendo la confiabilidad del sistema de información en su conjunto.

1.2.4. DESIGUALDAD EN PROTECCIÓN DE DATOS

La seguridad y la privacidad de la información sensible presentan grandes desigualdades entre las instituciones que documentan violaciones a los derechos humanos. Mientras algunas cuentan con políticas más robustas de protección de datos personales, cifrado y controles de acceso, otras operan con documentos compartidos en la nube o en soportes físicos sin protocolos claros de resguardo. Esta situación expone a riesgo información altamente sensible, como nombres e identificadores personales, antecedentes médicos o judiciales, que si no se encuentran adecuadamente custodiados pueden ser objeto de filtraciones o uso indebido. El peligro no es meramente hipotético: en contextos de protesta y represión, la exposición de estos datos puede derivar en revictimización, intimidación o nuevas vulneraciones para las personas afectadas. Cabe destacar que la regulación chilena ha avanzado recientemente con la promulgación de la Ley Nº 21.719 (Badillo, 2025), que moderniza el régimen de protección de datos personales, estableciendo estándares más exigentes de tratamiento y seguridad. Sin embargo, este avance normativo evidencia que muchas de las prácticas actuales todavía permanecen por debajo de los niveles de resguardo requeridos.

1.2.5. AUSENCIA DE UN SISTEMA INTEGRADO

A pesar de los esfuerzos parciales y locales por mejorar la gestión de información, no se ha logrado conformar un sistema institucionalizado que permita integrar de manera confiable los datos producidos por entidades estatales y organizaciones de la sociedad civil. Esta carencia implica que no existen estándares uniformes que aseguren la seguridad, privacidad, definiciones y formatos de los registros, ni mecanismos que permitan garantizar la trazabilidad completa de cada caso, desde la denuncia o queja inicial hasta su resolución final, incluyendo la atención médica recibida, el avance judicial o administrativo y las eventuales medidas de reparación. La falta de un sistema integrado tiene como consecuencia que las cifras disponibles resulten con frecuencia subestimadas, incompletas o desactualizadas, lo que debilita la capacidad del Estado y de los investigadores para formular políticas públicas basadas en evidencia sólida y para responder de manera oportuna a las demandas de verdad, justicia y reparación de las víctimas.

1.3. ACTORES Y USUARIOS

La gestión de la información sobre violaciones de derechos humanos durante el estallido social involucra a un amplio conjunto de instituciones y personas que producen, administran, analizan y utilizan estos datos.

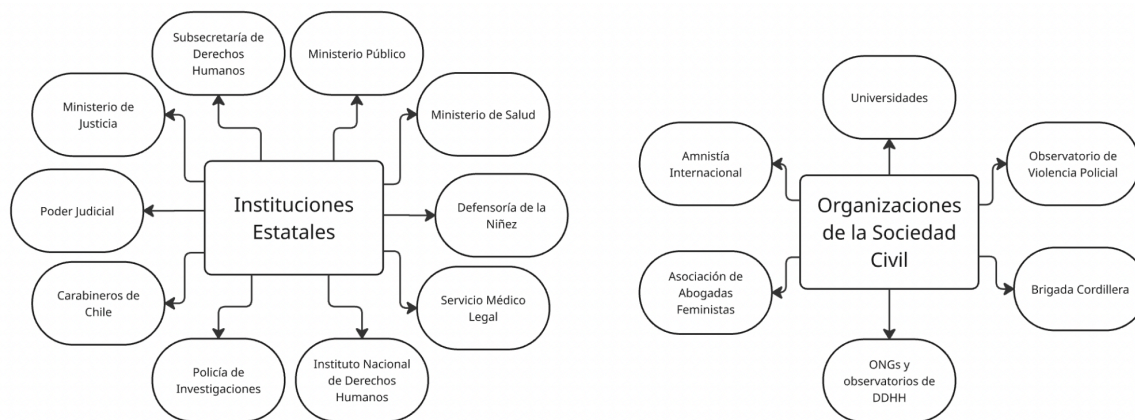


Figura 1: Actores de instituciones estatales y organizaciones de la sociedad civil.

Fuente: Elaboración propia.

1.3.1. INSTITUCIONES ESTATALES

- **Instituto Nacional de Derechos Humanos (INDH):** Documenta violaciones de derechos humanos, recibe denuncias y presenta querellas judiciales en representación de las víctimas cuando corresponde.

- **Ministerios:** Dirige las investigaciones penales asociadas a delitos cometidos durante el estallido, manteniendo bases de datos de causas y diligencias. Apoya con datos sobre víctimas.
- **Poder Judicial:** Administra el estado procesal de las causas, resolviendo sobre la imputación de responsabilidades y emitiendo sentencias.
- **Subsecretaría de Derechos Humanos:** Coordina políticas públicas de verdad, justicia, reparación y garantías de no repetición, y consolida información interinstitucional.
- **Defensoría de la Niñez:** Interviene en casos que afectan a niños, niñas y adolescentes, monitoreando vulneraciones de derechos y emitiendo recomendaciones.
- **Carabineros de Chile y Policía de Investigaciones (PDI):** Generan registros de detenciones, partes policiales y antecedentes.
- **Servicio Médico Legal (SML):** Realiza peritajes forenses, constataciones de lesiones y autopsias que sirven como insumo en procesos judiciales y en la documentación de violaciones de derechos.

1.3.2. ORGANIZACIONES DE LA SOCIEDAD CIVIL

- **ONG y observatorios de derechos humanos:** Como Amnistía Internacional y el Observatorio de Violencia Policial, que recopilan testimonios, elaboran informes y ejercen presión internacional para visibilizar las violaciones.
- **Colectivos de víctimas y organizaciones territoriales:** Como Brigada Cordillera, que mantiene listados propios, apoya a las personas afectadas y aportan datos complementarios sobre contexto, impacto psicosocial y necesidades de reparación.
- **Redes de profesionales de la salud y de abogados/as:** Como ABOFEM, que provee asistencia médica, psicológica y representación legal, registrando casos que en ocasiones no aparecen en los sistemas oficiales.

1.3.3. ACADÉMICOS E INVESTIGADORES

Universidades, centros de investigación y consultoras académicas brindaron atención a víctimas y utilizan esta información para producir análisis estadísticos, estudios de impacto y recomendaciones de política pública.

1.3.4. VÍCTIMAS Y FAMILIARES

Las víctimas y sus familias son las principales usuarias de los registros. Su acceso a información confiable es esencial para ejercer su derecho a la verdad, la justicia y la reparación.

1.4. IMPLICANCIAS DE NO ABORDAR EL PROBLEMA

La falta de acción para resolver las brechas diagnosticadas en los sistemas de registro de víctimas tiene efectos directos sobre el ejercicio de derechos fundamentales y sobre la capacidad del Estado y la sociedad civil de responder de manera efectiva a situaciones de crisis.

1.4.1. RIESGO DE PÉRDIDA O FILTRACIÓN DE INFORMACIÓN SENSIBLE

La ausencia de políticas unificadas de seguridad de la información, o su aplicación parcial e inconsistente, combinada con el uso de sistemas manuales y almacenamiento en plataformas sin protocolos claros, eleva el riesgo de filtraciones, accesos no autorizados o pérdida de datos críticos. Esto no solo tiene consecuencias legales para las instituciones, sino que puede exponer a las víctimas a nuevas vulneraciones, revictimización o represalias, especialmente en casos que involucran fuerzas de seguridad o agentes estatales.

1.4.2. DEBILITAMIENTO DE LA FORMULACIÓN DE POLÍTICAS PÚBLICAS

Las decisiones de política pública dependen de información confiable y oportuna. Si los datos disponibles son incompletos o inconsistentes, se corre el riesgo de diseñar programas de reparación insuficientes, asignar recursos de manera ineficiente o subestimar la magnitud de las violaciones. Esto puede perpetuar la desconfianza de la ciudadanía hacia el Estado y reducir el impacto de las medidas de justicia transicional.

1.4.3. INEFICIENCIA Y FALTA DE COORDINACIÓN

Sin un sistema integrado de registro, las instituciones continuarán operando de manera aislada, duplicando esfuerzos y generando cargas de trabajo innecesarias. Esta ineficiencia compromete la capacidad de respuesta en tiempo real ante futuras crisis sociales, ya que obliga a repetir procesos manuales de consolidación de datos y retrasa la producción de información para la toma de decisiones estratégicas.

1.5. MOTIVACIÓN Y ALCANCE DE LA MEMORIA

La motivación central de esta memoria radica en la necesidad de fortalecer la confiabilidad, seguridad e interoperabilidad de los sistemas de registro de víctimas en contextos sociales convulsionados. El estallido social de 2019 en Chile evidenció que las

plataformas de información disponibles no estaban preparadas para enfrentar el volumen, la especificidad ni la sensibilidad de los datos generados. La fragmentación de bases de datos, la falta de estandarización de campos, las limitaciones en trazabilidad y las debilidades en materia de seguridad de la información generaron vacíos y subregistros que afectan directamente el derecho de las víctimas a la verdad, justicia y reparación.

A partir de esta investigación se propone evaluar las prácticas actuales de diseño y gestión de bases de datos utilizadas por instituciones estatales y, en particular, por la Comisión de Víctimas de Violencia Institucional (CVVI) de la Subsecretaría de Derechos Humanos del Ministerio de Justicia y Derechos Humanos de Chile. El levantamiento de información se realizará mediante la aplicación de la Guía Técnica de Seguridad de la Información y Ciberseguridad, instrumento oficial que operacionaliza la Ley N° 21.180 sobre Transformación Digital del Estado y que se alinea con los estándares internacionales de seguridad de la información establecidos en las normas ISO/IEC 27001 y 27002:2022.

1.5.1. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

Evaluar las prácticas de diseño y gestión de bases de datos utilizadas por instituciones estatales durante el estallido social de 2019 en Chile, con énfasis en la estandarización y la seguridad informática, con el fin de proponer lineamientos de mejora.

Para ello se proponen los siguientes objetivos específicos:

- Analizar las estructuras de datos, esquemas y herramientas utilizadas para el registro de víctimas durante el estallido social, considerando el caso de CVVI.
- Evaluar los mecanismos de seguridad implementados en el sector estatal, tomando como referencia las normas ISO/IEC 27001 y 27002:2022.
- Diseñar un plan de acción con recomendaciones de controles de seguridad que permitan mitigar los riesgos identificados en la institución analizada.

El trabajo no incluirá instituciones privadas ni sociedades civiles por tratarse de una delimitación metodológica orientada a mantener comparabilidad y coherencia con el objetivo del estudio: la evaluación se centra en bases de datos bajo gobernanza estatal, sujetas a marcos de Transformación Digital, interoperabilidad y obligaciones de seguridad aplicables al sector público. Incluir actores privados o de sociedad civil ampliaría el alcance hacia regímenes normativos y modelos de gestión del dato heterogéneos, dificultando la evaluación con un marco común y excediendo los recursos de esta memoria.

Con esta memoria se busca generar un insumo técnico que contribuya a robustecer los sistemas de registro de víctimas, sirviendo de referencia para la implementación de buenas prácticas en otros organismos del Estado y garantizando que, en futuros escenarios de crisis, la información sensible pueda ser gestionada de manera segura, estandarizada y orientada a la protección de derechos humanos.

CAPÍTULO 2: MARCO CONCEPTUAL

2.1. INTRODUCCIÓN

Este capítulo presenta los fundamentos teóricos, técnicos y normativos que sustentan la evaluación de bases de datos en contextos sociales convulsionados. Se establecen los conceptos clave sobre infraestructuras de información, gestión de datos, seguridad de la información y gobernanza, así como los marcos regulatorios asociados a la protección de los derechos humanos y los datos personales en Chile. El objetivo es proporcionar una base común para comprender la relevancia y los alcances de la propuesta metodológica desarrollada en esta memoria, en particular respecto al registro de víctimas de violencia institucional durante el estallido social de 2019 y al rol de la Comisión de Víctimas de Violencia Institucional (CVVI).

2.2. INFRAESTRUCTURA DE INFORMACIÓN

Se entiende por infraestructuras de información (II) al entramado sociotécnico¹ compuesto por recursos tecnológicos, procedimientos, estándares y prácticas sociales que permiten producir, almacenar, intercambiar y mantener información a lo largo del tiempo. Este concepto es una evolución de las Tecnologías de la Información y Comunicación (TIC) de la década de 1990, que eran concebidas principalmente como un conjunto de recursos y técnicas para el procesamiento y transmisión de datos.

Con el avance de la tecnología en el siglo XXI, este enfoque pasó de un procesamiento local a uno distribuido, remoto, ubicuo y transmedia, lo que dio lugar a la noción de infraestructura, y en particular de infraestructuras de información (Hanseth & Monteiro, 1998).

Bowker (2008) propone que la infraestructura puede entenderse como el conjunto de equipamientos y arreglos necesarios para el funcionamiento de la actividad humana, mientras que Star y Ruhleder (1996) destacan que las infraestructuras presentan propiedades distintivas: se encuentran embebidas en otras estructuras sociales y tecnológicas, poseen un ámbito de aplicación espacial y temporal, se aprenden colectivamente en comunidades de práctica, están articuladas mediante estándares y normas para facilitar su socialización, evolucionan de forma gradual sobre una base instalada previa y se vuelven visibles cuando fallan.

Bajo estas perspectivas, las infraestructuras de información no sólo incluyen los elementos tecnológicos (plataformas, redes, bases de datos, software y protocolos) sino que también los acuerdos, convenciones y procesos institucionales que permiten que los datos circulen

¹ Término que se utiliza para designar la interacciones entre la tecnología y las personas.

de manera coherente entre distintos actores (ministerios, servicios públicos, fiscalías, organizaciones civiles).

2.3. ENFOQUE DE DERECHOS HUMANOS Y REGISTRO DE VÍCTIMAS

El análisis técnico de bases de datos que documentan hechos de violencia estatal requiere situarse en un marco normativo y conceptual basado en los derechos humanos. En este contexto, el concepto de víctima no se reduce a una categoría administrativa ni estadística: corresponde a toda persona que ha sufrido un daño físico, psicológico, económico o moral como consecuencia de acciones u omisiones que vulneran derechos fundamentales. Este entendimiento deriva de estándares internacionales como los Principios y Directrices Básicos sobre el Derecho de las Víctimas de Violaciones Manifiestas de las Normas Internacionales de Derechos Humanos (ONU, 2005), los cuales establecen obligaciones estatales directas en materia de documentación, protección y reparación.

2.3.1. DERECHO A LA VERDAD, JUSTICIA, REPARACIÓN Y NO REPETICIÓN

La existencia misma de registros fiables se relaciona directamente con cuatro derechos esenciales en materia de violaciones a los derechos humanos:

- **Derecho a la verdad:** exige que el Estado documente adecuadamente los hechos, actores involucrados, patrones de violencia y consecuencias. Sin datos precisos y verificables, no es posible reconstruir los hechos ni comprender la magnitud de las violaciones.
- **Derecho a la justicia:** requiere información íntegra y trazable que pueda utilizarse como evidencia administrativa o judicial. La ausencia de información, su inconsistencia o pérdida pueden obstaculizar investigaciones o favorecer la impunidad.
- **Derecho a la reparación:** las medidas de reparación (indemnización, rehabilitación, restitución, garantías de no repetición) dependen de registros que identifiquen correctamente a las personas afectadas, los daños sufridos y las acciones tomadas por el Estado.
- **Garantías de no repetición:** demandan sistemas de información robustos que permitan analizar patrones, monitorear prácticas institucionales y diseñar políticas preventivas basadas en evidencia.

Desde esta perspectiva, la calidad, integridad y seguridad de las bases de datos no son solo requisitos técnicos: constituyen obligaciones derivadas de la protección internacional de los derechos humanos.

2.3.2. EL REGISTRO DE VÍCTIMAS COMO HERRAMIENTA SOCIOTÉCNICA

El registro de víctimas cumple múltiples funciones en la estructura institucional del Estado. Estas funciones permiten entender las bases de datos no como repositorios estáticos, sino como dispositivos sociotécnicos que interactúan con prácticas administrativas, jurídicas y políticas.

- **Dispositivo de reconocimiento:** registrar a una persona como víctima implica un acto de reconocimiento social y jurídico. Lo que se registra, y lo que no, determina qué tipos de daño son visibles, qué hechos se consideran violaciones y qué personas son formalmente incorporadas a procesos de acompañamiento o reparación.
- **Herramienta de política pública:** los datos recopilados sirven como insumo para la formulación de políticas, priorización institucional, asignación de recursos y diseño de programas de reparación. Políticas mal informadas pueden reproducir desigualdades o dejar grupos enteros sin protección.
- **Base para estadísticas, memoria y análisis:** las bases de datos permiten construir estadísticas nacionales, identificar patrones de violencia, analizar tendencias y producir conocimiento para organismos públicos, academia y comunidad internacional. Estos registros se integran también en procesos de memoria, archivística y verdad histórica.

Así, los sistemas de registro de víctimas deben ser entendidos como artefactos sociotécnicos que median la relación entre hechos de violencia y las decisiones del Estado sobre ellos.

2.3.3. INFRAESTRUCTURAS DE INFORMACIÓN COMO PRODUCTORAS DE REALIDAD

Desde la perspectiva de los estudios de infraestructura y sociología del conocimiento, las bases de datos que documentan violaciones de derechos humanos son más que soportes técnicos: producen realidad institucional y política. Este carácter performativo se expresa en tres dimensiones:

- **Lo que se ve y lo que queda fuera:** cada campo, codificación y formulario define qué información existe institucionalmente. Si un tipo de daño no tiene campo propio, si una categoría es demasiado amplia o si no se registra determinada variable, ese aspecto de la experiencia desaparece del circuito institucional.
- **Quién cuenta como víctima:** los criterios de clasificación (por tipo de hecho, entidad responsable, nivel de daño) influyen en qué casos son considerados

violaciones, cuáles son priorizados y cómo se distribuyen recursos o medidas de reparación. La infraestructura informática condiciona el acceso a derechos.

- **Necesidad de estándares fuertes de calidad y seguridad:** en sistemas sensibles, errores técnicos (duplicidades, inconsistencias, pérdidas de datos), no son simplemente fallas operativas, estas pueden afectar procesos judiciales, impedir reparaciones o generar revictimización. Por ello, las bases de datos requieren estándares rigurosos de:
 - ❖ calidad de datos (precisión, completitud, consistencia, actualidad, validez);
 - ❖ gobernanza y trazabilidad (propiedad del dato, roles, metadatos, auditoría);
 - ❖ seguridad (CID, controles técnicos, registro de accesos, cifrado).

La infraestructura de información es, por tanto, inseparable de la protección de derechos: la forma en que se diseña y opera un sistema de registro influye directamente en la capacidad del Estado para cumplir sus obligaciones internacionales.

2.4. BASES DE DATOS, PRINCIPIOS Y BUENAS PRÁCTICAS

En términos generales, se entiende por dato una representación simbólica de un hecho, evento u observación (por ejemplo, una fecha de detención, un diagnóstico médico o un identificador de causa judicial), mientras que la información corresponde a los datos interpretados en un contexto, que permiten responder preguntas específicas y apoyar la toma de decisiones (Davenport, 1997). En otras palabras, los datos constituyen la materia prima, mientras que la información representa el producto derivado de su análisis, interpretación y uso.

Una base de datos puede definirse como un conjunto de datos relacionados, organizado de manera estructurada y gestionado por un Sistema de Gestión de Bases de Datos (SGBD o DBMS) que permite su almacenamiento, consulta y actualización de forma eficiente y segura (Date, 2004; Elmasri & Navathe, 2015). Los SGBD proporcionan mecanismos de control de acceso, transaccionalidad, respaldo y recuperación que garantizan la integridad y disponibilidad de los registros, convirtiéndose en un componente esencial para la gestión de información institucional.

En los entornos administrativos y gubernamentales, predominan las bases de datos relacionales, que modelan la información mediante tablas formadas por filas (casos) y columnas (atributos), vinculadas a través de claves primarias y foráneas. Este modelo relacional favorece la integridad referencial y la consistencia de los datos, reduciendo duplicidades y errores lógicos. No obstante, la coexistencia de sistemas heredados (legacy systems), hojas de cálculo y bases documentales ha impulsado la adopción de enfoques híbridos que combinan bases relacionales y NoSQL, especialmente cuando se requiere flexibilidad en el manejo de información semiestructurada (Elmasri & Navathe, 2015).

