Informe de Auditoría Técnica de Sistemas Computacionales y Evaluación de Riesgos de Gobernanza TI para la Ilustre Municipalidad de La Ligua

Tabla de contenido

1. Introducción: El Imperativo de la Modernización en el Nuevo Escenario Regulatorio Chileno 4

2. Marco Metodológico de la Auditoría 6

2.1. Estándares y Marcos de Referencia 6

2.2. Procedimientos de Auditoría Ejecutados 24

3. Análisis Forense de Contratos Tecnológicos 2025 29

3.1. Licitación ID 2783-74-LE24: "Servicio de Mantención de Hardware y Software" 29

3.2. Licitación ID 2784-23-LE24: "Adquisición e Implementación de Plataforma de Software" 30

4. Análisis de Gobernanza TI y Cumplimiento del Reglamento Interno 31

4.1. Evaluación de Madurez COBIT 2019 31

4.2. Análisis de Estructura Organizacional 31

4.3. Gestión de la Propiedad Intelectual y Riesgo Contractual 33

4.4. Ausencia de Documentación Técnica 33

5. Auditoría Técnica: Sistemas Legados y Riesgos 33

5.1. Riesgo Sistémico 34

5.2. Infraestructura de Redes y Seguridad Perimetral 35

5.3. Integridad y Respaldo de Datos (Backup & Recovery) 35

5.4. Desarrollo Web (Laravel/PHP): Riesgos de Implementación 36

Gestión del Proyecto y Retrasos 37

Calidad del Software y Seguridad (AppSec) 37

Evidencias de Seguridad 37

6. Evaluación Funcional y Satisfacción Usuaria 50

6.1. Dimensiones de Evaluación (Resultados de Entrevistas) 50

6.2. Análisis de Usabilidad 52

7. Análisis de Brechas Normativas (Gap Analysis) 52

7.1 Ley N° 21.180 de Transformación Digital del Estado 52

7.2 Ley N° 21.663 Marco de Ciberseguridad 53

7.3 Protección de Datos Personales (Ley 19.628 / Proyecto Ley) 54

8. Matriz de Hallazgos y Clasificación de Riesgos (Consolidada) 54
8.1. Marco Metodológico de la Matriz 54
8.2. Matriz Detallada 54
9. Propuesta de Líneas de Trabajo Críticas 56
Línea 1: Aseguramiento de la Continuidad y Propiedad (Inmediato - Mes 1) 56
Línea 2: Mitigación de Ciberseguridad de Emergencia (Corto Plazo - Mes 1-3) 56
Línea 3: Blindaje de Infraestructura e Identidad (Corto Plazo - Mes 1 a 3) 56
Línea 4: Licitar Alternativas de Mercado (Corto Plazo - Mes 2-4) 57
Línea 5: Auditoría y Saneamiento Financiero (Corto Plazo - Mes 2 a 4) 57
Línea 6: Plan de Migración y Modernización (Mediano Plazo - Mes 4-12) 58
Línea 7: Gestión del Cambio y Capacitación (Transversal) 58
Línea 8: Reestructuración del Gobierno TI (Mediano Plazo - Mes 3 a 6) 58
10. Evaluación Estratégica: ¿Desarrollo Propio o Software de Mercado? 59
10.1. Análisis de Costo Total de Propiedad (TCO) y Riesgo 59
11. Conclusiones 61
12. ANEXO 63
13. Bibliografía 68

1. Introducción: El Imperativo de la Modernización en el Nuevo Escenario Regulatorio Chileno

La administración pública en Chile atraviesa el momento de transformación más profundo de las últimas tres décadas. La convergencia de marcos normativos estructurales ha redefinido el estándar de lo que constituye una gestión municipal diligente, desplazando la tecnología desde un rol de soporte administrativo hacia una función crítica de gobernanza, transparencia y continuidad operacional. Para la Ilustre Municipalidad de La Ligua, este nuevo escenario no representa una opción, sino un mandato legal imperativo cuyo incumplimiento acarrea responsabilidades administrativas, civiles y políticas severas para la autoridad edilicia y los jefes de servicio.

El presente documento técnico constituye el informe final de la auditoría de sistemas realizada a la infraestructura computacional, el desarrollo de software y los procesos de gobernanza de Tecnologías de la Información (TI) de la Ilustre Municipalidad de La Ligua. Este análisis exhaustivo surge de la necesidad imperiosa de evaluar la sostenibilidad, seguridad y legalidad del ecosistema tecnológico actual, en un contexto nacional marcado por la entrada en vigencia de normativas exigentes como la Ley de Transformación Digital del Estado (Ley N° 21.180) y la Ley Marco de Ciberseguridad (Ley N° 21.663).