Desde una perspectiva técnica, el diseño y operación de bases de datos se rige por un conjunto de principios fundamentales:

- **Integridad y consistencia:** la base de datos debe mantener reglas que impidan estados inválidos y aseguren coherencia entre las relaciones definidas. La integridad referencial garantiza que los datos dependientes conserven correspondencia con las entidades principales, evitando registros huérfanos o inconsistentes.
- **Propiedades ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad):** definen el comportamiento esperado de las transacciones en bases de datos.
 - ❖ Atomicidad: las operaciones se ejecutan completamente o no se ejecutan.
 - ❖ Consistencia: cada transacción deja a la base en un estado válido.
 - ❖ Aislamiento: las transacciones concurrentes no interfieren entre sí.
 - ❖ Durabilidad: los cambios confirmados persisten incluso ante fallas del sistema (Date, 2004).
- **Normalización:** proceso de diseñar esquemas de tablas que reduzcan redundancias y anomalías de actualización, mejorando la integridad y eficiencia de las consultas. La normalización mejora la eficiencia, integridad y mantenibilidad del sistema, permitiendo representar entidades y relaciones de forma óptima.
- **Calidad de datos:** refiere a la precisión, completitud, consistencia, actualidad y validez de la información registrada (DAMA International, 2017). Mantener altos estándares de calidad permite obtener resultados confiables y comparables entre distintos sistemas. La información almacenada debe ser precisa, completa, actualizada, consistente y oportuna.

Estos principios se operacionalizan mediante un conjunto de buenas prácticas de diseño y administración de bases de datos, entre las que destacan:

- Definir identificadores únicos y estables para las entidades principales (personas, eventos, instituciones).
- Documentar la semántica y finalidad de cada campo mediante metadatos.
- Restringir los tipos de datos para evitar ambigüedades y errores de formato (por ejemplo, fechas heterogéneas o valores nulos no controlados).
- Implementar reglas de validación y restricciones de integridad directamente en el SGBD, además de las verificaciones aplicativas.

- Mantener registros de auditoría (logs) que permitan rastrear modificaciones, usuarios y fechas de actualización.
- Establecer políticas claras de respaldo, recuperación y retención de datos.

Estas prácticas constituyen la base técnica sobre la cual se construyen los sistemas de información institucionales.

2.5. GOBERNANZA DE DATOS

La gobernanza de datos constituye el conjunto de políticas, normas, roles, procesos y tecnologías que aseguran que los datos sean gestionados como un activo estratégico dentro de una organización. Su propósito central es garantizar la calidad, seguridad, disponibilidad y trazabilidad de los datos, de modo que puedan respaldar decisiones informadas, auditorías y políticas públicas basadas en evidencia (DAMA International, 2017). En otras palabras, la gobernanza de datos define quién puede hacer qué, con qué datos, bajo qué circunstancias y utilizando qué métodos, dentro de un marco normativo y tecnológico formalizado.

Desde una perspectiva de la ingeniería de datos², la gobernanza actúa como la capa superior del ciclo de vida de la información, sobre la cual se sustentan disciplinas operativas como la gestión de metadatos, la arquitectura de información, la calidad de datos, la seguridad de la información y la interoperabilidad de sistemas. El modelo propuesto por DAMA-DMBOK2 distingue entre *Data Governance* (nivel estratégico) y *Data Management* (nivel táctico), siendo la primera responsable de establecer las directrices y políticas de gestión, y la segunda encargada de su implementación práctica mediante tecnologías, procedimientos y controles específicos.

En este marco, la Gobernanza de Datos involucra cuatro componentes esenciales:

- **Políticas y marcos normativos:** define principios y estándares de gestión de datos, alineados con marcos internacionales (ISO/IEC 27001, DAMA-DMBOK2, NIST 800-53) y legislación nacional (Ley N° 21.180 y Ley N° 21.719).
- **Roles y responsabilidades:** establece funciones institucionales como *Data Owner* (propietario del dato), *Data Steward* (custodio) y *Data Custodian* (responsable técnico), garantizando la rendición de cuentas sobre el ciclo de vida de la información.

²IBM define la ingeniería de datos como la práctica de diseñar y construir sistemas para la agregación, el almacenamiento y el análisis de datos a escala.

<https://www.ibm.com/es-es/think/topics/data-engineering>

- **Procesos de gestión:** comprenden la adquisición, almacenamiento, control de calidad, clasificación y eliminación de datos, asegurando consistencia y trazabilidad en sistemas heterogéneos.
- **Herramientas tecnológicas:** incluyen catálogos de datos, repositorios de metadatos, sistemas de control de acceso, y mecanismos de monitoreo y auditoría que permiten la aplicación efectiva de las políticas definidas.

2.6. GESTIÓN DE LA INFORMACIÓN Y BUENAS PRÁCTICAS

La gestión de la información (Information Management) comprende el conjunto de procesos, metodologías y herramientas orientadas a garantizar que los datos generados, almacenados y utilizados por una organización sean accesibles, confiables, trazables y útiles a lo largo de todo su ciclo de vida. Desde una perspectiva de ingeniería, constituye una disciplina transversal que conecta el diseño de bases de datos, la arquitectura de información, la seguridad y la gobernanza organizacional (Davenport, 1997; Choo, 2002).

La gestión efectiva de la información no se limita al almacenamiento, sino que abarca la planificación, adquisición, procesamiento, mantenimiento, distribución y disposición final de los datos, asegurando que estos respalden de manera eficiente los procesos institucionales. Para ello, se requiere una infraestructura técnica y procedimental que establezca controles sobre calidad, integridad, acceso, preservación y eliminación segura de la información.

2.6.1. CICLO DE VIDA DE LA INFORMACIÓN

El ciclo de vida de la información describe las etapas que atraviesa un dato desde su creación hasta su eliminación definitiva. La Guía para la Gestión de Datos de la Administración del Estado (MGDE) (División de Gobierno Digital, 2023) y los marcos internacionales como DAMA-DMBOK2 establecen seis fases principales:

1. **Creación o captura:** corresponde a la generación inicial del dato, ya sea por ingreso manual, sensores, formularios digitales o integraciones automáticas. En esta etapa se definen los formatos, tipos y reglas de validación iniciales.
2. **Almacenamiento y organización:** implica la estructuración de los datos en bases relacionales, documentales o híbridas, con mecanismos de control de acceso y políticas de respaldo.
3. **Uso y procesamiento:** los datos son consultados, transformados o combinados para generar información útil; aquí se aplican reglas de integridad, normalización y consistencia.

4. **Intercambio y publicación:** se habilita la interoperabilidad mediante APIs, catálogos de datos o servicios web normalizados, siguiendo estándares de formato y seguridad.
5. **Preservación:** se resguarda la información en soportes duraderos y auditables, asegurando su integridad digital frente a obsolescencia tecnológica o corrupción de archivos.
6. **Eliminación o disposición final:** comprende la depuración o destrucción segura de datos obsoletos, conforme a políticas internas, normativas legales y criterios de retención definidos.

El control de cada fase requiere políticas de gestión documentadas, procedimientos operativos y trazabilidad verificable de los cambios efectuados sobre los datos (logging y versionamiento).

2.6.2. METADATOS Y TRAZABILIDAD

Los metadatos constituyen la descripción estructurada de los datos: identifican su origen, significado, formato, propietario, versión y condiciones de uso. En ingeniería de datos, permiten gestionar la semántica y el contexto de la información, habilitando su reutilización e interoperabilidad.

Una correcta gestión de metadatos facilita:

- La catalogación y búsqueda eficiente de información dentro de grandes volúmenes de datos.
- La trazabilidad, es decir, la capacidad de reconstruir el flujo completo del dato: quién lo generó, quién lo modificó y en qué condiciones se utilizó.
- La auditoría y el cumplimiento normativo, ya que cada cambio sobre la información puede ser verificado y justificado.

Técnicamente, los metadatos pueden almacenarse en repositorios especializados (data catalogs o metadata repositories) o integrarse dentro del propio modelo de datos mediante tablas de auditoría. Su gestión automatizada es un requisito fundamental en sistemas complejos o distribuidos, especialmente cuando existen múltiples fuentes de información y distintos niveles de acceso.

2.6.3. CALIDAD DE LA INFORMACIÓN

La calidad de la información determina el valor analítico y la confiabilidad operativa de un sistema. Según DAMA International (2017), puede evaluarse mediante varias dimensiones;

en esta memoria se enfatizan cinco que son especialmente relevantes para bases de datos de víctimas:

- **Precisión (accuracy):** se refiere al grado en que los datos almacenados reflejan de manera fiel la realidad que representan. Un dato es preciso cuando su valor coincide con la situación real observada. Desde la ingeniería de datos, mejorar la precisión implica definir reglas de validación en el SGBD (formatos, rangos permitidos, checks); establecer mecanismos de contraste con fuentes oficiales (por ejemplo, tablas de referencia de comunas, tribunales, instituciones); incorporar procesos de revisión y corrección de datos con apoyo de usuarios expertos.
- **Complejitud (completeness):** mide el grado en que los registros contienen todos los campos necesarios para cumplir adecuadamente su función. No se trata solo de que los campos no estén vacíos, sino de que la información considerada “obligatoria” efectivamente exista. Técnicamente, la completitud se mejora mediante definición explícita de campos obligatorios (NOT NULL, restricciones de integridad, reglas de negocio); formularios de captura que no permitan avanzar sin completar información crítica; indicadores periódicos que midan porcentaje de registros con datos faltantes en campos clave y disporen acciones de corrección.
- **Consistencia (consistency):** alude a la coherencia interna y externa de los datos, es decir, que no existan contradicciones entre campos de un mismo registro ni entre sistemas que comparten información. Un conjunto de datos puede estar completo pero ser inconsistente. Desde la perspectiva de diseño y operación de bases de datos, la consistencia se asegura mediante la integridad referencial (claves foráneas, restricciones entre tablas); reglas de negocio implementadas en el SGBD (constraints, triggers) que eviten combinaciones imposibles de estados; procesos de reconciliación entre sistemas (ETL, sincronización, controles de duplicidad) cuando existe más de una fuente para la misma entidad.
- **Actualidad (timeliness):** mide en qué medida los datos se encuentran actualizados de acuerdo con la frecuencia requerida por los procesos que los utilizan. Un dato puede ser preciso al momento de su captura, pero puede desactualizarse si no se mantiene. Desde el punto de vista técnico y organizacional, la actualidad se mejora mediante definir las ventanas temporales máximas para la actualización de ciertos campos (por ejemplo, plazo máximo para registrar un evento desde su ocurrencia); implementar procesos de carga y sincronización periódica (jobs, ETL programado) con trazabilidad de fechas de actualización; monitorear indicadores como “edad de los datos” o “tiempo promedio de actualización de estados”.
- **Validez (validity):** se refiere al grado en que los valores almacenados cumplen con las reglas de formato, tipo de dato, dominio permitido y rangos aceptables

definidos para cada campo. Un dato puede ser completo y reciente, pero inválido (por ejemplo, un RUT con formato incorrecto). Técnicamente, la validez se sostiene mediante tipos de datos adecuados (DATE, INTEGER, BOOLEAN, enumeraciones controladas) en lugar de campos genéricos tipo texto; restricciones de dominio (listas de valores permitidos, tablas de referencia, check constraints); validaciones en la capa de aplicación que se complementen con controles en el SGBD, evitando que datos inválidos ingresen al sistema.

Garantizar estas dimensiones implica implementar mecanismos de validación automática, control de versiones, auditorías de integridad y políticas de saneamiento de datos (data cleansing). Además, los SGBD deben permitir restricciones de integridad referencial, *triggers* y procedimientos almacenados que refuercen la consistencia interna.

2.6.4. BUENAS PRÁCTICAS EN LA GESTIÓN DE INFORMACIÓN

La correcta gestión de información dentro de una base de datos requiere la aplicación sistemática de buenas prácticas técnicas, entre las cuales destacan:

- **Definir políticas de retención y disposición de información:** establecer periodos de conservación y métodos de eliminación segura (borrado criptográfico o sobreescritura múltiple).
- **Implementar controles de versionamiento:** mantener historiales de cambios y versiones previas de registros críticos.
- **Asegurar interoperabilidad semántica y sintáctica:** usar formatos estructurados (JSON, XML, CSV estandarizado) y codificaciones consistentes (UTF-8) para permitir integración entre sistemas.
- **Aplicar procedimientos de respaldo incremental y verificación de integridad:** pruebas periódicas de restauración para validar la confiabilidad del almacenamiento.
- **Monitorear indicadores de calidad:** generar métricas periódicas sobre duplicidad, errores de validación y campos nulos.
- **Automatizar procesos ETL (Extract, Transform, Load):** garantizar consistencia y control de errores en la migración y consolidación de datos.
- **Mantener documentación técnica actualizada:** esquemas, diagramas entidad-relación, diccionarios de datos y matrices de flujo deben formar parte del repositorio institucional.

2.7. SEGURIDAD DE LA INFORMACIÓN Y BUENAS PRÁCTICAS EN BASES DE DATOS

La seguridad de la información puede definirse como el conjunto de medidas técnicas, organizacionales y procedimentales orientadas a proteger los activos de información, garantizando su confidencialidad, integridad y disponibilidad (CID):

- **Confidencialidad:** implica que la información sólo puede ser accedida por sujetos (usuarios, procesos o sistemas) debidamente autorizados.
- **Integridad:** se refiere a la protección de la exactitud y completitud de los datos frente a modificaciones no autorizadas o errores.
- **Disponibilidad:** asegura que los datos y servicios estén accesibles cuando se requieran, dentro de los niveles de servicio establecidos.

Estos tres principios, ampliamente reconocidos en la literatura y en estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002:2022, constituyen el eje sobre el cual se diseñan e implementan controles de seguridad en sistemas de información y, en particular, en bases de datos. Suele añadirse la **autenticación** (verificación de la identidad de usuarios o sistemas) y la **trazabilidad** (registro y auditoría de acciones sobre los datos), aspectos clave para el control y la rendición de cuentas.

2.7.1. RIESGOS TÍPICOS EN BASES DE DATOS CON DATOS SENSIBLES

Las bases de datos que almacenan información sensible (por ejemplo, datos personales, antecedentes médicos, información judicial o identificadores únicos), están expuestas a una serie de riesgos recurrentes desde la perspectiva de la seguridad de la información. Entre los más relevantes se pueden destacar:

- **Acceso no autorizado:**
 - ❖ Uso indebido de credenciales legítimas (robo de contraseñas, reutilización de claves débiles).
 - ❖ Cuentas con privilegios excesivos o mal gestionados.
 - ❖ Falta de separación de funciones entre administración, desarrollo y operación.
- **Divulgación o filtración de información (*data leakage*):**
 - ❖ Configuraciones inseguras en servicios de bases de datos expuestos a internet.
 - ❖ Copias de respaldo sin cifrado o almacenadas en medios no controlados.
 - ❖ Exportaciones masivas de datos sin controles de autorización ni registro.

- **Modificación o destrucción de datos:**
 - ❖ Actualizaciones o eliminaciones accidentales por errores humanos.
 - ❖ Modificaciones maliciosas de registros (fraude, manipulación de evidencias).
 - ❖ Ataques de ransomware que cifran bases completas o sus respaldos.
- **Explotación de vulnerabilidades técnicas:**
 - ❖ Ataques de SQL Injection y otros tipos de inyección en la capa de aplicación.
 - ❖ Fallas de configuración en el DBMS (puertos abiertos, cuentas por defecto, servicios innecesarios habilitados).
 - ❖ Falta de parcheo y actualización de software.
- **Pérdida de disponibilidad:**
 - ❖ Fallas de hardware o almacenamiento sin planes de contingencia.
 - ❖ Ataques de denegación de servicio (DoS) dirigidos al servidor de base de datos.
 - ❖ Problemas de capacidad o saturación por cargas no planificadas.
- **Uso inadecuado de datos en entornos no productivos:**
 - ❖ Replicación de bases con datos reales para pruebas o desarrollo.
 - ❖ Acceso de perfiles no autorizados a información sensible en ambientes de QA o laboratorio.

La gestión de estos riesgos requiere una aproximación sistemática basada en gestión de riesgos, donde se identifiquen activos, amenazas, vulnerabilidades e impactos, para luego seleccionar e implementar controles adecuados.

2.7.2. CONTROLES CLÁSICOS EN SEGURIDAD DE BASES DE DATOS

Para mitigar los riesgos descritos, la ingeniería de sistemas de información dispone de un conjunto de controles de seguridad ampliamente aceptados y aplicables específicamente a bases de datos:

- **Autenticación y autorización:**
 - ❖ Implementación de mecanismos robustos de autenticación (contraseñas fuertes, autenticación multifactor cuando corresponda).
 - ❖ Definición de roles y perfiles de acceso basados en el principio de mínimo privilegio.
 - ❖ Uso de *Role-Based Access Control* (RBAC) o modelos similares para asignar permisos de forma centralizada y controlada.

- **Gestión de cuentas y privilegios:**
 - ❖ Deshabilitar cuentas por defecto y credenciales genéricas del DBMS.
 - ❖ Revisión periódica de permisos y revocación de accesos innecesarios.
 - ❖ Separación de funciones entre administradores de base de datos, desarrolladores y usuarios finales.
- **Cifrado y protección de datos:**
 - ❖ Cifrado en reposo (en discos, respaldos, archivos de datos y *logs*) para proteger información ante pérdida o robo de soportes físicos.
 - ❖ Cifrado en tránsito mediante protocolos seguros (TLS/SSL) entre aplicaciones y servidores de base de datos.
 - ❖ Técnicas de enmascaramiento (*masking*) y pseudonimización para entornos de prueba o análisis donde no se requieran datos reales.
- **Registro de auditoría (*logging*) y monitoreo:**
 - ❖ Activación de *logs* de actividad en el SGBD para registrar accesos, consultas sensibles, modificaciones y operaciones administrativas.
 - ❖ Integración de estos registros con sistemas de correlación y monitoreo de eventos (SIEM) para detectar patrones anómalos.
 - ❖ Definición de umbrales y alertas para accesos inusuales, consultas masivas o intentos reiterados de autenticación fallida.
- **Respaldo, recuperación y continuidad operacional:**
 - ❖ Políticas de respaldo periódico (completo, incremental, diferencial) con verificación de integridad.
 - ❖ Pruebas regulares de restauración para asegurar que los planes de recuperación son efectivos.
 - ❖ Definición de estrategias de alta disponibilidad (réplicas, clustering) según los requisitos de continuidad del negocio.
- **Segregación de ambientes y datos:**
 - ❖ Separación estricta entre ambientes de desarrollo, pruebas y producción.
 - ❖ Uso de conjuntos de datos anonimizados o sintéticos en entornos no productivos.
 - ❖ Restricción del acceso directo a la base de datos de producción, priorizando el acceso mediante servicios y APIs controladas.
- **Gestión de vulnerabilidades y configuración segura:**
 - ❖ Aplicación oportuna de parches de seguridad del sistema operativo y del SGBD.

- ❖ Configuración segura (deshabilitar servicios innecesarios, limitar interfaces de red expuestas, configurar correctamente timeouts y límites de conexión).
- ❖ Realización periódica de pruebas de penetración y escaneos de vulnerabilidades focalizados en la capa de datos.

Estos controles deben documentarse en políticas de seguridad de la información, integrarse a los procesos de operación y soporte, y revisarse periódicamente como parte de un ciclo de mejora continua. Su evaluación se articula en este trabajo con las normas ISO/IEC 27001 y 27002:2022, desarrolladas en las siguientes secciones.

2.8. MARCO DAMA Y BUENAS PRÁCTICAS EN LA GESTIÓN DE LA INFORMACIÓN

El marco DAMA-DMBOK2 (Data Management Body of Knowledge, segunda edición) constituye el estándar de referencia internacional más completo para la gestión profesional de datos. Desarrollado por DAMA International (Data Management Association), este modelo proporciona un marco conceptual que define los principios, funciones, roles, áreas de conocimiento y buenas prácticas necesarias para administrar los datos como un activo estratégico dentro de cualquier organización (DAMA International, 2017).

A diferencia de los enfoques exclusivamente tecnológicos, el marco DAMA establece una visión sistémica y de ingeniería de la gestión de datos, integrando dimensiones organizacionales, arquitectónicas, de calidad, seguridad y gobernanza. A continuación se describen cada una de estas áreas.

2.8.1. DATA GOVERNANCE (GOBERNANZA DE DATOS)

La gobernanza de datos constituye la capa estratégica del modelo DAMA. Su propósito es establecer un marco de principios, políticas, estándares, roles y procesos que aseguren que los datos sean gestionados de manera coherente, ética y conforme a los objetivos de la organización. Desde un punto de vista técnico, la gobernanza define las reglas del juego: quién es responsable de cada conjunto de datos, bajo qué condiciones puede ser accedido, cómo se controla su calidad y cómo se mide su valor dentro del negocio o institución. En ingeniería de datos, este dominio se operacionaliza mediante la creación de comités de gobernanza, diccionarios de datos, políticas de seguridad, y mecanismos de auditoría y trazabilidad. Su función es garantizar que los activos de datos no dependan de decisiones *ad-hoc*, sino de políticas consistentes y medibles.

2.8.2. DATA ARCHITECTURE (ARQUITECTURA DE DATOS)

La arquitectura de datos describe la estructura lógica y física de los sistemas que almacenan, procesan y distribuyen información dentro de la organización. Su objetivo es diseñar un entorno de información coherente, escalable y alineado con las necesidades operativas y analíticas de la institución. Comprende la definición de modelos de datos conceptuales, lógicos y físicos, los flujos de información entre sistemas, y las reglas de interoperabilidad entre aplicaciones.

En términos técnicos, una arquitectura de datos bien diseñada permite evitar redundancia e inconsistencia de datos entre sistemas; optimizar consultas y transacciones mediante esquemas normalizados o desnormalizados según el caso; integrar sistemas heterogéneos mediante interfaces estandarizadas (APIs, conectores o middleware) y documentar los modelos mediante diagramas entidad-relación, catálogos de metadatos y repositorios centralizados.

Este dominio actúa como la “capa estructural” del ecosistema de información, sobre la cual se implementan los procesos de almacenamiento, seguridad y análisis.

2.8.3. DATA MODELING AND DESIGN (MODELADO Y DISEÑO DE DATOS)

El modelado y diseño de datos se enfoca en la representación formal de los objetos de información y sus relaciones. Incluye desde el modelado conceptual (representación semántica de entidades y relaciones) hasta el diseño físico (estructuras de almacenamiento en tablas, índices o colecciones).

Sus objetivos son garantizar integridad y consistencia de los datos mediante reglas y restricciones adecuadas, reducir redundancias mediante la normalización (formas normales); facilitar la trazabilidad entre modelos conceptuales, lógicos y físicos y soportar tanto operaciones transaccionales (OLTP) como analíticas (OLAP).

En el contexto estatal o institucional, el modelado de datos permite representar con precisión entidades críticas (como personas, instituciones, hechos o casos), y establecer relaciones verificables entre ellas. El cumplimiento de estándares de diseño asegura interoperabilidad y sostenibilidad técnica a largo plazo.

2.8.4. DATA STORAGE AND OPERATIONS (ALMACENAMIENTO Y OPERACIONES DE DATOS)

Este dominio aborda la implementación, mantenimiento y administración operativa de las bases de datos y de la infraestructura subyacente. Incluye actividades como instalación, configuración, optimización de rendimiento, respaldo, recuperación y monitoreo.

Los componentes técnicos clave son sistemas de Gestión de Bases de Datos (SGBD): relacionales (PostgreSQL, MySQL, Oracle) o NoSQL (MongoDB, Cassandra); gestión de rendimiento: índices, particionamiento, *tuning* de consultas y administración de concurrencia; respaldo y recuperación (Backup & Recovery); políticas de continuidad operativa y restauración ante fallas y automatización de tareas rutinarias y uso de *schedulers*, *scripts* o herramientas de orquestación (por ejemplo, Airflow o cron jobs).

El objetivo final es asegurar la disponibilidad, consistencia y resiliencia de los datos frente a fallas técnicas o eventos catastróficos.

2.8.5. DATA SECURITY (SEGURIDAD DE DATOS)

La seguridad de datos garantiza la protección de los activos de información frente a accesos no autorizados, pérdida, corrupción o uso indebido. Se basa en los tres pilares fundamentales: Confidencialidad, Integridad y Disponibilidad (CID), a los que se suman autenticidad y trazabilidad.

Las estrategias técnicas incluyen cifrado en reposo y en tránsito, enmascaramiento y anonimización; control de acceso basado en roles (RBAC) y privilegios mínimos; registro de auditoría y monitoreo de eventos (SIEM) y planes de recuperación ante desastres (DRP) y respaldos verificados.

Este dominio es transversal a todos los demás, dado que la seguridad debe integrarse en el ciclo de vida del dato. Se relaciona directamente con las normas ISO/IEC 27001 y 27002:2022, que proporcionan el marco formal de controles de seguridad.

2.8.6. DATA INTEGRATION AND INTEROPERABILITY (INTEGRACIÓN E INTEROPERABILIDAD DE DATOS)

La integración de datos se refiere a los procesos que permiten combinar información procedente de distintas fuentes en una vista coherente y unificada. En entornos complejos (como la administración pública), la interoperabilidad es un desafío crítico debido a la coexistencia de sistemas heterogéneos y marcos legales distintos.

Las principales técnicas incluyen procesos ETL (Extract, Transform, Load): extracción, limpieza, transformación y carga de datos en almacenes o repositorios centrales; APIs y servicios web (REST, SOAP): mecanismos normalizados para intercambio de información; mensajería y colas de eventos (Kafka, RabbitMQ): integración en tiempo real y estándares de interoperabilidad (JSON-LD, XML Schema, RDF, DCAT).

Una integración efectiva mejora la consistencia de la información, reduce duplicidades y habilita el análisis transversal entre instituciones, siendo esencial en proyectos de transformación digital del Estado (Ley 21.180).

2.8.7. DOCUMENT AND CONTENT MANAGEMENT (GESTIÓN DE DOCUMENTOS Y CONTENIDOS)

Este dominio aborda la gestión de información no estructurada, que incluye documentos de texto, archivos multimedia, imágenes, formularios escaneados y registros en formato libre. Sus objetivos son garantizar la preservación, disponibilidad, trazabilidad y control de versiones de dichos contenidos.

Las buenas prácticas incluyen implementación de sistemas de gestión documental (DMS) con control de acceso y metadatos; uso de estándares de preservación digital (PDF/A, OAIS, METS); indexación mediante motores de búsqueda (ElasticSearch, Solr) e integración con flujos de aprobación y firmas electrónicas.

En organizaciones públicas, este dominio es clave para mantener el valor probatorio de los documentos y cumplir con las leyes de transparencia, archivo y protección de datos personales.

2.8.8. REFERENCE AND MASTER DATA MANAGEMENT (GESTIÓN DE DATOS MAESTROS Y DE REFERENCIA)

La gestión de datos maestros (MDM) busca establecer una fuente única y autorizada de información sobre entidades críticas (como personas, instituciones, regiones o categorías). El objetivo es eliminar inconsistencias entre sistemas y asegurar que todos los procesos utilicen versiones actualizadas y coherentes de los mismos datos.

Los componentes principales son repositorios maestros centralizados o federados; procesos de deduplicación y reconciliación semántica; reglas de sincronización y publicación de cambios e identificadores únicos y consistentes que permitan correlacionar registros entre sistemas.

La correcta implementación de MDM reduce la fragmentación institucional y mejora la interoperabilidad, especialmente relevante en bases de datos de víctimas donde múltiples instituciones comparten información sensible sobre las mismas personas o hechos.

2.8.9. DATA WAREHOUSING AND BUSINESS INTELLIGENCE (ALMACENES DE DATOS E INTELIGENCIA DE NEGOCIOS)

El dominio de Data Warehousing y Business Intelligence (BI) se orienta a la consolidación, análisis y visualización de datos para la toma de decisiones estratégicas. Un Data Warehouse (DW) recopila información histórica desde múltiples fuentes, transformada y normalizada, para soportar consultas analíticas complejas.

Los componentes técnicos incluyen modelos *star schema* y *snowflake*; herramientas de explotación analítica (OLAP cubes, dashboards, reportes dinámicos), procesos de actualización incremental y control de versiones de datos históricos.

La BI complementa al DW mediante el uso de indicadores clave de desempeño (KPIs), tableros y análisis predictivos. En el contexto estatal, estos sistemas permiten generar estadísticas de víctimas, evaluar políticas de reparación o identificar patrones de violencia, siempre que los datos provengan de fuentes interoperables y seguras.

2.8.10. METADATA MANAGEMENT (GESTIÓN DE METADATOS)

La gestión de metadatos provee el contexto necesario para comprender, usar y compartir los datos de forma controlada. Los metadatos describen el significado, origen, formato, propietario, calidad y relaciones de los datos, y son esenciales para la trazabilidad y auditoría de la información.

Las principales prácticas incluyen creación de catálogos de datos corporativos accesibles para usuarios y técnicos; uso de repositorios de metadatos automatizados que capturan definiciones desde los propios sistemas; estándares de descripción (Dublin Core, ISO 11179) y mecanismos de versionamiento y control de cambios sobre definiciones de campos y estructuras.

Una gestión robusta de metadatos es requisito fundamental para lograr interoperabilidad, cumplimiento normativo y control de calidad.

2.8.11. DATA QUALITY MANAGEMENT (GESTIÓN DE CALIDAD DE DATOS)

El dominio de calidad de datos establece los procesos y métricas que aseguran que los datos sean precisos, completos, consistentes, actualizados y válidos. Su implementación requiere tanto controles automáticos como supervisión humana y auditorías periódicas.

Las actividades centrales incluyen definición de reglas de calidad (rangos válidos, formatos, relaciones obligatorias); monitoreo y métricas de calidad mediante dashboards o informes automáticos; procesos de limpieza (data cleansing) para corregir errores, eliminar duplicados y estandarizar valores; gestión de incidentes de calidad, con registro, análisis y corrección documentada y retroalimentación continua desde usuarios y sistemas analíticos.

El dominio de calidad de datos constituye el eje operativo del modelo DAMA, ya que toda decisión o política basada en información depende de la confiabilidad de los datos subyacentes.

2.9. ESTÁNDARES ISO/IEC 27001 Y 27002:2022

ISO/IEC 27001:2022 define los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI / ISMS). Es el estándar nuclear de la familia 27000 y es certificable. Su objetivo es que una organización gestione riesgos de seguridad de forma sistemática con un enfoque de mejora continua.

ISO/IEC 27002:2022, por su parte, no es certificable: proporciona la guía de implementación y buenas prácticas de los controles que el SGSI selecciona, estructurados por temas (organizacionales, de personas, físicos y tecnológicos). 27002:2022 detalla el “cómo” mientras 27001 fija el “qué requisitos”.

2.9.1. ARQUITECTURA DE ISO/IEC 27001 (ISMS) Y CICLO PDCA

ISO/IEC 27001 estructura el SGSI con un ciclo *Plan–Do–Check–Act* (PDCA) y se materializa mediante un conjunto de cláusulas normativas (4 a 10) que guían el diseño, implementación, operación y revisión del SGSI. A continuación se desarrollan estas cláusulas de manera integrada:

CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN

El SGSI se fundamenta en la comprensión detallada del contexto en que opera la organización a fin de identificar factores que pueden introducir riesgos, facilitar controles o limitar su implementación. Esto implica analizar condiciones internas y externas que influyen en la seguridad de la información, tales como el marco regulatorio aplicable, el nivel de madurez tecnológica, la estructura organizacional y los procesos existentes.

Asimismo deben identificarse las partes interesadas, que pueden incluir actores internos (unidades, áreas de negocio, equipos técnicos) y externos (clientes, proveedores, organismos fiscalizadores). Cada parte interesada posee expectativas y requisitos específicos relativos a la confidencialidad, integridad y disponibilidad de la información, los cuales deben ser reconocidos explícitamente.

También debe considerarse la definición del alcance del SGSI como una tarea crítica. En esta etapa se determinan los sistemas, procesos, ubicaciones, servicios y activos de información que estarán cubiertos por los controles del SGSI. Un alcance insuficiente puede dejar activos críticos fuera del sistema de gestión, generando brechas de seguridad.

Finalmente, la organización debe establecer los procesos necesarios para implementar, operar y mejorar el SGSI. Esto incluye definir interacciones, entradas, salidas, responsables, dependencias y criterios operativos.

CLÁUSULA 5: LIDERAZGO

Se exige que la seguridad de la información sea respaldada explícitamente por la alta dirección. El SGSI no puede existir únicamente como un conjunto de controles técnicos: requiere compromiso, directrices estratégicas y supervisión ejecutiva.

La dirección debe demostrar liderazgo mediante la asignación de recursos adecuados (humanos, tecnológicos y financieros), el establecimiento de una política de seguridad de la información, coherente con los objetivos y riesgos de la organización, el apoyo a auditorías internas y revisiones de desempeño, y la promoción de la mejora continua. La política debe definir el propósito del SGSI, los principios orientadores, los compromisos organizacionales y la alineación con requisitos legales y contractuales.

Asimismo, ISO 27001 exige definir formalmente roles y responsabilidades vinculados a la seguridad de la información. Esto incluye responsables de activos, administradores técnicos, encargados de implementar controles, supervisores del SGSI y autoridades para la toma de decisiones. Una estructura clara evita ambigüedades operativas y permite la trazabilidad de la gestión de seguridad.

CLÁUSULA 6: PLANIFICACIÓN

La planificación constituye el núcleo técnico del SGSI, pues en ella se define cómo se gestionarán los riesgos de seguridad de la información. La organización debe establecer un proceso sistemático para identificar activos de información, sus propietarios, su valor y sus dependencias; identificar amenazas asociadas a dichos activos (acceso no autorizado, alteración, pérdida, indisponibilidad, falla operativa, etc.); identificar vulnerabilidades que podrían ser explotadas (configuraciones débiles, controles insuficientes, fallos humanos, obsolescencia tecnológica); evaluar riesgos combinando probabilidad e impacto; definir criterios de aceptación de riesgo y priorizar acciones.

A partir de esta evaluación, la organización debe seleccionar los controles adecuados. Esta selección se formaliza en la Declaración de Aplicabilidad (*SoA, Statement of Applicability*), documento obligatorio que enumera todos los controles de ISO/IEC 27002:2022, indicando cuáles se aplican, su justificación y su estado de implementación. La *SoA* constituye una pieza central del SGSI, pues vincula el análisis de riesgos con los controles que se operarán.

Además, la organización debe establecer objetivos de seguridad medibles, consistentes con la política y proporcionales a los riesgos identificados. Estos objetivos orientan la planificación operativa y permiten evaluar el desempeño posterior.

CLÁUSULA 7: SOPORTE

El funcionamiento del SGSI depende de la disponibilidad de recursos adecuados. ISO 27001 exige que la organización asegure recursos humanos con competencias técnicas y de gestión; infraestructura tecnológica suficiente para operar los controles; herramientas de monitoreo y auditoría; presupuestos operativos adecuados.

La norma también resalta la importancia de asegurar las competencias del personal, mediante formación, experiencia documentada y capacitación continua. La falta de competencias suele ser uno de los principales vectores de incidentes de seguridad.

La concientización es otro componente esencial. Todos los usuarios deben comprender las políticas, los riesgos, las prácticas seguras y los procedimientos operativos, ya que el factor humano constituye una parte sustancial de la superficie de ataque.

A nivel organizacional, la comunicación debe ser clara y oportuna, incluyendo canales formales para reportar incidentes, solicitar permisos, coordinar controles o difundir actualizaciones.

Finalmente, la cláusula exige la gestión rigurosa de la información documentada, lo que incluye políticas, procedimientos, registros, bitácoras, inventarios de activos, informes de auditoría y evidencias de cumplimiento. Esta documentación permite demostrar trazabilidad, coherencia y conformidad con la norma.

CLÁUSULA 8: OPERACIÓN

La fase de operación es la ejecución material del SGSI. Aquí se implementan los controles seleccionados durante la planificación, y se realiza el tratamiento de riesgos conforme a los procedimientos establecidos.

La organización debe planificar y controlar las operaciones relacionadas con la seguridad, lo que incluye aplicar controles de acceso; monitorear registros de actividad; gestionar incidentes; asegurar la segregación de ambientes; revisar configuraciones técnicas; ejecutar procesos de respaldo y restauración; supervisar proveedores; y validar la eficacia de los controles técnicos.

Además, la organización debe mantener una evaluación continua del riesgo, actualizando su análisis cuando cambian las condiciones tecnológicas, operativas o normativas, o cuando aparecen nuevas amenazas.

La fase de operación también incluye la implementación efectiva del “tratamiento del riesgo”, que corresponde a la aplicación concreta de los controles (tecnológicos, organizacionales y físicos) necesarios para reducir los riesgos identificados a niveles aceptables.

CLÁUSULA 9: EVALUACIÓN DEL DESEMPEÑO

ISO 27001 exige medir y evaluar la eficacia del SGSI de forma continua. Para ello, la organización debe definir indicadores, métricas y métodos de análisis que permitan evaluar el cumplimiento de los objetivos de seguridad.

Las actividades de evaluación incluyen monitoreo y medición de la efectividad de controles; análisis de tendencias de incidentes; evaluación del estado de actualización de software; verificación de tiempos de recuperación; revisión de permisos y cuentas activas.

La auditoría interna es un componente formal de esta cláusula. Su finalidad es verificar el cumplimiento de requisitos, detectar desviaciones, revisar evidencias, evaluar riesgos residuales y promover mejoras.

Finalmente, la revisión por la dirección constituye un mecanismo de gobernanza mediante el cual los niveles ejecutivos evalúan el desempeño global del SGSI, toman decisiones sobre recursos, priorizan mejoras y aseguran la alineación estratégica con los objetivos de la organización.

CLÁUSULA 10: MEJORA

El SGSI debe incorporar un proceso permanente de mejora continua. La organización debe gestionar de manera formal las no conformidades, analizando sus causas, definiendo acciones correctivas y verificando su eficacia.

Las mejoras pueden surgir de auditorías, incidentes, cambios tecnológicos, nuevas amenazas, actualizaciones normativas o hallazgos de monitoreo. La cláusula 10 posiciona al SGSI como un sistema vivo, adaptable y resiliente, capaz de evolucionar con el entorno y los riesgos emergentes.

2.9.2. 27002: ESTRUCTURA TEMÁTICA Y CONTROLES (ed. 2022)

La norma ISO/IEC 27002:2022 constituye el cuerpo de referencia para la implementación de controles de seguridad de la información en un Sistema de Gestión de Seguridad de la Información (SGSI). A diferencia de ISO/IEC 27001 (que establece los requisitos del SGSI), la 27002:2022 proporciona orientaciones prácticas, objetivos de control y métodos recomendados para la implementación de medidas técnicas, organizacionales, físicas y humanas.

La edición 2022 reorganizó y actualizó el catálogo de controles, reduciendo su número desde 114 a 93 controles, incorporando dominios emergentes como seguridad en la nube; monitoreo continuo; inteligencia de amenazas; configuración segura; borrado de datos; prevención de fuga de información (DLP); gestión de identidad robusta.

La norma estructura sus controles en cuatro grandes temáticas, cada una asociada a un conjunto de objetivos y lineamientos de implementación. A continuación, se explican de manera sistemática.

CONTROLES ORGANIZACIONALES

Este conjunto agrupa los controles que establecen la estructura administrativa, estratégica y documental necesaria para gestionar la seguridad de la información en toda la organización. Se enfocan en la creación de condiciones organizacionales que permitan gestionar riesgos, definir responsabilidades y asegurar el cumplimiento normativo. Las áreas más relevantes incluyen:

- **Políticas de seguridad de la información:** la organización debe desarrollar, aprobar, comunicar y revisar políticas que definan los principios rectores, roles, responsabilidades y lineamientos generales de seguridad.
- **Roles y responsabilidades:** se deben establecer estructuras organizacionales que definan claramente responsabilidades en la gestión de seguridad, propiedad de activos, gestión de incidentes y operación de controles.
- **Relación con terceros:** los proveedores y socios deben ser gestionados mediante acuerdos formales, cláusulas de seguridad, evaluaciones de riesgos y mecanismos de monitoreo. La subcontratación introduce riesgos que deben ser controlados sistemáticamente.
- **Clasificación y manejo de información:** la información debe clasificarse según su nivel de sensibilidad, lo que incluye reglas de etiquetado, manejo, almacenamiento, transmisión y eliminación acorde con dicha clasificación.
- **Gestión de continuidad de negocios:** incluye la elaboración de estrategias de continuidad, análisis de impacto (BIA), planes de continuidad, pruebas periódicas y mecanismos de recuperación frente a interrupciones.
- **Cumplimiento normativo y contractual:** la organización debe cumplir requisitos legales, regulatorios y contractuales aplicables a la protección de información, incluyendo auditorías, revisión documental y evidencias verificables.

En conjunto, estos controles establecen la base estructural del sistema de seguridad, garantizando que la organización opere bajo reglas formales y auditables.

CONTROLES DE PERSONAS

Este grupo se enfoca en los factores humanos, parte crítica de la superficie de riesgo de cualquier organización. Los controles abordan desde la selección de personal hasta la formación continua y gestión de su ciclo laboral. Las áreas clave son:

- **Selección y verificación:** antes de contratar personal con acceso a información, la organización debe verificar antecedentes, experiencia y aptitudes, de acuerdo con la sensibilidad de los activos que serán gestionados.
- **Acuerdos de confidencialidad:** la organización debe implementar programas de concientización periódicos, enfocados en amenazas, buenas prácticas, riesgos comunes y obligaciones relacionadas con la seguridad.
- **Responsabilidades durante el empleo:** el personal debe entender claramente sus obligaciones en relación con el manejo seguro de la información, incluyendo prácticas autorizadas, uso aceptable de sistemas y reportes de incidentes.
- **Término o cambio de funciones:** cuando un colaborador cambia de funciones o finaliza su labor, la organización debe asegurar la revocación oportuna de accesos y la devolución de activos, evitando riesgos residuales.

Estos controles fortalecen la dimensión humana del SGSI, reduciendo riesgos asociados a errores, negligencia o uso indebido de información.

CONTROLES FÍSICOS

Los controles físicos protegen los activos tangibles (instalaciones, equipos, servidores, medios de almacenamiento) contra daños, acceso indebido o interferencias. La seguridad física es complementaria a la seguridad lógica y constituye la primera línea de defensa en muchos escenarios. Las áreas más relevantes incluyen:

- **Zonas y perímetros seguros:** las instalaciones que albergan infraestructura crítica deben contar con restricciones de acceso físico, medidas de vigilancia, registros de entrada y sistemas de control.
- **Control de acceso físico:** los accesos deben ser limitados por mecanismos como tarjetas, biometría, supervisión o cerraduras, dependiendo de la criticidad del área.
- **Protección de equipos:** incluye disposiciones sobre condiciones ambientales (climatización, energía), ubicación segura de servidores, protección frente a incendios y resguardo contra robo o daños.

- **Gestión de oficinas remotas y teletrabajo:** las organizaciones deben implementar lineamientos claros sobre el uso seguro de dispositivos fuera de las instalaciones, manejo seguro de documentos y restricciones para trabajar con información sensible en entornos no controlados.

Estos controles permiten mitigar riesgos físicos que podrían comprometer la disponibilidad, integridad o confidencialidad de la información.

CONTROLES TECNOLÓGICOS

Constituyen la parte más extensa del estándar e incluyen controles aplicables a sistemas, aplicaciones, redes, criptografía, gestión de vulnerabilidades y desarrollo seguro. Son esenciales para proteger activos digitales en entornos complejos y distribuidos. Las principales categorías son:

- **Control de acceso lógico y gestión de identidades:** incluye autenticación robusta, política de contraseñas, gestión del ciclo de vida de las cuentas, control de privilegios y separación de funciones.
- **Criptografía:** define el uso de mecanismos criptográficos en tránsito y en reposo, incluyendo gestión de llaves, algoritmos aprobados, controles de intercambio seguro y procedimientos de destrucción de llaves.
- **Logging y monitoreo:** la organización debe generar, almacenar y revisar registros de actividad relevantes, detectando eventos anómalos, accesos no autorizados y fallas operativas. Los logs son un insumo fundamental para auditorías y análisis forense.
- **Gestión de vulnerabilidades:** incluye procesos para identificar, evaluar, priorizar y tratar vulnerabilidades mediante parches, configuraciones adecuadas y monitoreo continuo.
- **Seguridad en el desarrollo y adquisición:** los sistemas desarrollados o adquiridos deben cumplir principios de desarrollo seguro, revisión de código, pruebas de penetración, controles de cambios y verificación de integridad.
- **Seguridad de aplicaciones y bases de datos:** comprende medidas específicas como configuración segura de SGBD, sanitización, consultas parametrizadas, segregación entre ambientes y monitoreo de accesos privilegiados.

- **Copia de seguridad y recuperación:** incluye políticas de respaldo completo e incremental, pruebas de restauración, procedimientos de recuperación ante desastres y requisitos de disponibilidad.
- **Protección de redes y servicios:** define medidas para firewalling, segmentación de redes, sistemas de detección de intrusiones, gestión de tráfico y protección contra ataques.

Estos controles permiten la aplicación concreta de los requisitos del SGSI a la infraestructura tecnológica y constituyen el núcleo técnico de la seguridad de información.

2.10. MARCO NORMATIVO CHILENO APLICABLE A LA GESTIÓN DE BASES DE DATOS DE VÍCTIMAS

El tratamiento de información sensible en organismos estatales (en particular datos relativos a violaciones de derechos humanos, salud, antecedentes judiciales o identificación personal) se encuentra fuertemente regulado por el ordenamiento jurídico chileno. Para efectos de esta memoria, tres instrumentos normativos y técnicos son fundamentales: la Ley 21.180 sobre Transformación Digital del Estado, la Ley 21.719 de Protección de Datos Personales, y la Guía para la Gestión de Datos de la Administración del Estado (MGDE) elaborada por la División de Gobierno Digital.

Estos marcos regulan cómo deben diseñarse, administrarse y protegerse las bases de datos estatales que registran víctimas, y proporcionan criterios evaluativos para analizar las brechas existentes durante el estallido social y proponer mejoras.

2.10.1. LEY N°21.180 DE TRANSFORMACIÓN DIGITAL DEL ESTADO

La Ley 21.180 (2019) moderniza los procesos administrativos del Estado mediante la digitalización, interoperabilidad y gestión eficiente de información. Aunque su foco principal son los procedimientos administrativos, establece principios y obligaciones directamente aplicables a los sistemas de registro de víctimas. Entre sus aspectos relevantes se encuentran:

- **Digitalización y trazabilidad documental:** la ley obliga a que los procesos estatales generen documentos electrónicos con registro de origen, responsables y fecha, requisito directamente relacionado con la trazabilidad de datos en bases de víctimas. Para efectos de esta memoria, implica que los sistemas deberían permitir rastrear quién ingresó o modificó un dato sensible, cuándo y bajo qué autorización.
- **Interoperabilidad entre organismos públicos:** la ley ordena que los sistemas estatales intercambien información mediante plataformas seguras, estandarizadas y auditables. Este principio responde a uno de los problemas centrales

diagnosticados en el estallido social: la fragmentación de registros entre INDH, Fiscalía, SML, Carabineros, CVVI y organizaciones civiles.

- **Uso obligatorio de plataformas electrónicas oficiales:** el Estado debe adoptar sistemas homologados y con requisitos mínimos de seguridad, integridad y disponibilidad. Para bases de datos con víctimas, esto implica exigencias sobre respaldo electrónico, integridad de documentos, autenticación de funcionarios, almacenamiento seguro.
- **Validez probatoria de documentos electrónicos:** los registros deben ser íntegros, auditables y verificables para tener valor legal y administrativo. Esto refuerza la necesidad de controles ACID, logs, control de versiones y respaldo seguro en bases de datos de víctimas.

2.10.2. LEY N° 21.719 SOBRE PROTECCIÓN DE DATOS PERSONALES

La Ley 21.719 (2024–2025) moderniza el régimen de protección de datos personales en Chile, estableciendo un estándar alineado con referentes internacionales. Para el contexto de víctimas, esta es la ley más crítica, ya que clasifica muchos de los datos tratados durante el estallido social como datos sensibles. Entre sus aspectos conceptuales clave se encuentran:

- **Definición de datos sensibles:** la Ley establece como datos sensibles salud física y psicológica, vida sexual, antecedentes judiciales o policiales, datos biométricos y convicciones políticas o sociales, todos presentes en los registros de víctimas del estallido.
- **Principio de licitud y minimización:** los datos sólo pueden tratarse si existe base legal, consentimiento informado o interés público legítimo; además, sólo deben recopilarse los datos estrictamente necesarios para el propósito definido.
- **Principio de finalidad y limitación del uso:** los datos no pueden usarse para fines distintos a aquellos para los que fueron recolectados. En sistemas de víctimas, esto es crucial para prevenir filtraciones, usos indebidos o transferencias no autorizadas a otras agencias (por ejemplo, policiales o militares).
- **Deber de seguridad y responsabilidad proactiva:** las instituciones deben implementar medidas técnicas y organizativas apropiadas como cifrado, control de acceso, pseudonimización, registro de incidentes, pruebas de seguridad.

- **Notificación de brechas:** la ley obliga a informar incidentes de seguridad que afecten a titulares de datos. Esto es crucial en sistemas con datos extremadamente sensibles como lesiones, denuncias o identificadores personales.
- **Derechos del titular:** incluye el derecho del titular a acceso, rectificación, cancelación, oposición y portabilidad, que deben ser implementados en la arquitectura de datos y en los procesos de gestión de la información.

2.10.3. GUÍA PARA LA GESTIÓN DE DATOS DE LA ADMINISTRACIÓN DEL ESTADO

Es el estándar técnico más relevante para evaluar la madurez en gobernanza, interoperabilidad y calidad de datos en organismos públicos. Constituye el primer intento sistemático del Gobierno de Chile por unificar la gestión de datos entre todas las instituciones del Estado. Sus componentes clave incluyen:

- **Modelo de roles y responsabilidades:** define funciones de *Data Owner*, *Data Steward* y *Data Custodian*. Para sistemas de víctimas, es fundamental determinar quién es responsable del dato, quién lo administra, quién lo usa y quién lo resguarda.
- **Ciclo de vida del dato:** la guía establece seis etapas: creación, almacenamiento, uso, intercambio, preservación y eliminación. Este modelo se alinea con lo expuesto anteriormente y permite evaluar si las instituciones cumplen con estándares de gestión a lo largo de todo el ciclo de vida.
- **Metadatos institucionales:** la guía exige documentar origen del dato, responsable, semántica, fecha de actualización, formato y nivel de sensibilidad. Este componente es esencial en un entorno con registros fragmentados y definiciones semánticas dispares como el estallido social.
- **Catálogo de Datos y esquemas de interoperabilidad:** La guía propone que los organismos mantengan catálogos públicos cuando sea posible, y catálogos cerrados cuando existen restricciones de seguridad. En esta memoria se evaluará, por ejemplo, si la CVVI o el Ministerio mantienen esquemas documentados que faciliten la interoperación con INDH, SML o Ministerio Público.
- **Lineamientos de calidad de datos:** define indicadores mínimos de completitud, coherencia, unicidad y validez. Estos lineamientos ofrecen criterios objetivos para evaluar la calidad de los registros de víctimas en las bases analizadas.

2.11. CASO DE ESTUDIO: COMISIÓN DE VÍCTIMAS DE VIOLENCIA INSTITUCIONAL (CVVI)

La Comisión de Víctimas de Violencia Institucional (CVVI) es una instancia dependiente de la Subsecretaría de Derechos Humanos, perteneciente al Ministerio de Justicia y Derechos Humanos de Chile, cuyo mandato principal es documentar información relativa a víctimas de violencia institucional.

La Unidad de Documentación y Archivo, a la cual pertenece la contraparte institucional consultada para esta memoria, cumple un rol clave en los procesos de documentación, sistematización y resguardo de información. Su trabajo constituye la base sobre la cual se construyen procesos de registro, verificación, seguimiento y eventual entrega de antecedentes para fines judiciales, administrativos o de reparación.

2.11.1. ROL INSTITUCIONAL Y RELEVANCIA PARA EL REGISTRO DE VÍCTIMAS

La CVVI opera como un nodo estatal especializado en el procesamiento de información asociada a hechos de violencia institucional, lo cual incluye recepción y consolidación de antecedentes; clasificación y validación de información; coordinación con otras instituciones (INDH, Ministerio Público, Poder Judicial, SML); resguardo documental; análisis técnico para apoyo de decisiones administrativas y políticas públicas.

En el contexto del estallido social de 2019, la CVVI asumió un rol prioritario en el levantamiento de información sobre víctimas de lesiones, detenciones, violencia sexual, trauma ocular y otros tipos de vulneraciones asociadas a actuaciones de agentes del Estado.

2.12. NATURALEZA SOCIOTÉCNICA DEL PROBLEMA

La gestión de información sobre víctimas de violencia institucional es un fenómeno sociotécnico, donde las tecnologías de información (bases de datos, flujos documentales, sistemas de registro) se entrelazan con prácticas institucionales, criterios jurídicos y administrativos, requerimientos de derechos humanos, capacidades técnicas de funcionarios, limitaciones materiales y organizacionales.

El caso CVVI permite observar cómo estos elementos interactúan en situaciones reales: cómo se definen los campos, cómo se clasifican los hechos, cómo se garantiza la integridad del registro, bajo qué criterios se limita el acceso y cómo se resguarda la evidencia documental.

CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

3.1. ALCANCE DE LA INVESTIGACIÓN

Esta investigación se restringió al ecosistema sociotécnico de registro, gestión y resguardo de información utilizado por la Comisión de Víctimas de Violencia Institucional (CVVI), específicamente a los procesos y artefactos que conforman su infraestructura de información: la planilla maestra de casos, las planillas externas provenientes de otros organismos públicos, las carpetas digitales y físicas por caso, los repositorios institucionales utilizados para almacenar documentos, y las prácticas operativas de los equipos encargados de su administración.

Este ámbito fue seleccionado porque concentra los activos de información más críticos para el trabajo de la CVVI: registros de víctimas, antecedentes documentales con valor probatorio, comunicaciones oficiales y bases de datos que sostienen la verificación de hechos y la coordinación interinstitucional. Asimismo, se trata del espacio organizacional donde se encuentran las principales vulnerabilidades operativas que pueden afectar la calidad, trazabilidad, integridad y seguridad de los datos que sustentan las decisiones del Estado en materia de víctimas de violencia institucional.

A diferencia de un entorno TI tradicional centrado en data centers y equipamiento físico, el proceso evaluado en la CVVI se caracteriza por ser un proceso sociotécnico que combina prácticas documentales, flujos de colaboración interinstitucional y mecanismos de almacenamiento en entornos compartidos.

3.2. ACTIVIDADES DESARROLLADAS

Los principales hallazgos de esta investigación se obtuvieron mediante un proceso de levantamiento que combinó:

1. Entrevistas semiestructuradas con personal de la Unidad de Documentación y Archivo, responsable directo del registro y gestión de casos (ver Anexo A).
2. Revisión documental de procedimientos, planillas, estructuras de almacenamiento y flujos de trabajo internos (ver Anexo B).
3. Aplicación de un análisis de riesgos alineado con los requisitos de ISO/IEC 27001:2022 y los controles de ISO/IEC 27002:2022, considerando tanto dimensiones técnicas como organizacionales.

A partir de estas actividades se desarrollaron las siguientes tareas:

1. Levantamiento de activos de información y valoración de su criticidad (confidencialidad, integridad y disponibilidad).
2. Identificación de amenazas, vulnerabilidades y escenarios de riesgo asociados al uso de planillas, carpetas de caso, repositorios institucionales y cuentas de usuario.
3. Estimación de probabilidad, impacto y nivel de severidad para cada riesgo.
4. Determinación del riesgo aceptable considerando el contexto institucional, la sensibilidad de los datos y las capacidades operativas actuales.
5. Mapeo de riesgos altos y extremos a controles específicos de ISO/IEC 27002:2022, seleccionando aquellos que resultan viables y pertinentes para la CVVI.
6. Elaboración de un plan de mitigación, priorizando iniciativas de corto, mediano y largo plazo que permitan fortalecer la seguridad, continuidad y calidad de la información.

3.3. DESCRIPCIÓN DEL PROCESO DE REGISTRO Y GESTIÓN DE INFORMACIÓN

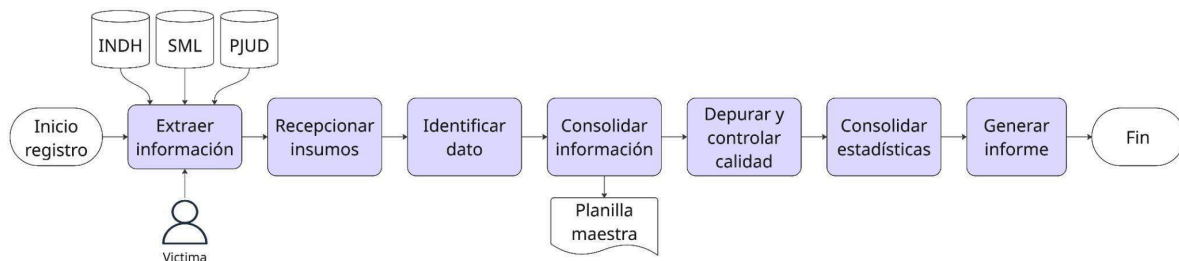


Figura 2: Proceso de registro y generación de productos CVVI.

Fuente: Elaboración propia.

El proceso evaluado abarca el conjunto de actividades mediante las cuales la CVVI recibe, registra, clasifica, consolida, analiza y resguarda información relativa a víctimas. La infraestructura de información involucrada incluye:

- la planilla maestra interna donde se consolida la información principal de cada caso;

- planillas externas provenientes de INDH, Ministerio Público, Poder Judicial, SML u otros organismos;
- carpetas documentales por caso (digitales y a veces físicas) que contienen oficios, fichas, antecedentes médicos, comunicaciones o registros probatorios;
- repositorios institucionales en unidades compartidas o servicios de almacenamiento oficial;
- cuentas de usuario, perfiles de acceso y prácticas de manejo cotidiano de documentos;
- sistemas de correo institucional y mecanismos informales de intercambio.

Este proceso constituye la base funcional para el trabajo de la CVVI y soporta sus obligaciones de análisis, registro, sistematización y producción de antecedentes administrativos y probatorios. Por ello, su integridad y seguridad son esenciales.

3.3.1. ENTRADAS DEL PROCESO

En coherencia con ISO/IEC 27001:2022, el proceso de registro y gestión de información recibe como entradas un conjunto de insumos provenientes de actividades organizacionales, técnicas y normativas, entre ellos:

Tabla 1: Entradas del proceso de registro y gestión de información de CVVI.

Desde	Entrada	Descripción
Poder Judicial	Documentos judiciales (sentencias, resoluciones, causas, expedientes, RUC)	Fuente principal del catastro, revisada manualmente y sistematizada por pasantes y equipo técnico. Da origen a validación, actualización y descubrimiento de casos nuevos.
Atención directa a personas	Fichas de atención y entrevistas	Información capturada durante orientación jurídica o psicosocial. Permite corregir, completar o actualizar registros existentes, con distintos grados de formalidad y calidad.
Organizaciones de víctimas	Nóminas, listados o antecedentes	Se utilizan para contraste, identificación de duplicados y búsqueda de casos no registrados previamente.
Consejo de Defensa del Estado	Planillas externas	Bases entregadas para cotejar datos, contrastar duplicados y actualizar el universo de casos.
Mesa o programa previo	Disco duros con respaldos, planillas heredadas, expedientes	Material recibido sin traspaso formal ni documentación estructurada; requiere arqueología y reconstrucción semántica.

Equipo interno	Planillas instrumentales, hojas auxiliares, notas	Herramientas internas de control de avance, asignación de casos, seguimiento de revisión y consolidación estadística para reportes.
Gestiones interinstitucionales	Minutas, correos, solicitudes	Trazas administrativas que permiten registrar actualizaciones, aclaraciones y derivaciones para completar información.
Documentación interna	Criterios, lineamientos, libro de códigos	Definiciones internas para estandarizar qué se considera caso, qué documentos son válidos, y cómo se registran los campos.

3.3.2. SALIDAS DEL PROCESO

El proceso genera varios productos que sirven como insumos para otras funciones de la CVVI y para organismos externos:

Tabla 2: Salidas del proceso de registro y gestión de información de CVVI.

Hacia	Salida	Descripción
Equipo de pasantes	Planillas auxiliares de revisión	Set de hojas intermedias creadas para limitar intervención directa sobre el catastro, controlar asignación de casos y registrar avance individual.
Coordinación de la Comisión	Reportes internos de avance	Consolidaciones periódicas sobre casos revisados, casos nuevos, calidad de datos y vacíos pendientes; sirven para justificar metas y carga operativa.
Subsecretaría / Gabinete	Minutas internas, consolidaciones, solicitudes	Productos administrativos derivados del catastro: cifras, listados, validaciones, argumentos de consistencia y documentos para toma de decisiones.
Instituciones externas	Fichas de derivación	Documentos formales para atención de casos, generados a partir del registro y revisión del catastro y la atención directa.
Auditoría interna del equipo	Planillas de depuración, duplicados, consistencia	Instrumentos intermedios creados para limpieza de datos, identificación de duplicados, diferencias de formato y control de calidad.
Proceso de gobernanza interna	Criterios, definiciones, reglas semánticas	Ajustes progresivos del libro de códigos, criterios de inclusión/exclusión, definición temporal del estallido y clasificación de hechos.

3.4. INVENTARIO DE ACTIVOS DE INFORMACIÓN

A partir de la entrevista y la revisión documental se identificaron y sistematizaron los principales activos de información involucrados en el proceso de registro y gestión documental. Este levantamiento responde al requisito establecido en la cláusula 8 de ISO/IEC 27001:2022, que exige planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información, lo cual incluye la identificación y documentación de los activos involucrados en el alcance del SGSI. Los atributos de cada activo (tipo, ubicación, responsable, soporte y personas autorizadas) fueron obtenidos directamente del personal de la CVVI en las entrevistas semiestructuradas detalladas en el Anexo A, y complementados con la revisión de la documentación interna disponible (Anexo B).

Tabla 3: Activos del proceso de registro y gestión de información de CVVI.

Nombre Activo	Código	Tipo	Ubicación	Responsable / Dueño	Soporte	Persona Autorizada para Manipular
Planilla Maestra de Casos	PMC	Base de Datos	Carpeta digital interna de la Comisión	Encargado/a de documentación	Digital	Equipo de documentación y análisis
Planillas Externas Recibidas desde Organismos	PEO	Documento	Correo institucional y carpeta de trabajo	Encargado/a documental	Digital	Equipo documental autorizado
Carpetas Documentales por Caso	CDC	Expediente	Archivo físico interno de la Comisión	Unidad de Documentación y Archivo	Físico y digital (mixto)	Equipo documental y encargado de archivo
Documentos Probatorios (fichas, informes, oficios)	DCP	Documento	Archivo físico y repositorio digital	Responsable documental	Físico y digital	Equipo documental; funcionarios autorizados
Digitalizaciones y Escaneos	DIG	Documento	Carpeta digital interna	Unidad de Documentación	Digital	Equipo documental
Base Estadística Consolidada (indicadores y conteos)	BEC	Base de Datos	Repositorio digital de trabajo	Coordinación documental	Digital	Equipo documental autorizado

Minutas Internas y Actas de Discusión	MIA	Documento	Carpeta de coordinación de la Comisión	Coordinación de la Comisión	Digital	Equipo documental y directivos autorizados
Correos Institucionales Asociados al Proceso	COR	Documento	Outlook institucional	Encargado/a documental	Digital	Equipo documental autorizado
Repositorio Institucional de Documentos	RID	Sistema	Carpeta institucional controlada	Unidad de Documentación y Archivo	Digital	Equipo documental; administrador técnico
Equipos computacionales utilizados en el proceso	EQU	Equipos	Dependencias internas de la Comisión	Área TI institucional	Digital (en disco)	Funcionarios autorizados
Soportes físicos de transferencia (pendrive, discos externos, CD, etc.)	SFT	Equipos	Uso temporal interno	Unidad documental	Digital portátil	Equipo documental autorizado
Personal del equipo de la Comisión	PER	Persona	Dependencias de la Comisión / modalidad presencial	Coordinación de la Comisión y Subsecretaría	No aplica	Equipo documental, coordinación, personal autorizado
Oficina del equipo de la Comisión	OFI	Infraestructura física	Dependencias internas de la Subsecretaría (espacio físico donde trabaja el equipo)	Unidad Administrativa / Dirección	No aplica	Funcionarios autorizados y equipo documental
Sala de reunión utilizada para coordinación	SRU	Infraestructura física	Dependencias internas de la Subsecretaría	Unidad Administrativa	No aplica	Equipo. dirección, invitados autorizados

Los atributos atributos (columnas) de cada activo se explican a continuación:

- **Nombre Activo:** Corresponde al nombre del activo de información, y es en esta columna donde se incluyen todos los activos de información identificados en el proceso evaluado.
- **Identificador o Código:** Código dado por la institución que identifica en forma única al activo de información.
- **Tipo:** Clasificación del activo, estos pueden ser:
 - ❖ **Persona:** Funcionario o personal a honorarios que participa en un proceso de negocio.
 - ❖ **Documento:** Corresponde a un escrito que refleja el resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.
 - ❖ **Base de Datos:** Es la información sistematizada y organizada.
 - ❖ **Formulario:** Corresponde a documentos utilizados para recoger información.
 - ❖ **Software:** Programa computacional empaquetado producido por una empresa que lo comercializa.
 - ❖ **Sistema:** Programa computacional a medida, desarrollado por la institución o por un externo, cuyo objetivo es apoyar un proceso de negocio.
 - ❖ **Equipos:** Objetos o dispositivos que realizan o apoyan la realización de una función.
 - ❖ **Infraestructura Física:** Estructura que permite almacenar y/o custodiar activos de información del proceso, tales como: Data Center, oficinas de partes, bodegas, caja fuerte, etc.
 - ❖ **Expediente:** Conjunto de documentos y formularios dispuestos en estricto orden de ocurrencia, de ingreso o egreso. Este puede ser físico o electrónico.
- **Ubicación:** Corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.
- **Responsable/Dueño:** Corresponde al rol o cargo de la persona autorizada para tomar decisiones respecto del activo. Esto no implica necesariamente derecho de propiedad sobre el activo.
- **SopORTE:** Corresponde al medio en el cual se encuentra registrado el activo, este puede ser en papel o digital.

- **Persona Autorizada para manipular:** Corresponde al rol o cargo de la(s) persona(s) autorizada(s) para usar el activo de información, ya sea modificándolo, actualizándolo, trasladándolo o limpiándolo.

3.4.1. ANÁLISIS DE CRITICIDAD

La valoración de criticidad de cada activo se determinó a partir de la información levantada en las entrevistas semiestructuradas y la revisión documental descritas en la sección 3.2. Este análisis responde al requisito de la cláusula 6 de ISO/IEC 27001:2022, que establece que la organización debe evaluar las consecuencias potenciales asociadas a la pérdida de confidencialidad, integridad y disponibilidad de los activos de información. Para cada activo se evaluaron tres dimensiones: confidencialidad (nivel de restricción de acceso requerido según la naturaleza del dato), integridad (consecuencia de una modificación no deseada sobre la operación institucional) y disponibilidad (impacto de la inaccesibilidad del activo en los procesos de la CVVI).

Tabla 4: Riesgos del proceso de registro y gestión de información de CVVI.

ACTIVO DE INFORMACIÓN		ANÁLISIS DE CRITICIDAD			
Nombre Activo	Código	Confidencialidad	Integridad	Disponibilidad	Criticidad
Planilla Maestra de Casos	PMC	Reservada	Alta	Alta	Alta
Planillas Externas Recibidas desde Organismos	PEO	Reservada	Alta	Media	Alta
Carpetas Documentales por Caso	CDC	Reservada	Alta	Alta	Alta
Documentos Probatorios (fichas, informes, oficios)	DCP	Reservada	Alta	Alta	Alta
Digitalizaciones y Escaneos	DIG	Reservada	Alta	Media	Alta
Base Estadística Consolidada (indicadores y conteos)	BEC	Reservada	Alta	Media	Alta
Minutas Internas y Actas de Discusión	MIA	Reservada	Media	Media	Alta
Correos Institucionales Asociados al Proceso	COR	Reservada	Alta	Alta	Alta
Repositorio Institucional de Documentos	RID	Reservada	Alta	Alta	Alta
Equipos computacionales utilizados en el proceso	EQU	Reservada	Alta	Alta	Alta
Soportes físicos de transferencia (pendrive, discos externos, CD, etc.)	SFT	Reservada	Alta	Media	Alta
Personal del equipo de la Comisión	PER	Reservada	Alta	Alta	Alta
Oficina del equipo de la Comisión	OFI	Reservada	Media	Media	Alta
Sala de reunión utilizada para coordinación y revisión de casos	SRU	Público	Baja	Baja	Baja

La confidencialidad Reservada se asignó a todos los activos que contienen o gestionan datos de víctimas, antecedentes probatorios o comunicaciones internas, dado que su divulgación no autorizada podría comprometer derechos fundamentales o afectar procesos administrativos y judiciales en curso, lo cual constituye una consecuencia inaceptable conforme al principio de confidencialidad recogido en la norma. La integridad Alta se asignó a activos cuya modificación no deseada podría alterar conteos, derivaciones o el valor probatorio de la evidencia, afectando la fiabilidad de la información que sustenta las decisiones institucionales. La disponibilidad Alta se reservó a activos cuya inaccesibilidad impediría la operación cotidiana del equipo, comprometiendo la continuidad del proceso evaluado. A continuación se detallan los criterios formales que sustentan cada columna:

- **Confidencialidad:** Puede tomar los siguientes valores:
 - ❖ **Pública:** El activo no tiene restricciones de acceso.
 - ❖ **Reservada:** Activo de información cuyo acceso no autorizado tiene impacto para la institución o terceros.
- **Integridad:** Se identifican las siguientes categorías:
 - ❖ **Baja:** Activo de Información cuya modificación no deseada tiene consecuencias con impacto leve para la institución o terceros.
 - ❖ **Media:** Activo de Información cuya modificación no deseada tiene consecuencias con impacto significativo para la institución o terceros.
 - ❖ **Alta:** Activo de Información cuya modificación no deseada tiene consecuencias con impacto grave para la institución o terceros.
- **Disponibilidad:** Se identifican las siguientes categorías:
 - ❖ **Baja:** Activo de Información cuya inaccesibilidad, tiene impacto leve para la institución o terceros.
 - ❖ **Media:** Activo de Información cuya inaccesibilidad, tiene impacto significativo para la institución o terceros.
 - ❖ **Alta:** Activo de Información cuya inaccesibilidad, tiene impacto grave para la institución o terceros
- **Criticidad:** Es calculada de acuerdo a los criterios de confidencialidad, integridad y disponibilidad con valores (Baja, Media, Alta) cuyo cálculo se detalla en Anexo C Tabla de Cálculo de Criticidad de Activos.

3.5. IDENTIFICACIÓN DE RIESGOS POR ACTIVOS

En esta sección se presenta el análisis de riesgo de cada activo identificado en la sección anterior, en cumplimiento de la cláusula 6 de ISO/IEC 27001:2022, que establece que la organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la

información que identifique los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad, y que estime tanto su probabilidad de ocurrencia como sus consecuencias. Las amenazas y vulnerabilidades asociadas a cada activo fueron determinadas a partir de dos fuentes principales: (i) la información obtenida en las entrevistas semiestructuradas con el personal de la CVVI, donde se identificaron prácticas operativas, ausencias de control y situaciones de riesgo reportadas o percibidas por el equipo, y (ii) la revisión de la documentación interna disponible, incluyendo planillas, procedimientos y estructuras de almacenamiento. A partir de esta base se contrastó las condiciones observadas con los controles establecidos en ISO/IEC 27002:2022, lo que permitió identificar brechas concretas que configuran vulnerabilidades explotables. La probabilidad de ocurrencia se estimó considerando el registro histórico mencionado en las entrevistas y las características del entorno operativo (ausencia de controles automatizados, prácticas manuales, soporte mixto físico-digital). El impacto se evaluó en función de las consecuencias que la materialización de cada riesgo tendría sobre la operación institucional, la trazabilidad de los antecedentes y los derechos de las víctimas registradas. La severidad final se calcula multiplicando los valores de probabilidad e impacto según la matriz definida en el Anexo D. A continuación se detallan los parámetros utilizados en cada columna de las tablas:

- **ID Riesgo:** Código de identificación único del riesgo
- **Amenaza:** Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o a una organización. Independiente de si se tiene registro de su materialización en el pasado.
- **Vulnerabilidad (Debilidad):** Condición de debilidad o fragilidad que se encuentra presente en el activo identificado.
- **Descripción del Riesgo:** Descripción de la consecuencia que existiría para el proceso, en el caso de que la Amenaza descrita afectase concretamente alguna condición de debilidad del activo de información.
- **Probabilidad de ocurrencia:** Posibilidad de que el riesgo se materialice, este punto debe ser consistente con el registro histórico, en caso de que haya. Los valores posibles son:
 - ❖ Casi Certeza
 - ❖ Probable
 - ❖ Moderado
 - ❖ Improbable
 - ❖ Muy Improbable

- **Impacto:** Corresponde a los efectos que tiene en la institución la materialización del riesgo. Los valores posibles son:
 - ❖ Catastróficas
 - ❖ Mayores
 - ❖ Moderadas
 - ❖ Menores
 - ❖ Insignificantes

- **Severidad:** Corresponde al nivel de gravedad del riesgo, que es calculado en base a la probabilidad de ocurrencia por el impacto (Anexo D Tabla de Cálculo de Severidad de Riesgos). Los resultados posibles son:
 - ❖ Extremo
 - ❖ Alto
 - ❖ Moderado
 - ❖ Bajo

En cumplimiento de ISO/IEC 27001, cada riesgo será evaluado a nivel de activo identificando amenazas, vulnerabilidades, probabilidad, impacto y severidad (riesgo inherente). Los resultados serán comparados con los criterios de aceptación formales. Para los riesgos que excedan el umbral aceptable, se propondrán controles basados en ISO/IEC 27002:2022. Posteriormente, se estimará el riesgo residual considerando la implementación de los controles seleccionados.

3.5.1. RIESGOS DEL ACTIVO PLANILLA MAESTRA DE CASOS (PMC)

Tabla 5: Riesgos del activo Planilla Maestra de Casos.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-PMC-01	Acceso no autorizado	No existe control formal documentado de perfiles ni revocación sistemática	Exposición o filtración de datos sensibles contenidos en la planilla maestra	Moderado	Mayores	Extremo
RSK-PMC-02	Eliminación accidental	No existe respaldo automatizado ni versionamiento formal de la planilla. Hacen respaldo manual cada 3 meses.	Pérdida de información consolidada sin posibilidad de restauración segura	Improbable	Mayores	Alto

RSK-PMC-03	Modificación inadvertida	La planilla maestra se actualiza manualmente sin validación automática	Alteración de datos clave que afectan conteos, derivaciones o seguimientos	Moderado	Mayores	Extremo
RSK-PMC-04	Uso indebido del archivo	La planilla puede copiarse a equipos personales sin registro ni trazabilidad	Exposición no trazable de información sensible	Moderado	Mayores	Extremo
RSK-PMC-05	Indisponibilidad operativa	Dependencia de un único archivo centralizado sin alta disponibilidad	Imposibilidad de trabajar, consolidar o reportar casos ante contingencia	Muy improbable	Moderadas	Moderado
RSK-PMC-06	Exposición masiva de datos sensibles	La planilla maestra no está cifrada ni cuenta con anonimización o pseudoanonimización en hojas derivadas	En caso de pérdida del archivo, robo de un equipo, acceso indebido o reenvío accidental, toda la información sensible queda expuesta en texto claro; no hay capas de protección que limiten el daño ni versiones anonimizadas para usos operativos.	Probable	Catastróficas	Extremo

3.5.2. RIESGOS DEL ACTIVO PLANILLAS EXTERNAS RECIBIDAS (PEO)

Tabla 6: Riesgos del activo Planillas Externas Recibidas.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-PEO-01	Datos corruptos o inconsistentes	Entrada manual sin validación automática	Registros duplicados, campos inválidos o errores de consolidación	Moderado	Menores	Moderado
RSK-PEO-02	Fuga de datos por reenvío	Los documentos se distribuyen por correo sin restricciones técnicas	Riesgo de reenviar o compartir antecedentes sensibles a destinatarios indebidos	Moderado	Mayores	Extremo
RSK-PEO-03	Alteración no detectada	Las planillas pueden ser editadas por distintos equipos antes de su consolidación central	Cambios no trazados en información de origen que dificultan reconstruir qué dato estaba originalmente en cada planilla remitente	Moderado	Mayores	Extremo

3.5.3. RIESGOS DEL ACTIVO CARPETAS DOCUMENTALES POR CASO (CDC)

Tabla 7: Riesgos del activo Carpetas Documentales por Caso.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-CDC-01	Pérdida física	No existe inventario digital completo ni respaldo uniforme	Pérdida irrecuperable de expedientes originales	Moderado	Catastróficas	Extremo
RSK-CDC-02	Inexistencia de respaldo sistemático	La digitalización no es siempre completa ni controlada	Imposibilidad de restaurar expedientes extraviados	Moderado	Catastróficas	Extremo

3.5.4. RIESGOS DEL ACTIVO DOCUMENTOS PROBATORIOS (DCP)

Tabla 8: Riesgos del activo Documentos Probatorios.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-DCP-01	Pérdida u omisión documental	Soporte mixto sin control de inventario	Falta de evidencia para análisis administrativos o judiciales	Moderado	Catastróficas	Extremo
RSK-DCP-02	Exposición indebida	Transporte y manipulación sin cifrado ni registro formal	Fuga de datos extremadamente sensibles	Moderado	Mayores	Extremo
RSK-DCP-03	Alteración involuntaria	Ausencia de controles automáticos de integridad a nivel de archivo digital (hashes, firmas, etc.)	Dudas sobre originalidad o integridad de ciertos documentos que pueden afectar su valor probatorio.	Improbable	Mayores	Alto

3.5.5. RIESGOS DEL ACTIVO DIGITALIZACIONES Y ESCANEOS (DIG)

Tabla 9: Riesgos del activo Digitalizaciones y Escaneos.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-DIG-01	Digitalización deficiente	No hay control de calidad sistemático	Información ilegible o incompleta en copias digitales que impide prescindir del documento físico.	Probable	Menores	Alto

3.5.6. RIESGOS DEL ACTIVO BASE ESTADÍSTICA CONSOLIDADA (BEC)

Tabla 10: Riesgos del activo Base Estadística Consolidada.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-BEC-01	Error en consolidación	Cargas manuales sin validación	Indicadores incorrectos que afectan reportes institucionales	Moderado	Mayores	Extremo
RSK-BEC-02	Indisponibilidad	Repositorio no replicado	Afectación a informes, reportes y seguimiento	Improbable	Moderadas	Moderado

3.5.7. RIESGOS DEL ACTIVO MINUTAS INTERNAS Y ACTAS (MIA)

Tabla 11: Riesgos del activo Minutas Internas y Actas.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-MIA-01	Fuga interna	Documentos compartidos sin restricción de lectura	Exposición de deliberaciones internas o decisiones reservadas	Improbable	Moderadas	Moderado
RSK-MIA-02	Pérdida documental	No hay respaldo estructurado	Pérdida de evidencia administrativa	Improbable	Moderadas	Moderado

3.5.8. RIESGOS DEL ACTIVO CORREOS INSTITUCIONALES (COR)

Tabla 12: Riesgos del activo Correos Institucionales.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-COR-01	Fuga accidental	Reenvío o copia sin controles técnicos	Exposición de datos personales y antecedentes sensibles	Improbable	Mayores	Alto
RSK-COR-02	Pérdida de trazabilidad	No existe política formal de archivado y clasificación	Información irreproducible para auditoría, análisis o seguimiento	Moderado	Moderadas	Alto

3.5.9. RIESGOS DEL ACTIVO REPOSITORIO INSTITUCIONAL (RID)

Tabla 13: Riesgos del activo Repositorio Institucional.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-RID-01	Acceso indebido	Perfiles y accesos no auditados periódicamente	Lectura o copia no autorizada de antecedentes	Improbable	Mayores	Alto
RSK-RID-02	Pérdida o corrupción	No hay verificación sistemática de respaldos ni simulacros de restauración	Imposibilidad de restaurar documentos críticos ante corrupción, error humano o incidente técnico en el repositorio.	Improbable	Catastróficas	Extremo

RSK-RID-03	Falta de catálogo completo	No existe un catastro documental totalmente exhaustivo; el catastro 2023 cubre sólo lo ya identificado	Riesgo de que ciertos documentos o series documentales queden “invisibles” para la Comisión, afectando la capacidad de búsqueda, análisis y respuesta	Moderado	Mayores	Extremo
------------	----------------------------	--	---	----------	---------	---------

3.5.10. RIESGOS DEL ACTIVO EQUIPOS COMPUTACIONALES (EQU)

Tabla 14: Riesgos del activo Equipos Computacionales.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-EQU-01	Robo físico	Equipos cifrado de disco	Exposición total del contenido	Muy improbable	Catastrófico	Alto
RSK-EQU-02	Daño ambiental o técnico	Equipos sin plan explícito de continuidad ante fallas (reemplazo inmediato, acceso alternativo)	Indisponibilidad operativa de herramientas clave para el trabajo diario del equipo.	Muy improbable	Moderadas	Moderado

3.5.11. RIESGOS DEL ACTIVO SOPORTES FÍSICOS DE TRANSFERENCIA (SFT)

Tabla 15: Riesgos del activo Soportes Físicos de Transferencia.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-SFT-01	Pérdida o traspaso no controlado	Pendrive o discos sin cifrado ni registro	Fuga de información sensible	Moderado	Mayores	Alto
RSK-SFT-02	Uso indebido	Transferencia sin registro	Fuga de datos no detectada	Moderado	Mayores	Alto

3.5.12. RIESGOS DEL ACTIVO PERSONAL DEL EQUIPO (PER)

Tabla 16: Riesgos del activo Personal del Equipo.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-PER-01	Salida de funcionarios	No existe procedimiento documentado para revocación inmediata de accesos	Exfuncionario mantiene credenciales activas o acceso a repositorios antiguos	Muy improbable	Mayores	Alto
RSK-PER-02	Falta de continuidad operativa	Alta dependencia de ciertas personas clave para la operación del registro y el manejo de planillas	Riesgo de indisponibilidad del servicio o de pérdida de coherencia en los procesos si una persona clave se ausenta o deja la institución.	Muy improbable	Moderadas	Moderado
RSK-PER-03	Phishing / Ingeniería Social	No existen capacitaciones sistemáticas ni simulaciones	Un funcionario puede entregar credenciales o documentos sensibles sin darse cuenta	Probable	Catastróficas	Extremo

3.5.13. RIESGOS DEL ACTIVO OFICINA DEL EQUIPO (OFI)

Tabla 17: Riesgos del activo Oficina del Equipo.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-OFI-01	Acceso físico no autorizado	Espacios sin control de acceso físico robusto ni registro de visitas	Riesgo de exposición, robo o manipulación de documentación y equipos	Improbable	Mayores	Alto
RSK-OFI-02	Exposición accidental de información	Documentos impresos o pantallas a la vista. Claves escritas en pizarra.	Observación o escucha no autorizada de deliberaciones internas, e información privilegiada	Improbable	Mayores	Alto

3.5.14. RIESGOS DEL ACTIVO SALA DE REUNIÓN (SRU)

Tabla 18: Riesgos del activo Sala de Reunión.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción	Probabilidad	Impacto	Severidad
RSK-SRU-01	Exposición accidental de información	Reuniones con documentos impresos o pantallas visibles sin control del entorno	Observación o escucha no autorizada de deliberaciones internas	Improbable	Mayores	Alto
RSK-SRU-02	Acceso físico indebido a dependencias institucionales	Es posible ingresar al edificio ministerial sin un control de identidad riguroso en recepción	Terceros podrían acceder a áreas mientras se maneja documentación o se discuten antecedentes, con potencial exposición deliberada o accidental de información reservada	Moderado	Catastróficas	Extremo

3.6. ANÁLISIS DE RIESGO ACEPTABLE

El nivel de riesgo aceptable se determinó como un umbral metodológico que permite decidir qué riesgos requieren tratamiento prioritario, en coherencia con la cláusula 6 de ISO/IEC 27001:2022, que exige que la organización defina criterios de aceptación del riesgo y garantice que las evaluaciones produzcan resultados consistentes, válidos y comparables. La tabla a continuación consolida todos los riesgos identificados en la sección 3.5, ordenados según su nivel de severidad calculado conforme al Anexo D. Cada combinación de probabilidad e impacto produce un código SR (por ejemplo, Moderado x Mayores = SR 32) que se traduce en una categoría de severidad: Extremo, Alto, Moderado o Bajo. Esta traducción no es arbitraria: los riesgos que combinan alta probabilidad con consecuencias catastróficas o mayores se clasifican como Extremo porque su materialización comprometería los derechos de las víctimas y la capacidad operativa de la institución, superando cualquier umbral de aceptación razonable en el contexto de la CVVI. La decisión de tratar prioritariamente los riesgos con severidad Extremo responde además a la cláusula 6 de ISO/IEC 27001:2022, que exige seleccionar opciones de tratamiento apropiadas en función de los resultados de la evaluación de riesgos. Los riesgos con severidad Alto, Moderado o Bajo, si bien no son descartados, quedan fuera del

alcance de esta memoria dado que los de nivel Extremo representan la brecha más crítica y urgente de abordar con los recursos institucionales disponibles.

Tabla 19: Nivel de Riesgo Aceptable.

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S=(PxI)	RIESGOS ANALIZADOS
Casi Certeza	Catastróficas	Extremo	
Casi Certeza	Mayores	Extremo	
Casi Certeza	Moderadas	Extremo	
Probable	Catastróficas	Extremo	RSK-PMC-06 RSK-PER-03
Probable	Mayores	Extremo	
Moderado	Catastróficas	Extremo	RSK-PMC-03 RSK-CDC-01 RSK-CDC-02 RSK-DCP-01 RSK-SRU-02
Moderado	Mayores	Extremo	RSK-PMC-01 RSK-PMC-04 RSK-PEO-02 RSK-PEO-03 RSK-DCP-02 RSK-BEC-01 RSK-RID-03 RSK-SFT-01 RSK-SFT-02
Improbable	Catastróficas	Extremo	RSK-RID-02
Casi Certeza	Menores	Alto	
Casi Certeza	Insignificantes	Alto	
Probable	Moderadas	Alto	
Probable	Menores	Alto	RSK-DIG-01
Moderado	Moderadas	Alto	RSK-COR-02
Improbable	Mayores	Alto	RSK-PMC-02 RSK-DCP-03 RSK-COR-01 RSK-RID-01 RSK-OFI-01 RSK-OFI-02 RSK-SRU-01

Muy Improbable	Catastróficas	Alto	RSK-EQU-01
Muy Improbable	Mayores	Alto	RSK-PER-01
Probable	Insignificantes	Moderado	
Moderado	Menores	Moderado	RSK-PEO-01
Improbable	Moderadas	Moderado	RSK-BEC-02 RSK-MIA-01 RSK-MIA-02
Muy Improbable	Moderadas	Moderado	RSK-PMC-05 RSK-EQU-02 RSK-PER-02
Moderado	Insignificantes	Baja	
Improbable	Menores	Baja	
Improbable	Insignificantes	Baja	
Muy Improbable	Menores	Baja	
Muy Improbable	Insignificantes	Baja	

En la tabla se observan los niveles de riesgos analizados para el proceso de gestión de información de la CVVI, cuya decisión metodológica en esta memoria radica en abordar prioritariamente aquellos riesgos con severidad Extremo. Estos riesgos se concentran en tres frentes que, de materializarse, podrían generar efectos críticos: (i) exposición no autorizada de información altamente sensible, (ii) pérdida irrecuperable o invisibilización de antecedentes/documentos, y (iii) alteración no trazable de registros que sostiene reportes, seguimientos y capacidad de respuesta institucional. En términos prácticos, los riesgos extremos identificados muestran que la infraestructura y las prácticas actuales (planilla maestra, circulación de planillas por equipos y correo, soportes físicos/mixtos, repositorios y transferencias) no cuentan con controles de acceso, trazabilidad, respaldo, cifrado y validación, por lo que un incidente puede escalar rápidamente a una afectación mayor.

3.7. SELECCIÓN DE CONTROLES DE MITIGACIÓN DE RIESGOS EXTREMOS

A continuación se muestran los controles de la Norma ISO 27002:2022 (ISO/IEC., 2022b) que se proponen implementar como medida de mitigación y su respectiva justificación para riesgos extremos.

3.7.1. RIESGO RSK-PMC-01 (PLANILLA MAESTRA DE CASOS)

Tabla 20: Riesgo Acceso no autorizado.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-PMC-01	Acceso no autorizado	No existe control formal documentado de perfiles ni revocación sistemática.	Exposición o filtración de datos sensibles contenidos en la planilla maestra.	Extremo

Tabla 21: Medidas de control para Riesgo Acceso no Autorizado.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.15	Access control	Debe establecer reglas formales de acceso físicas y lógicas a la planilla maestra y repositorios asociados, reduciendo la exposición por acceso no autorizado.
5.18	Access rights	La asignación, revisión y revocación sistemática de permisos reduce accesos heredados o innecesarios.
8.2	Privileged access rights	Se debe restringir privilegios elevados a un número acotado de responsables reduce la superficie de exposición de información sensible.
8.3	Information access restriction	Para acceder a la planilla maestra se debe segmentar acceso por rol y necesidad de saber, y así evitar visualización o extracción de datos por usuarios no autorizados.
8.15	Logging	Se deben trazar los accesos y acciones permite generar evidencia, detectar, investigar y responder ante usos indebidos o filtraciones.

3.7.2. RIESGO RSK-PMC-03 (PLANILLA MAESTRA DE CASOS)

Tabla 22: Riesgo Modificación inadvertida.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-PMC-03	Modificación inadvertida	La planilla maestra se actualiza manualmente sin validación automática	Alteración de datos clave que afectan conteos o seguimientos	Extremo

Tabla 23: Medidas de control para Riesgo Modificación inadvertida

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.37	Documented operating procedures	No se debería operar sobre la planilla maestra sin una guía o procedimientos documentados de carga y actualización reducen la variabilidad operativa y el error humano.

8.15	Logging	Se debería contar con un sistema de registro de modificaciones que permita reconstruir cambios, identificar responsables y corregir inconsistencias.
8.16	Monitoring activities	Debe existir un encargado del monitoreo de actividades críticas, y así poder detectar patrones de edición anómalos o errores recurrentes.
8.32	Change management	La planilla maestra debe contar con controles de cambios formales, que deben ser validados para reducir errores de actualización y alteraciones no controladas.

3.7.3. RIESGO RSK-PMC-04 (PLANILLA MAESTRA DE CASOS)

Tabla 24: Riesgo Uso indebido del archivo.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-PMC-04	Uso indebido del archivo	La planilla puede copiarse a equipos personales sin registro ni trazabilidad	Exposición no trazable de información sensible	Extremo

Tabla 25: Medidas de control para Riesgo Uso indebido del archivo.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.10	Acceptable use of information and other associated assets	Se deben establecer reglas explícitas sobre copias, almacenamiento local y uso de archivos sensibles. Con esto se busca reducir las prácticas informales como uso de Whatsapp para compartir archivos.
5.14	Information transfer	Los canales autorizados y condiciones de transferencia deben estar definidos, disminuyendo así la circulación no controlada de la planilla.
8.15	Logging	Al aplicar trazabilidad de accesos y transferencias, es posible detectar y reconstruir usos indebidos.

3.7.4. RIESGO RSK-PMC-06 (PLANILLA MAESTRA DE CASOS)

Tabla 26: Riesgo Exposición masiva de datos sensibles.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-PMC-06	Exposición masiva de datos sensibles	La planilla maestra no está cifrada ni cuenta con anonimización o pseudoanonimización en hojas derivadas	En caso de pérdida del archivo, robo de un equipo, acceso indebido o reenvío accidental, toda la información sensible queda expuesta en texto claro.	Extremo

Tabla 27: Medidas de control para Riesgo Exposición masiva de datos sensibles.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.12	Classification of information	Se debe clasificar la planilla y hojas derivadas según sensibilidad, para así habilitar controles diferenciados de acceso, cifrado y transferencia.
5.13	Labelling of information	El etiquetado visible de información sensible reduce errores de uso, reenvío o compartición indebida.
5.14	Information transfer	Se debe restringir el envío/circulación de archivos sensibles a mecanismos autorizados, estos deben estar documentados y se debe capacitar al personal para utilizarlos.
8.11	Data masking	Cuando se quiera trabajar con los datos en escenarios de divulgación se deben enmascarar/pseudoanonimizar.
8.24	Use of cryptography	Debe existir una política de cifrado de datos de la planilla maestra. El cifrado reduce drásticamente el impacto de pérdida, robo o acceso indebido al archivo, evitando exposición en texto claro.

3.7.5. RIESGO RSK-PEO-02 (PLANILLAS EXTERNAS RECIBIDAS)

Tabla 28: Riesgo Fuga de datos por reenvío.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-PEO-02	Fuga de datos por reenvío	Los documentos se distribuyen por correo sin restricciones técnicas	Riesgo de reenviar o compartir antecedentes sensibles a destinatarios indebidos	Extremo

Tabla 29: Medidas de control para Riesgo Fuga de datos por reenvío.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.12	Classification of information	La clasificación previa obliga a tratar de forma diferenciada antecedentes sensibles antes de su envío. Las planillas recibidas deben clasificarse para no compartir información sin querer.
5.13	Labelling of information	Cuando se reciba información externa, como archivos/correos, se deben etiquetar como sensibles. Esto reduce errores de reenvío por falta de contexto del usuario.
5.14	Information transfer	Al compartir información sensible se debe definir una vía de transferencia de datos oficial y documentada. Esto permite formalizar el uso de canales autorizados, restricciones de envío y condiciones de intercambio de información sensible.
6.3	Information security awareness, education and training	Se debe capacitar a las personas que interactúen con datos sensibles. Esto reduce incidentes por error humano, especialmente reenvíos indebidos y destinatarios incorrectos.
8.12	Data leakage prevention	Controles de prevención de fuga pueden bloquear (no permitir copy/paste) o alertar reenvíos con contenido sensible. Se deben establecer vías para compartir archivos que cuenten con estas configuraciones.

3.7.6. RIESGO RSK-PEO-03 (PLANILLAS EXTERNAS RECIBIDAS)

Tabla 30: Riesgo Alteración no detectada.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-PEO-03	Alteración no detectada	Las planillas pueden ser editadas por distintos equipos antes de su consolidación central	Cambios no trazados en información de origen que dificultan reconstruir qué dato estaba originalmente en cada planilla remitente	Extremo

Tabla 31: Medidas de control para Riesgo.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.37	Documented operating procedures	Se debe establecer una guía de procedimientos de consolidación. Cuando se reciba una planilla externa o archivo se debe establecer un proceso claro disminuya prácticas individuales.
8.3	Information access restriction	Para reducir la probabilidad de cambios involuntarios se debe limitar quién puede editar y quién solo consultar.
8.15	Logging	Al registrar ediciones y accesos, se habilita la trazabilidad de cambios antes de la consolidación.
8.16	Monitoring activities	Se debe ejercer un monitoreo sistemático para ayudar a detectar cambios anómalos o alteraciones fuera de flujo.
8.32	Change management	Formalizar versiones, responsables y aprobación de cambios para reducir alteraciones no controladas. Estos roles deben estar documentados y debe establecerse periodicidad.

3.7.7. RIESGO RSK-CDC-01 (CARPETAS DOCUMENTALES POR CASO)

Tabla 32: Riesgo Pérdida física.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-CDC-01	Pérdida física	No existe inventario digital completo ni respaldo uniforme	Pérdida irrecuperable de expedientes originales	Extremo

Tabla 33: Medidas de control para Riesgo Pérdida física.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.9	Inventory of information and other associated assets	Se debe generar un inventario de la información. Las carpetas documentales no cuentan con un catastro completo de expedientes y soportes. Esto imposibilita controlar, priorizar ni recuperar adecuadamente la información crítica.
8.13	Information backup	El respaldo sistemático reduce el impacto de pérdida física y mejora la capacidad de restauración de antecedentes críticos. Se debe establecer una vía y responsable.
7.1	Physical security perimeters	Delimitar áreas físicas protegidas reduce robo, extravío o acceso no autorizado a expedientes.
7.8	Equipment siting and protection	La correcta ubicación/protección de equipos y soportes disminuye daño físico y pérdida de información. Se aconseja voltear pantallas, no guardar documentos directamente en escritorio, despejar el espacio de trabajo.

3.7.8. RIESGO RSK-CDC-02 (CARPETAS DOCUMENTALES POR CASO)

Tabla 34: Riesgo Inexistencia de respaldo sistemático.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-CDC-02	Inexistencia de respaldo sistemático	La digitalización no es siempre completa ni controlada	Imposibilidad de restaurar expedientes extraviados	Extremo

Tabla 35: Medidas de control para Riesgo Inexistencia de respaldo sistemático.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
8.13	Information backup	Se debe establecer un esquema formal de respaldo (alcance, periodicidad, responsables) para reducir pérdida irreversible de expedientes.
8.16	Monitoring activities	El monitoreo de tareas de respaldo permite identificar fallas, brechas de cobertura o respaldos no ejecutados.

3.7.9. RIESGO RSK-DCP-01 (DOCUMENTOS PROBATORIOS)

Tabla 36: Riesgo Pérdida u omisión documental.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-DCP-01	Pérdida u omisión documental	Soporte mixto sin control de inventario	Falta de evidencia para análisis administrativos o judiciales	Extremo

Tabla 37: Medidas de control para Riesgo Pérdida u omisión documental

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.9	Inventory of information and other associated assets	Los documentos probatorios deben ser identificados con tal de saber si existen, dónde se encuentran y cuáles faltan, para así reducir omisiones e invisibilización documental. Se debe establecer un responsable o mecanismo responsable de revisar el inventario.
5.12	Classification of information	Para poder aplicar correctamente el control 5.9 se debe hacer una clasificación documental exhaustiva que identifique propiedad, nivel de confidencialidad, nivel de impacto que tiene en el proceso.
5.33	Protection of records	La organización debe establecer guías de almacenamiento, propiedad, protección ante manipulaciones. También se debe definir un periodo de tiempo en el que los documentos serán resguardados.

5.37	Documented operating procedures	Se debe estandarizar la recepción, digitalización y registro. Cuando muchas personas entran en contacto con estos documentos se debe establecer un protocolo claro, responsables, periodos en los que se puede tener acceso.
8.13	Information backup	Se deben generar copias de seguridad periódicamente. Las copias de respaldo reducen el impacto de pérdida de documentos digitalizados o consolidados.

3.7.10. RIESGO RSK-DCP-02 (DOCUMENTOS PROBATORIOS)

Tabla 38: Riesgo Exposición indebida.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-DCP-02	Exposición indebida	Transporte y manipulación sin cifrado ni registro formal	Fuga de datos extremadamente sensibles	Extremo

Tabla 39: Medidas de control para Riesgo Exposición indebida.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.14	Information transfer	Se deben formalizar procedimientos y condiciones de transporte/transferencia de información sensible. La información que transita debe contar con políticas organizacionales de información clasificada.
7.9	Security of assets off-premises	Los dispositivos o archivos que transiten fuera de la organización deben protegerse. No debe dejarse un activo sin supervisión; se deben proteger de humedad, calor, campos electromagnéticos, polvo; cuando pase por muchas manos se debe mantener un registro de quien lo tiene y por cuanto tiempo está autorizado a tenerlo; si no es necesario no debe mostrarse en la vía pública; de ser posible instalar un sistema de trackeo remoto.
8.15	Logging	El registro de transferencias y accesos permite trazabilidad y reconstrucción de incidentes.
8.24	Use of cryptography	El cifrado de archivos y soportes reduce el impacto si se pierden, sustraen o acceden sin autorización durante traslado/manipulación.

3.7.11. RIESGO RSK-BEC-01 (BASE ESTADÍSTICA CONSOLIDADA)

Tabla 40: Riesgo Error en consolidación.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-BEC-01	Error en consolidación	Cargas manuales sin validación	Indicadores incorrectos que afectan reportes institucionales	Extremo

Tabla 41: Medidas de control para Riesgo Error en consolidación.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.37	Documented operating procedures	Para disminuir errores por ejecución manual se deben estandarizar pasos de consolidación y revisión.
8.15	Logging	Permite rastrear cargas, modificaciones y correcciones para auditoría y control de calidad de datos.
8.16	Monitoring activities	Facilita detectar inconsistencias o desviaciones repetidas en la consolidación antes de emitir reportes.
8.32	Change management	Introduce validaciones y control de cambios en procesos de consolidación, reduciendo errores críticos de carga.

3.7.12. RIESGO RSK-RID-02 (REPOSITORIO INSTITUCIONAL)

Tabla 42: Riesgo Pérdida o corrupción.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-RID-02	Pérdida o corrupción	No hay verificación sistemática de respaldos ni simulacros de restauración	Imposibilidad de restaurar documentos críticos ante corrupción, error humano o incidente técnico en el repositorio.	Extremo

Tabla 43: Medidas de control para Riesgo Pérdida o corrupción.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
8.13	Information backup	El repositorio institucional debe contar con una política de respaldo (qué se respalda, con qué frecuencia y dónde). Se deben definir planes, softwares a utilizar, lugar en donde se almacenará (remoto o local).
8.15	Logging	La evidencia de fallas/incidentes y de restauraciones permite aprendizaje, auditoría y mejora del proceso.
8.16	Monitoring activities	Permite monitorear ejecución y resultado de respaldos, identificando fallas oportunamente.

3.7.13. RIESGO RSK-RID-03 (REPOSITORIO INSTITUCIONAL)

Tabla 44: Riesgo Falta de catálogo completo.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-RID-03	Falta de catálogo completo	No existe un catastro documental totalmente exhaustivo; el catastro 2023 cubre sólo lo ya identificado	Riesgo de que ciertos documentos o series documentales queden “invisibles” para la Comisión.	Extremo

Tabla 45: Medidas de control para Riesgo Falta de catálogo completo.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.9	Inventory of information and other associated assets	Se debe realizar un inventario exhaustivo del repositorio institucional. Esta medida reduce la invisibilización documental y mejora la capacidad de búsqueda y respuesta. Cuando se realiza este repositorio se debe identificar su importancia en términos de privacidad, idealmente se deben establecer cargas automáticas que actualicen el inventario.
5.12	Classification of information	Se debe clasificar la documentación según criterios de confidencialidad, integridad, disponibilidad y requerimientos de las partes interesadas en hacer uso de ellos. Se debe definir a un responsable de clasificar, quien se encargará de actualizar dicha clasificación.
5.33	Protection of records	La organización debe asegurar que los documentos serán protegidos de pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada. Se debe definir el tiempo que la organización guardara dicha información.
5.37	Documented operating procedures	Se deben documentar los procesos y operaciones de manera que todo el personal tenga conocimiento de ellos. El equipo debe definir un encargado de documentación.

3.7.14. RIESGO RSK-SFT-01 (SOPORTES FÍSICOS DE TRANSFERENCIA)

Tabla 46: Riesgo Pérdida o traspaso no controlado.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-SFT-01	Pérdida o traspaso no controlado	Pendrive o discos sin cifrado ni registro	Fuga de información sensible	Extremo

Tabla 47: Medidas de control para Riesgo Pérdida o traspaso no controlado.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.10	Acceptable use of information and other associated assets	Establecer reglas formales para uso y transporte de medios removibles. Se debe capacitar al personal sobre el uso aceptable de dichos dispositivos y el tipo de información que se puede cargar en ellos.
7.9	Security of assets off-premises	Los dispositivos o archivos que transiten fuera de la organización deben protegerse. No debe dejarse un activo sin supervisión; se deben proteger de humedad, calor, campos electromagnéticos, polvo; cuando pase por muchas manos se debe mantener un registro de quien lo tiene y por cuanto tiempo está autorizado a tenerlo; si no es necesario no debe mostrarse en la vía pública; de ser posible instalar un sistema de trackeo remoto.
8.11	Data masking	Permite que, cuando sea posible, los datos transportados no sean nominativos completos, disminuyendo daño ante exposición.
8.15	Logging	El registro de asignación/uso de medios mejora trazabilidad y respuesta ante pérdida.
8.24	Use of cryptography	El cifrado de medios removibles reduce el impacto de pérdida o robo.

3.7.15. RIESGO RSK-SFT-02 (SOPORTES FÍSICOS DE TRANSFERENCIA)

Tabla 48: Riesgo Uso indebido.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-SFT-02	Uso indebido	Transferencia sin registro	Fuga de datos no detectada	Extremo

Tabla 49: Medidas de control para Riesgo Uso indebido.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.14	Information transfer	Se deben formalizar procedimientos y condiciones de transporte/transferencia de información sensible. La información que transita debe contar con políticas organizacionales de información clasificada.
8.12	Data leakage prevention	Para reducir la fuga de datos se debe identificar y clasificar información sujeta a protección (ej información privada), monitorear los dispositivos donde se realizan transferencias de datos, capacitar a personal sobre el manejo de los dispositivos que cuentan con información sensible.
8.15	Logging	La trazabilidad es esencial para detectar y reconstruir fugas que hoy podrían pasar inadvertidas.
8.16	Monitoring activities	El monitoreo de transferencias permite identificar patrones o eventos anómalos.

3.7.16. RIESGO RSK-PER-03 (PERSONAL DEL EQUIPO)

Tabla 50: Riesgo Phishing / Ingeniería Social.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-PER-03	Phishing / Ingeniería Social	No existen capacitaciones sistemáticas ni simulaciones	Un funcionario puede entregar credenciales o documentos sensibles sin darse cuenta	Extremo

Tabla 51: Medidas de control para Riesgo Phishing / Ingeniería Social.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
5.24	Information security incident management planning and preparation	Se debe definir cómo actuar ante incidentes que comprometan la privacidad de la información. Deben existir protocolos, capacitaciones y simulacros que pongan a prueba y retroalimenten las políticas de seguridad interna del equipo.
5.26	Response to information security incidents	Se deben establecer roles y responsables ante una posible incidencia. Una vez ocurrido un ataque se debe recolectar evidencia, escalar la situación, identificar las debilidades y accesos.

6.3	Information security awareness, education and training	La capacitación periódica y simulaciones reducen la probabilidad de éxito de ataques de ingeniería social.
8.7	Protection against malware	Se deben implementar reglas de control que no permitan descargas de softwares no autorizados.

3.7.17. RIESGO RSK-SRU-02 (SALA DE REUNIÓN)

Tabla 52: Riesgo Acceso físico indebido a dependencias institucionales.

ID Riesgo	Amenaza	Vulnerabilidad	Descripción del Riesgo	Severidad
RSK-SRU-02	Acceso físico indebido a dependencias institucionales	Es posible ingresar al edificio ministerial sin un control de identidad riguroso en recepción (según lo que comentaste fuera de la entrevista)	Terceros podrían acceder a pisos o salas de reunión mientras se maneja documentación o se discuten antecedentes, con potencial exposición deliberada o accidental de información reservada	Extremo

Tabla 53: Medidas de control para Riesgo Acceso físico indebido a dependencias institucionales.

Control para mitigar el riesgo	Nombre del Control	Justificación del control
7.2	Physical entry	Para asegurar solo el acceso autorizado se debe ejercer control de ingreso (identificación, registro de visitas y autorización). Se debe solicitar a las personas y visitas que siempre lleven a la vista algún identificador; asegurar las salidas de emergencia para evitar accesos no deseados.
7.3	Securing offices, rooms and facilities	Fortalecer el resguardo de salas y oficinas donde se manipulan antecedentes reservados reduce exposición accidental o deliberada.
7.4	Physical security monitoring	El monitoreo físico mejora detección, disuasión y reconstrucción de incidentes de acceso indebido.
7.7	Clear desk and clear screen	Mantener un escritorio y pantalla limpios reduce la exposición de documentos visibles durante el tránsito de personas externas o visitas.

3.8. ANÁLISIS DEL PATRÓN DE CONTROLES PROPUESTOS

Una vez identificados los riesgos con severidad Extremo, se realizó el mapeo de cada riesgo a controles específicos de ISO/IEC 27002:2022. A continuación se consolidaron los controles seleccionados y se contabilizó la frecuencia con que cada control fue recomendado. Este ejercicio permite observar el patrón de mitigación dominante que estructura la propuesta.



Figura 3: Top 10 Cantidad de veces que un Control fue recomendado.

Fuente: Elaboración Propia.

A partir de este resultado, es posible concluir:

- **Predominio de controles de trazabilidad y gobierno operativo:** La alta frecuencia de *Logging* y *Monitoring activities* indica que una debilidad estructural del entorno analizado es la falta de visibilidad operativa sobre lo que ocurre con la información. No sólo existen riesgos de fuga, pérdida o alteración, sino también un riesgo adicional: que dichos eventos ocurran sin evidencia suficiente para detectarlos, reconstruirlos y/o atribuirlos. En términos de gobernanza, esto se traduce en baja capacidad de rendición de cuentas y dificultad para sostener decisiones operativas con trazabilidad. Por ello, desde una perspectiva técnica, fortalecer mecanismos de registro y monitoreo aparece como un “primer piso” de seguridad, incluso antes de incorporar soluciones más sofisticadas.

- **Relevancia de procedimientos y disciplina operativa:** La presencia destacada de *Documented operating procedures* confirma que una parte importante del riesgo se origina en la variabilidad de prácticas de trabajo. En otras palabras, la seguridad no se ve afectada únicamente por “faltas de tecnología”, sino por la inexistencia de procedimientos claros para tareas críticas como consolidación de datos, transferencia, respaldo, registro documental y manejo de archivos sensibles. Este patrón fundamenta que la propuesta incorpore estandarización operativa como medida de control: transformar trabajo tácito en procesos explícitos, repetibles y auditables.
- **Centralidad del problema de transferencia y circulación de información:** La frecuencia de *Information transfer* y *Classification of information* muestra que el riesgo extremo se concentra, en gran medida, en el movimiento de la información. Enviar información por correo, compartir entre equipos, traspasar mediante medios removibles y circulación de archivos sin clasificación ni etiquetado. Esto refuerza que la seguridad de la información no puede entenderse solo como “protección en reposo”, sino también como gestión segura de la circulación, lo cual resulta especialmente crítico en entornos colaborativos y con alta urgencia operativa.
- **Importancia del respaldo e inventario como base de continuidad:** La presencia de *Information backup* e *Inventory of information and other associated assets* entre los controles más frecuentes refleja una fragilidad estructural en la capacidad institucional de preservar memoria documental y continuidad operativa. La pérdida de antecedentes, la inexistencia de respaldo verificable o la invisibilización de documentos no afectan sólo la eficiencia del trabajo, sino que también afectan la posibilidad de responder institucionalmente con integridad y oportunidad.
- **La criptografía como medida necesaria, pero no suficiente:** La aparición de *Use of cryptography* en el Top 10 confirma que el cifrado es una medida importante, especialmente para reducir impacto en casos de pérdida, robo o acceso indebido. Sin embargo, su frecuencia relativa menor respecto de *logging*, monitoreo y procedimientos muestra que el cifrado por sí solo no resuelve el problema. Si bien encriptar archivos puede ser una medida inicial valiosa y de bajo costo, la reducción sostenida del riesgo requiere complementar esta acción con clasificación, reglas de transferencia, inventario, respaldo y trazabilidad.

CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN

Como la solución propuesta no corresponde a un software implementado, sino a un conjunto de metodologías de trabajo, lineamientos operativos y controles de seguridad de la información orientados a robustecer la gestión de activos de información críticos en el proceso de registro de víctimas de la Comisión de Víctimas de Violencia Institucional (CVVI, su validación no puede abordarse exclusivamente mediante pruebas funcionales tradicionales

En este sentido la estrategia de validación obedecerá a criterios de factibilidad técnica y pertinencia contextual, centrándose en responder las siguientes preguntas:

- ¿La propuesta aborda los riesgos efectivamente identificados en el diagnóstico?
- ¿Los controles seleccionados son técnicamente consistentes con normas y buenas prácticas (ISO/IEC 27002:2022)?
- ¿La CVVI reconoce la relevancia de los riesgos y la necesidad de mitigarlos?
- ¿Existen condiciones mínimas para implementar al menos una parte de las medidas propuestas?

4.1. ALCANCE Y LIMITACIONES DE LA VALIDACIÓN

La validación de la solución propuesta presenta limitaciones derivadas del contexto institucional estudiado. Durante el levantamiento de antecedentes y la conversación con la contraparte de la CVVI, se señaló que no es factible implementar en el corto plazo la totalidad de las medidas de mitigación propuestas, debido a restricciones estructurales que afectan la capacidad de ejecución institucional. Estas restricciones pueden agruparse en tres dimensiones:

4.1.1. RESTRICCIONES PRESUPUESTARIAS

La implementación de varias medidas de seguridad requiere recursos monetarios para adquisición de insumos y servicios, por ejemplo: medios de almacenamiento seguros; licencias de software; soluciones de respaldo; herramientas de cifrado/gestión centralizada (cuando se requieren versiones institucionales); servicios de almacenamiento en nube con controles adecuados. La CVVI indicó que actualmente no dispone de presupuesto específico para abordar estas mejoras de manera integral, lo que limita la posibilidad de ejecutar controles que dependen de inversión directa en tecnología o infraestructura.

4.1.2. RESTRICCIONES DE CAPACIDADES TÉCNICAS

La contraparte también señaló que el área informática disponible no cuenta necesariamente con formación específica en seguridad de la información, gestión de riesgos o implementación de controles alineados a ISO/IEC 27001-27002:2022. Esto genera una brecha entre la recomendación técnica y la capacidad de implementación autónoma de los controles propuestos. Esta limitación es relevante, ya que la efectividad de una medida de seguridad no depende sólo de su definición documental, sino también de su correcta configuración, adopción operativa y mantenimiento en el tiempo.

4.1.3. RESTRICCIONES OPERACIONALES Y DE HORAS HOMBRE

Se identificó una limitación de carga laboral: el equipo de trabajo prioriza tareas críticas de atención, registro, revisión y gestión de casos, lo que reduce el tiempo disponible para ejecutar acciones de mejora en seguridad de la información. Esta situación es consistente con un patrón observado en múltiples organizaciones: la gestión del riesgo suele postergarse mientras no ocurra un incidente material. En consecuencia, **no fue posible realizar una validación por implementación completa**, ni medir indicadores “antes/después” asociados a una adopción real de todos los controles propuestos.

4.2. ESTRATEGIA DE VALIDACIÓN ADOPTADA

Dado el escenario descrito, la validación se realiza mediante una estrategia compuesta por tres niveles complementarios:

1. **Validación de consistencia técnica de la propuesta:** Se verificó que los controles seleccionados para riesgos extremos sean coherentes con la naturaleza de los activos, amenazas y vulnerabilidades identificadas, y que se encuentren alineados con buenas prácticas y controles de ISO/IEC 27002:2022.
2. **Validación contextual con informante clave (factibilidad organizacional):** Se contrasta la propuesta con la realidad operativa de la CVVI, identificando qué medidas son percibidas como prioritarias, cuáles resultan inviables en el corto plazo y cuáles podrían iniciarse con recursos mínimos.
3. **Validación de implementabilidad incremental (mínimo viable de seguridad):** Se reconoce y documenta un subconjunto de medidas de bajo costo o costo cero que sí podrían ser implementadas como punto de partida, lo que permite demostrar aplicabilidad parcial de la solución.

La validación de los puntos (1) y (2) fue aplicada por informante clave de la CVVI con rol de coordinación/gestión documental y conocimiento del flujo de trabajo y restricciones operativas de la CVVI. Para asegurar trazabilidad y comparabilidad, se utilizó una rúbrica

de evaluación (ver Anexo E) que califica cada control propuesto en los dos últimos criterios anteriores mediante una escala de 1 a 5 (1 = no cumple; 5 = cumple plenamente). Se definió como umbral de aceptación que un control sea considerado “validado” si obtiene $\geq 3/5$ en pertinencia contextual e implementabilidad incremental; los controles bajo umbral se marcan como “no viable en el corto plazo”.

Esta estrategia no reemplaza una implementación institucional completa, pero sí permite sostener metodológicamente que la propuesta es válida como hoja de ruta técnica, priorizada y contextualizada.

4.3. VALIDACIÓN DE IMPLEMENTACIÓN INCREMENTAL (MÍNIMO VIABLE DE SEGURIDAD)

Considerando las restricciones de recursos descritas, la solución propuesta se valida parcialmente mediante el concepto de implementación incremental, priorizando controles de alto impacto relativo y bajo costo de adopción.

Tabla 54: Gantt de alto nivel para aplicación de controles.

Control / paquete de controles	0–1 mes	1–3 meses	3–6 meses	6–12 meses
Use of cryptography (cifrado en archivos sensibles + medios removibles)	■	■■■■		
Information transfer (reglas mínimas de transferencia + registro básico)	■	■	■■■■	
Classification of information (criterios simples)	■	■■■■		
Labelling of information (etiquetado básico)	■	■	■■■■	
Documented operating procedures (carga, consolidación, respaldo)		■	■	■■■■
Acceptable use (reglas de uso aceptable + compromisos del equipo/pasantes)	■	■■■■		
Information backup (respaldo + verificación básica de restauración)		■	■	■■■■
Information security awareness (phishing + manejo seguro)	■	■	■■■■	■■■■
Information access restriction (restricción práctica por carpetas/archivos)		■	■	■■■■
Incident management planning + response (cómo reportar/recuperar)		■	■	■■■■
Inventory of assets (catastro de activos/documentos críticos)			■	■

Logging / Monitoring activities (registro y monitoreo sistemático)			■	■
Access control / Access rights / Privileged access rights (roles formales)				■
Data masking / Protection of records (enfoque formal y sostenido)				■
Data leakage prevention (prevención de fuga, desarrollo de herramientas)				■

Leyenda:

■ = Ejecución

▨ = Ajuste

4.3.1. MEDIDAS DE IMPLEMENTACIÓN INMEDIATA (BAJO COSTO/COSTO CERO)

Son medidas que pueden iniciarse con recursos institucionales ya disponibles o con esfuerzo acotado, por ejemplo: cifrado de archivos sensibles y medios removibles; definición de reglas mínimas de manejo y transferencia de información; etiquetado básico de archivos sensibles; procedimientos documentados de operación para tareas críticas (carga, consolidación, respaldo); registro manual o semiestructurado de transferencias y accesos relevantes; capacitaciones breves de concientización sobre phishing y manejo de datos.

4.3.2. MEDIDAS DE IMPLEMENTACIÓN DE MEDIANO PLAZO (REQUIEREN GESTIÓN INSTITUCIONAL)

Corresponden a controles que requieren coordinación con áreas TI, apoyo formal o tiempo de configuración, por ejemplo: esquemas más robustos de control de acceso por roles; monitoreo de actividades y logging sistemático; respaldo institucional con verificación de restauración; catastro exhaustivo y gobernanza documental formalizada.

4.3.3. MEDIDAS DE IMPLEMENTACIÓN DE LARGO PLAZO (REQUIEREN PRESUPUESTO E INFRAESTRUCTURA)

Incluyen controles que dependen de inversión y priorización institucional, tales como: soluciones centralizadas de prevención de fuga de datos; plataformas seguras de intercambio documental; modernización de repositorios; fortalecimiento de controles físicos y monitoreo de acceso en dependencias.

4.4. DISCUSIÓN DE RESULTADOS DE VALIDACIÓN

A partir de la estrategia de validación adoptada, se concluye que la solución propuesta es válida en términos técnicos y contextuales, aunque su validación empírica completa (mediante implementación y medición de resultados) queda pendiente para una fase posterior de ejecución institucional.

La principal contribución de esta memoria en materia de validación no es demostrar una reducción cuantitativa inmediata del riesgo (lo que requeriría aplicación efectiva de controles y observación longitudinal), sino demostrar que: el problema fue diagnosticado con un método estructurado; la priorización de riesgos es justificable; los controles propuestos son consistentes con el estándar ISO/IEC 27002:2022; la institución reconoce barreras reales para implementar; aun así, existe un conjunto de medidas iniciales factibles de adoptar. De esta forma se logra aportar, transformando una situación difusa en una ruta de implementación priorizada, técnicamente fundamentada y adaptada a capacidades reales.

4.5. AMENAZAS DE LA VALIDEZ

Al ser una evaluación aplicada a un caso institucional específico, esta validación presenta amenazas que deben declararse:

- **Ausencia de implementación completa:** No se ejecutaron todos los controles propuestos, por lo que no fue posible medir reducción efectiva de incidentes, tiempos de respuesta o mejoras en trazabilidad.
- **Dependencia de una contraparte institucional:** La validación contextual se apoya en información proporcionada por la contraparte entrevistada y en observaciones del levantamiento, lo que puede no capturar completamente la heterogeneidad de prácticas de otras unidades del Ministerio.
- **Evolución institucional y normativa:** Cambios futuros en dotación, presupuesto, estructura organizacional, lineamientos ministeriales, cambios de gobierno, pueden modificar las condiciones de factibilidad de los controles propuestos.
- **Restricciones temporales de una memoria de título:** El horizonte temporal de una memoria de pregrado no permite acompañar ciclos de implementación, adopción y mejora continua.

4.6. PROPUESTA DE VALIDACIÓN FUTURA

Como proyección de esta memoria, se propone que una etapa posterior de implementación institucional incluya una validación empírica con indicadores antes/después. Algunos indicadores posibles son: porcentaje de archivos sensibles cifrados; porcentaje de respaldos ejecutados y verificados; porcentaje de activos documentales inventariados; número de transferencias registradas vs. no registradas; porcentaje de personal capacitado en phishing/manejo de información; tiempo de recuperación ante pérdida de archivo; número de incidentes o cuasi-incidentes reportados por manejo de datos. La medición de estos indicadores permitiría pasar desde una validación de factibilidad y pertinencia a una validación de efectividad.

CAPÍTULO 5: CONCLUSIONES

5.1. CONCLUSIÓN GENERAL Y CUMPLIMIENTO DE OBJETIVOS

La presente memoria abordó el problema de la seguridad de la información en la gestión de antecedentes sensibles en un entorno institucional público, utilizando como caso de estudio a la Comisión de Víctimas de Violencia Institucional (CVVI) del Ministerio de Justicia y Derechos Humanos de Chile. El trabajo se desarrolló desde una perspectiva de Ingeniería Civil Informática, entendiendo que la seguridad de la información no depende únicamente de herramientas tecnológicas, sino de la interacción entre activos, procesos, personas, controles y capacidades organizacionales.

El objetivo general de la memoria fue proponer una metodología de trabajo para robustecer la seguridad de la información, orientada a la identificación, priorización y mitigación de riesgos en activos físicos y digitales involucrados en el registro y gestión de información sensible. A partir del desarrollo del diagnóstico, la priorización de riesgos y el mapeo de controles, se concluye que el objetivo general fue cumplido en términos de diseño metodológico, en tanto se logró construir una propuesta técnicamente fundamentada, contextualizada y alineada con el estándar ISO/IEC 27002:2022.

5.1.1. CARACTERIZACIÓN DEL PROBLEMA Y DEL ENTORNO DE APLICACIÓN

Se logró caracterizar el entorno de trabajo de la CVVI desde una perspectiva de gestión de información, identificando activos críticos, prácticas operativas, vulnerabilidades y puntos de exposición. Esta caracterización permitió evidenciar que el problema de seguridad no se restringe a un sistema informático en particular, sino que se distribuye en una red de elementos sociotécnicos: planillas maestras, documentos físicos, digitalización parcial, transferencias por correo, soportes removibles, espacios físicos y prácticas de trabajo no siempre formalizadas. Este resultado es relevante porque permitió desplazar la discusión desde una noción genérica de “falta de seguridad” hacia una descripción concreta de riesgos observables y gestionables.

5.1.2. IDENTIFICACIÓN Y PRIORIZACIÓN DE RIESGOS

Se identificaron riesgos asociados a confidencialidad, integridad y disponibilidad de la información, y se priorizaron mediante una matriz de severidad basada en probabilidad e impacto. La decisión metodológica de focalizar el análisis en riesgos con severidad Extremo resultó adecuada para el alcance de la memoria, ya que permitió concentrar los esfuerzos en escenarios con mayor impacto potencial sobre la operación institucional y el resguardo de antecedentes sensibles. La priorización cumplió un rol central, ya que transformó un conjunto amplio de vulnerabilidades en una agenda concreta de intervención, evitando una lista dispersa de recomendaciones sin criterio de urgencia.

5.1.3. PROPUESTA DE CONTROLES DE MITIGACIÓN

Se elaboró una propuesta de mitigación para los riesgos extremos, asociando a cada riesgo controles específicos de ISO/IEC 27002:2022, con justificación contextualizada. Este resultado constituye una de las principales contribuciones de la memoria, puesto que entrega una trazabilidad explícita entre riesgo identificado y control propuesto, permitiendo pasar desde el diagnóstico a una hoja de ruta de mejora.

5.1.4. VALIDACIÓN DE LA SOLUCIÓN

La validación es coherente con el alcance y los objetivos de esta memoria, los cuales se orientan a evaluar prácticas de diseño y gestión de bases de datos, evaluar mecanismos de seguridad respecto de ISO/IEC 27001 y 27002:2022, y diseñar un plan de acción con controles recomendados para mitigar riesgos. Así, la solución se valida como propuesta técnica y hoja de ruta mediante tres dimensiones complementarias: (i) consistencia técnica, verificando que los controles propuestos se relacionen adecuadamente con los activos, vulnerabilidades y riesgos identificados y que sean coherentes con ISO/IEC 27002:2022; (ii) pertinencia contextual, contrastando su aplicabilidad con las condiciones operativas reales de la CVVI; e (iii) implementabilidad incremental, identificando un conjunto de medidas de alto impacto y bajo costo que pueden iniciarse progresivamente.

5.2. PRINCIPALES RESULTADOS Y HALLAZGOS

Uno de los principales resultados de esta memoria es haber demostrado que, en el caso analizado, los riesgos más críticos no se concentran únicamente en ‘fallas tecnológicas complejas’, sino en una combinación de brechas de gobernanza de la información (roles, responsabilidades y reglas de decisión poco explicitadas), prácticas operativas no formalizadas, baja trazabilidad, circulación informal de información sensible y debilidades en respaldo e inventario.

En particular, el análisis de riesgos extremos permitió identificar patrones recurrentes de exposición en torno a: accesos no controlados o insuficientemente restringidos a información sensible; alteraciones no detectadas en planillas y procesos de consolidación; fugas de información por transferencia informal (correo, copias locales, medios removibles); pérdida u omisión documental por falta de inventario y respaldo sistemático; debilidades humanas y organizacionales (phishing, ausencia de capacitaciones, sobrecarga operativa); debilidades físicas en el control de acceso a dependencias donde se maneja información reservada.

Este hallazgo refuerza una conclusión importante desde la ingeniería aplicada: la seguridad de la información, especialmente en instituciones públicas, debe abordarse como una capacidad organizacional integral, y no únicamente como la adquisición de software o hardware.

5.3. APORTES E IMPACTO DEL TRABAJO

La contribución principal de esta memoria es la propuesta y aplicación de una metodología sistemática, trazable y replicable para evaluar y mitigar riesgos de seguridad de la información en procesos de registro de víctimas basados en planillas, repositorios documentales y flujos sociotécnicos. Su aplicación en la CVVI demuestra que es posible pasar desde un diagnóstico general de vulnerabilidades a una hoja de ruta priorizada con foco en riesgos de severidad extrema, sustentada en estándares internacionales.

En términos concretos, el trabajo entrega un procedimiento de levantamiento y modelamiento de activos, amenazas y vulnerabilidades; un esquema de priorización de riesgos por severidad; un mapeo justificable de riesgos a controles de ISO/IEC 27002:2022; criterios de pertinencia contextual e implementabilidad incremental para adaptar la propuesta a restricciones reales; y un plan de acción por etapas que puede reutilizarse en otras instituciones con ajustes al contexto.

5.4. ALCANCES Y LIMITACIONES DE LA PROPUESTA

En términos de alcance la memoria logró cumplir sus objetivos, realizando las siguientes actividades: identificar y priorizar riesgos en el caso de estudio; focalizar el análisis en riesgos de severidad extrema; proponer controles de mitigación concretos y justificados; validar la propuesta en términos técnicos y contextuales; establecer un enfoque de implementación incremental, compatible con restricciones institucionales.

Las principales limitaciones del trabajo fueron: **restricciones de recursos en la institución**, la falta de presupuesto, la escasez de capacidades técnicas especializadas y la sobrecarga operacional limitaron la posibilidad de pilotaje; **horizonte temporal acotado de una memoria de pregrado**, la seguridad de la información requiere ciclos de adopción, ajuste y mejora continua que exceden el plazo disponible para este trabajo; y **alcance de estudio de caso**, los resultados son altamente pertinentes para el entorno analizado, pero su generalización a otros organismos requiere adaptación y validación adicional.

5.5. REFLEXIONES SOBRE CAPACIDADES ESTATALES Y FALTA DE PERFILES INFORMÁTICOS

Uno de los aprendizajes más importantes que deja esta memoria es que existe una tensión estructural entre la criticidad de la información gestionada por organismos públicos y la capacidad efectiva disponible para protegerla. En el caso estudiado, esta tensión se expresa en tres dimensiones: restricción presupuestaria, sobrecarga operacional y ausencia o insuficiencia de perfiles especializados en seguridad de la información.

En la práctica, esto genera un escenario en que equipos que trabajan con información altamente sensible deben sostener su operación diaria con recursos limitados, priorizando

tareas urgentes de gestión de casos por sobre actividades de prevención, documentación y fortalecimiento de controles. Este patrón no es excepcional, sino representativo de una problemática más amplia en el sector público: la seguridad de la información tiende a ser abordada de forma reactiva, muchas veces después de un incidente o de una exigencia externa.

5.6. RECOMENDACIONES Y TRABAJO FUTURO

A partir de los resultados obtenidos, se proponen las siguientes líneas de continuidad:

5.6.1. RECOMENDACIONES PARA IMPLEMENTACIÓN INSTITUCIONAL (CORTO Y MEDIANO PLAZO)

1. **Iniciar con medidas de bajo costo y alto impacto:** Tales como cifrado de archivos sensibles y medios removibles; clasificación y etiquetado básico de información; reglas mínimas de transferencia de información; procedimientos documentados para tareas críticas.
2. **Priorizar trazabilidad operativa:** Dado el peso de logging y monitoreo en el conjunto de controles propuestos, se recomienda avanzar tempranamente en mecanismos de registro y seguimiento, incluso si inicialmente son manuales o semiestructurados.
3. **Fortalecer inventario y respaldo:** Consolidar un inventario de activos y un esquema de respaldo verificable constituye una base crítica para continuidad operativa y preservación documental.
4. **Implementar capacitación breve y recurrente:** Capacitaciones prácticas sobre phishing, manejo de información sensible y transferencias seguras pueden reducir riesgos con baja inversión.
5. **Definir responsables por control:** Cada medida priorizada debería tener un responsable explícito de ejecución y seguimiento para evitar que la propuesta quede sólo a nivel documental.

5.6.2. TRABAJO FUTURO

1. **Pilotaje de controles e indicadores antes/después:** Una fase posterior debería implementar un subconjunto de medidas y evaluar su efectividad mediante indicadores de cumplimiento y reducción de incidentes.
2. **Modelo de madurez de seguridad para unidades públicas con recursos limitados:** Futuras investigaciones podrían proponer niveles progresivos de adopción de

controles, adaptados al contexto estatal.

3. **Extensión a otras unidades del Ministerio o a otros organismos públicos:** Replicar la metodología permitiría identificar patrones comunes y ajustar una estrategia más general de fortalecimiento.
4. **Articulación con gobernanza documental y protección de datos:** Una línea de profundización relevante consiste en integrar esta propuesta con políticas de gestión documental y resguardo de datos personales/sensibles.

5.7. CONCLUSIÓN FINAL

La presente memoria permitió abordar un problema real de seguridad de la información en un entorno institucional público caracterizado por alta sensibilidad de los antecedentes, restricciones operativas y limitaciones estructurales de implementación. El principal resultado no fue una plataforma tecnológica desplegada ni una intervención completa, sino la construcción de una propuesta de mitigación de riesgos extremos técnicamente fundamentada, priorizada y contextualizada.

El trabajo demuestra que, incluso en escenarios donde no existen condiciones inmediatas para una implementación integral, es posible generar valor desde la Ingeniería Civil Informática mediante metodologías que permitan diagnosticar, priorizar y proponer medidas viables por etapas. Asimismo, evidencia que la reducción del riesgo en este tipo de contextos depende en gran medida de fortalecer trazabilidad, procedimientos, clasificación, transferencia segura e inventario, antes de pensar exclusivamente en soluciones tecnológicas de mayor complejidad.

Finalmente, la memoria deja una base concreta para futuras decisiones institucionales y para posteriores etapas de implementación y evaluación empírica. En ese sentido, su aporte no se limita a describir un problema, sino que proporciona una ruta de acción técnicamente justificada para avanzar hacia una gestión de información más segura, trazable y consistente con la responsabilidad institucional que implica trabajar con antecedentes sensibles.

REFERENCIAS BIBLIOGRÁFICAS

ACNUDH. (2019). *Informe sobre la Misión a Chile 20 de octubre - 22 de noviembre de 2019. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*. https://www.ohchr.org/sites/default/files/Documents/Countries/CL/Report_Chile_2019_SP.pdf

Badillo, M. (2025). *Chile's New Data Protection Law: Context, Overview, and Key Takeaways*. Future of Privacy Forum. <https://fpf.org/blog/chiles-new-data-protection-law-context-overview-and-key-takeaways/>

Bowker, G. (2008). *Memory practices in the sciences*. <https://mitpress.mit.edu/9780262524896/memory-practices-in-the-sciences/>

Choo, C. W. (2002). *Information Management for the Intelligent Organization: The Art of Scanning the Environment (3rd ed.)*. Information Today Inc.

Date, C. J. (2004). *An Introduction to Database Systems (8th ed.)*.

DAMA International. (2017). *DAMA-DMBOK: Data Management Body of Knowledge (2nd ed.)*. Technics Publications. Dataversity+1

Davenport, T. H. (1997). *Information Ecology: Mastering the Information and Knowledge Environment*. Oxford University Press.

Elmasri, R., & Navathe, S. B. (2015). *Fundamentals of Database Systems (7th ed.)*.

Hanseth, O., & Monteiro, E. (1998). Understanding information infrastructures.

Human Rights Watch. (2020). *World Report 2020: Chile*. Human Rights Watch. <https://www.hrw.org/world-report/2020/country-chapters/chile>

INDH. (2020). *Informe Anual 2020: Situación de los Derechos Humanos en Chile*. Instituto Nacional de Derechos Humanos. <https://bibliotecadigital.indh.cl/items/95b3e91e-ad1a-48c8-bef7-0f63dc35a175>

ISO/IEC. (2022a). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.

ISO/IEC. (2022b). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls*. International Organization for Standardization.

Jiménez-Yañez, C. (2020). #Chiledespertó: causas del estallido social en Chile. *Revista Mexicana De Sociología*, 82(4). <https://doi.org/10.22201/iis.01882503p.2020.4.59213>

Leigh Star, S., & Ruhleder, K. (1996). *Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces*. *Information Systems Research*. <https://doi.org/10.1287/isre.7.1.111>

Lindeberg, J., & Henkel, M. (2024). A Shared Data Model for Improved Documentation of Human Rights Violations. *Journal of Human Rights Practice*, 16(3), 1007-1019. <https://academic.oup.com/jhrp/article/16/3/1007/7729217>

Sasse, L. (2021). *Chile Despertó – The Reasons for the Mass Protests in Chile 2019/2020*. https://www.ipe-berlin.org/fileadmin/institut-ipe/Dokumente/Working_Papers/ipe_working_paper_166.pdf

The Engine Room, & HURIDOCS. (n.d.). *Civil society documentation of human rights abuses*. <https://documentation-tools.theengineroom.org/findings-documentation/>

ANEXOS

ANEXO A: PAUTA DE ENTREVISTA

Presentación

¿Podrías contarnos cuál es tu función actual en la institución y cómo ha sido tu trayectoria en otras instituciones relativas a este tema (víctimas de violencia, femicidios, trata, violencia institucional)? (Acá se podría preguntar si ha tenido otras funciones en la CVVI)

1. ¿Quién se considera responsable de la calidad de los datos (definiciones, consistencia, semántica)?

Misión y organización

¿Cuál es el mandato o propósito de esta Comisión? (explorar si es que ha habido cambios)

¿Cómo está organizado el equipo para cumplirlo? (perfiles profesionales y distribución de tareas)

Sobre el catastro

¿Cómo surgió el catastro? ¿En qué consiste el catastro? ¿por qué o para qué hacer este registro?

¿Qué usos tiene o podría tener?

Preguntas

CONTEXTO

Dentro de mi memoria tengo que identificar estructuras de datos, bases de datos. Ya sabemos del catastro.

- ¿Usan otras? Por ejemplo el excel que tienen para coordinar pasantes.
- Nombra los que recuerdes y cuéntame un poco de:
 - su función, el tipo de dato que almacenan y si se han ido ajustando en el tiempo.
 - Recordar **atención a víctimas presencialmente**.
 - Si no menciona **el uso que se le da** (como seguimiento/estadísticas) preguntar por ese proceso crítico.

Ahora que conocemos las BBDD, me podrías contar

- El “ciclo típico” que tienen?
 - cómo se capturan, actualizan y cierran los datos que entran.
 - de cuáles fuentes beben estos datos (pjud, por ejemplo)
- Quienes son/serían los usuarios dentro y fuera de la subsecretaría
 - (dentro) unidades que interactúan, profesiones que tienen las personas
 - (fuera) INDH, PJUD les pide cosas? ¿Tienen expectativas? (como trazabilidad, confidencialidad) por qué medio piden?

GOBERNANZA Y ROLES

- A propósito del cambio de gobierno ¿bajo quién queda la propiedad de este trabajo? ¿Se entregan los datos a la subsecretaría? ¿Está establecido en alguna resolución, contrato?
- ¿Cuentan con el apoyo de algún profesional informático?
 - de quién depende ese apoyo?
- Sobre el protocolo ¿Se definen políticas de seguridad? (como accesos, uso de información)
- ¿Recibieron o reciben directrices de alguna entidad como gobierno digital? ¿Existe algún lineamiento escrito que manejen?

GESTIÓN DE RIESGO Y CONTROLES

- ¿Cuáles consideran que son los principales riesgos que enfrenta la información que manejan?
 - ej: acceso no autorizado, phishing, ransomware, errores de carga, filtraciones
- Han definido criterios formales para evaluar estos riesgos (si no tienen informático no aplica)
- Tienen algún control para proteger la información?

RECURSOS, COMPETENCIAS Y CULTURA

Sobre las personas que trabajan en el equipo con las BBDD

- ¿Cómo se capacitó al equipo en su uso?
- Cuando alguien nuevo ingresa ¿qué inducción recibe?
- De casualidad hacen actividades de sensibilización sobre riesgos y buenas prácticas?

OPERACIONES EN LAS BBDD

Ahora sobre los accesos a las BBDD

- ¿Cómo son las cuentas que acceden? (correos personales, perfiles, ...)
- ¿Se establecen roles por distintos niveles de permisos? ¿cuales? (lector, editor, ...)
- Cuando alguien se va ¿cómo se gestiona su salida? (se cierra su acceso, quién lo hace?)
- Hay algún registro de quién interviene el Excel y cómo lo hace?
 - ¿Ha habido algún error en el ingreso? han mirado estos registros?
- ¿Se realizan respaldos de información?
 - ¿cómo? defina frecuencia, quien lo hace
- ¿Cómo gestionan cambios necesarios en el excel, de columnas, nuevos campos?
- Cambian información entre instituciones?
 - ¿Cómo lo hacen? (por correo, whatsapp, página web)

MONITOREO

- ¿Manejan algún tipo de métrica para evaluar la seguridad y calidad del dato en la BBDD?
 - ver campos incompletos, errores de carga
- ¿Ha habido algún incidente?
 - como pérdida de algún registro, acceso indebido
- ¿Alguna entidad de la Subsecretaría realiza auditoría sobre cómo se maneja la información?

COMENTARIOS

- Su opinión/perspectiva ¿Qué aspectos funcionan bien y cuales consideran más frágiles o vulnerables?
- ¿Qué cambios/mejoras considera prioritarios para fortalecer la seguridad y calidad de los registros? (en lo técnico, los procesos, la organización)
- ¿Sabe si existen proyectos o cursos planificados (formal o informal) para modernizar sistemas, fortalecer controles?
- ¿Sientes que los marcos normativos (ley de digitalización del estado, privacidad de datos, o normas internas) se han aterrizado de manera concreta en los sistemas o metodologías que ustedes usan? ¿por qué?
- Si pudieras definir condiciones mínimas que debería cumplir un sistema ideal para registrar víctimas ¿cuáles serían?
- ¿Qué recursos técnicos o institucionales te gustaría o necesitarías recibir para concretar esas condiciones?

ANEXO B: ENTREVISTAS Y CORPUS DOCUMENTAL

Entrevistas y reuniones realizadas.

Fecha	Integrantes	Resumen de reunión
30/06/2025	Los cuatro miembros de la Comisión	Se nos dió información inicial sobre la comisión. Los integrantes de la comisión y los integrantes de Data Justa se presentaron.
4/09/2025	Los cuatro miembros de la Comisión y alumnos pasantes	Se coordinó una visita para observar reuniones de trabajo grupal de la Comisión. En estas instancias se revisan casos complejos, se discuten procedimientos y se deciden buenas prácticas dentro del equipo.
26/09/2025	Los cuatro miembros de la Comisión y alumnos pasantes	Se fue nuevamente a observar el trabajo grupal del equipo y los pasantes.
21/11/2025	Encargado de planilla maestra	Se realizó la entrevista semi estructurada del Anexo A.

Corpus Documental

Documento	Descripción
Planilla Maestra	Planilla en Excel que cuenta con los casos de las víctimas de violencia institucional ejercida en el contexto del estallido social de 2019. Centraliza información de distintas fuentes: Poder Judicial, Policías, Organizaciones sociales, Servicio médico legal, entre otros
Excel de estadísticas	Planilla que servía como insumo para los reportes que se hacen periódicamente a la entidad pertinente en el ministerio.
Fojas de Poder Judicial	Documentos descargados desde el portal del poder judicial donde se encontraban las causas de las víctimas.

ANEXO C: TABLA DE CÁLCULO DE CRITICIDAD DE ACTIVOS

Confidencialidad			CID	CRITICIDAD	
Público	1		111	1	Baja
Reservada	3		112	2	Media
			113	3	Alta
Integridad			121	2	Media
Baja	1		122	2	Media
Media	2		123	3	Alta
Alta	3		131	3	Alta
			132	3	Alta
Disponibilidad			133	3	Alta
Baja	1		311	3	Alta
Media	2		312	3	Alta
Alta	3		313	3	Alta
			321	3	Alta
Criticidad			322	3	Alta
Baja	1		333	3	Alta
Media	2		331	3	Alta
Alta	3		332	3	Alta
			333	3	Alta

ANEXO D: TABLA DE CÁLCULO DE SEVERIDAD DEL RIESGO

NIVEL DE PROBABILIDAD (P)	P	NIVEL IMPACTO (I)	I	SR	SEVERIDAD DEL RIESGO $S=(P \times I)$
Casi Certeza	1	Catastróficas	1	11	Extremo
Casi Certeza	1	Mayores	2	12	Extremo
Casi Certeza	1	Moderadas	3	13	Extremo
Probable	2	Catastróficas	1	21	Extremo
Probable	2	Mayores	2	22	Extremo
Moderado	3	Catastróficas	1	31	Extremo
Moderado	3	Mayores	2	32	Extremo
Improbable	4	Catastróficas	1	41	Extremo
Casi Certeza	1	Menores	4	14	Alto
Casi Certeza	1	Insignificantes	5	15	Alto
Probable	2	Moderadas	3	23	Alto
Probable	2	Menores	4	24	Alto
Moderado	3	Moderadas	3	33	Alto
Improbable	4	Mayores	2	42	Alto
Muy Improbable	5	Catastróficas	1	51	Alto
Muy Improbable	5	Mayores	2	52	Alto
Probable	2	Insignificantes	5	25	Moderado
Moderado	3	Menores	4	34	Moderado
Improbable	4	Moderadas	3	43	Moderado
Muy Improbable	5	Moderadas	3	53	Moderado
Moderado	3	Insignificantes	5	35	Baja
Improbable	4	Menores	4	44	Baja
Improbable	4	Insignificantes	5	45	Baja
Muy Improbable	5	Menores	4	54	Baja
Muy Improbable	5	Insignificantes	5	55	Baja

ANEXO E: RÚBRICA DE EVALUACIÓN

Evaluación

Nivel de aceptación	Valoración (1-5)
No cumple	1
Cumple parcialmente	2
Cumple aceptablemente	3
Cumple bien	4
Cumple plenamente	5

Validación de viabilidad

Control para mitigar el riesgo	Pertinencia Contextual	Implementabilidad incremental	Viable a corto plazo
Logging	4	2	NO
Monitoring activities	2	2	NO
Documented operating procedures	3	3	SÍ
Information transfer	5	4	SÍ
Classification of information	4	4	SÍ
Information backup	5	3	SÍ
Change management	4	2	NO
Inventory of information and other associated assets	4	2	NO
Use of cryptography	4	5	SÍ
Acceptable use of information and other associated assets	4	4	SÍ
Data leakage prevention	5	1	NO
Data masking	3	2	NO
Information access restriction	5	3	SÍ
Information security awareness, education and training	4	3	SÍ
Labelling of information	3	4	SÍ
Protection of records	4	2	NO

Security of assets off-premises	4	3	SÍ
Access control	5	2	NO
Access rights	5	2	NO
Clear desk and clear screen	3	4	SÍ
Equipment siting and protection	3	2	NO
Information security incident management planning and preparation	4	3	SÍ
Physical entry	3	2	NO
Physical security monitoring	3	1	NO
Physical security perimeters	3	2	NO
Privileged access rights	4	2	NO
Protection against malware	4	2	NO
Response to information security incidents	4	3	SÍ