En primer lugar, la **Ley N° 21.180 de Transformación Digital del Estado** ha establecido un cronograma perentorio para la digitalización de los procedimientos administrativos. Esta normativa no busca la mera "digitalización del papel" (PDF), sino la tramitación electrónica nativa, la interoperabilidad de datos entre instituciones y la notificación electrónica fehaciente. La realidad observada en La Ligua, caracterizada por sistemas legados desconectados y procesos manuales en departamentos críticos como Rentas y Obras, colisiona frontalmente con la fase de implementación de la ley, que exige para 2025 un avance sustantivo en la integración con las plataformas transversales del Estado (DocDigital, ClaveÚnica, PIE).[1] El incumplimiento de estas fases no es un problema técnico menor; es una barrera de acceso a la justicia administrativa para los ciudadanos de La Ligua.

En segundo lugar, la promulgación de la **Ley N° 21.663, Ley Marco de Ciberseguridad**, eleva la seguridad de la información a un asunto de seguridad pública. Los municipios, como tenedores de datos territoriales y prestadores de servicios esenciales, quedan sujetos a la regulación de la Agencia Nacional de Ciberseguridad (ANCI). La auditoría ha detectado que la infraestructura municipal se sustenta en tecnologías obsoletas (Visual Basic 6.0, SQL Server 2000) que carecen de soporte de seguridad hace más de una década. Bajo la nueva ley, operar con sistemas "End-of-Life" (EOL) sin medidas compensatorias puede ser constitutivo de infracción grave, dado que expone los datos de los vecinos a riesgos

inminentes de exfiltración, secuestro (Ransomware) y destrucción, sin capacidad de respuesta ante incidentes.[3]

En tercer lugar, la **Ley N° 21.719 sobre Protección de Datos Personales** impone un régimen de sanciones draconiano (multas de hasta 20.000 UTM) y establece la responsabilidad proactiva (*accountability*) en el tratamiento de datos. Los sistemas actuales de La Ligua, diseñados en una época donde la privacidad no era un requisito de arquitectura, carecen de controles granulares de acceso, trazabilidad de auditoría y mecanismos de cifrado. La gestión de fichas sociales, datos de salud y deudas tributarias en plataformas vulnerables sitúa al municipio en una posición de responsabilidad legal directa ante la nueva Agencia de Protección de Datos.[6]

Finalmente, la **Ley N° 21.634 de Modernización de Compras Públicas** exige estándares superiores de probidad, eficiencia y planificación en el gasto público. El análisis de los contratos tecnológicos vigentes en La Ligua revela una dependencia crónica de un proveedor único, adjudicaciones directas o licitaciones sin competencia real, y la adquisición de servicios de desarrollo sobre tecnologías muertas. Estas prácticas, bajo la nueva óptica de la Contraloría General de la República (CGR) y la Dirección de Compras Públicas, pueden ser observadas como una falta al principio de eficiencia y una vulneración a la libre competencia, perpetuando un "Vendor Lock-in" (secuestro tecnológico) que drena recursos municipales sin aportar valor público moderno.[8]

Este informe desglosa, con evidencia técnica y documental, cómo la brecha entre la realidad operativa de La Ligua y el mandato legal se ha vuelto insostenible, proponiendo una hoja de ruta crítica para evitar el colapso funcional de los servicios municipales.

2. Marco Metodológico de la Auditoría

Para garantizar que los hallazgos de esta auditoría sean objetivos, trazables y técnicamente irrefutables, se ha diseñado un marco metodológico híbrido que integra estándares internacionales de auditoría de sistemas, marcos de gestión de riesgos gubernamentales y mejores prácticas de ingeniería de software.

2.1. Estándares y Marcos de Referencia

La auditoría se estructura sobre la base de cinco pilares normativos y técnicos:

1. **NIST SP 800-30 Rev. 1 (Guide for Conducting Risk Assessments):** Este estándar del Instituto Nacional de Estándares y Tecnología de EE.UU. se utiliza como la metodología central para la evaluación de riesgos. Permite descomponer el riesgo tecnológico en sus factores atómicos: Amenazas (ej. ciberatacantes, fallas de hardware), Vulnerabilidades (ej. software sin parches, falta de segmentación), Probabilidad de Ocurrencia e Impacto en la Misión. Este enfoque asegura que cada hallazgo técnico (ej. "Despliegue de sistemas con configuración por defecto") se traduzca en un riesgo de negocio cuantificable.[10]

   La guía establece que el riesgo es una medida de la extensión en que una entidad está amenazada por una circunstancia o evento potencial. El riesgo se determina típicamente como una función de:

   1. La probabilidad de que ocurra el evento de amenaza.
   2. El impacto adverso que resultaría si el evento ocurriese.

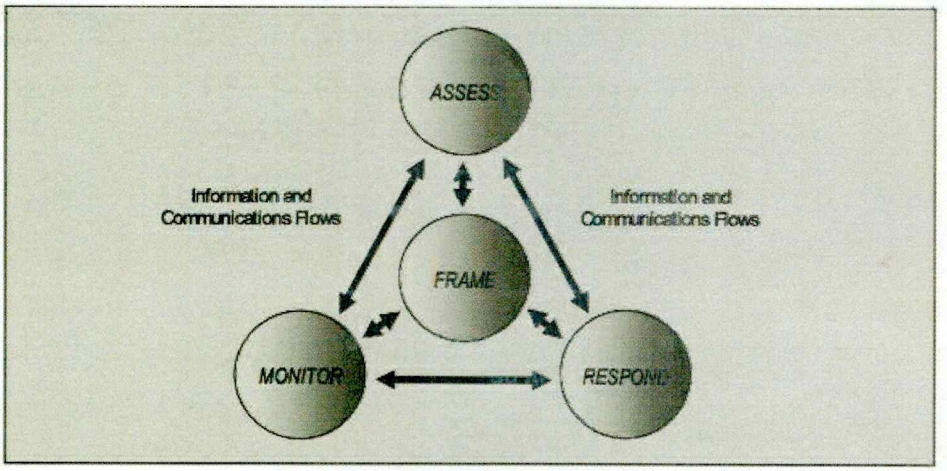


Figura 1: Evaluación de riesgos dentro del proceso de gestión de riesgos. Extraído de NIST SP 800-30 Rev1.

Factores de Riesgo Clave

Para evaluar el riesgo, se analizan los siguientes componentes:

- Amenazas (Threats): Cualquier circunstancia o evento con el potencial de impactar adversamente las operaciones y activos de la organización. Se dividen en fuentes de amenaza (quién o qué origina la amenaza) y eventos de amenaza (qué sucede).
- Vulnerabilidades: Debilidades en un sistema de información, procedimientos de seguridad, controles internos o implementación que podrían ser explotadas por una fuente de amenaza.
- Condiciones Predisponentes: Condiciones existentes en la organización (como la ubicación geográfica o la arquitectura de red) que aumentan o disminuyen la probabilidad de que una amenaza tenga éxito.
- Probabilidad (Likelihood): La posibilidad de que una amenaza inicie un ataque o evento y de que este resulte en un impacto adverso.
- Impacto (Impact): La magnitud del daño que se espera como resultado de las consecuencias de la divulgación, modificación, destrucción o pérdida de información.

Jerarquía de Gestión de Riesgos

Las evaluaciones pueden realizarse en tres niveles o "tiers":

- Nivel 1 (Organización): Riesgos que afectan la gobernanza y estrategia general.
- Nivel 2 (Procesos de Misión/Negocio): Riesgos asociados con los procesos de negocio y la arquitectura empresarial.
- Nivel 3 (Sistemas de Información): Riesgos desde la perspectiva de los sistemas técnicos y operacionales.

El Proceso de Evaluación de Riesgos

El documento define un proceso de cuatro pasos para la evaluación de riesgos:

Paso 1: Preparación para la Evaluación

El objetivo es establecer el contexto. Las actividades incluyen:

- Identificar el propósito y el alcance de la evaluación.

- Definir suposiciones y restricciones (ej. recursos disponibles).
- Identificar las fuentes de información (ej. reportes previos, inteligencia de amenazas).
- Seleccionar el modelo de riesgo y el enfoque analítico (cuantitativo, cualitativo o semi-cuantitativo).

Paso 2: Realización de la Evaluación

Es el núcleo del proceso, donde se analizan las amenazas y vulnerabilidades para determinar el riesgo. Incluye las siguientes tareas:

- Identificar Fuentes de Amenaza: Determinar quiénes son los adversarios (capacidad, intención, objetivo) o las fuentes no adversarias (ej. desastres naturales, errores humanos).
- Identificar Eventos de Amenaza: Definir qué eventos podrían ser producidos por esas fuentes.
- Identificar Vulnerabilidades y Condiciones Predisponentes: Encontrar las debilidades que podrían ser explotadas.
- Determinar la Probabilidad: Estimar la probabilidad de que la amenaza inicie el evento y de que tenga éxito.
- Determinar el Impacto: Estimar el daño a las operaciones, activos o individuos si se explota la vulnerabilidad.
- Determinar el Riesgo: Combinar la probabilidad y el impacto para calcular el nivel de riesgo final.

Paso 3: Comunicación de Resultados

El objetivo es asegurar que los tomadores de decisiones tengan la información necesaria.

- Comunicar los resultados a las partes interesadas (ej. mediante informes ejecutivos o dashboards).
- Compartir información relacionada con el riesgo para apoyar otras actividades de gestión.

Paso 4: Mantenimiento de la Evaluación

Dado que los riesgos cambian, la evaluación debe mantenerse actualizada.

- Monitorear continuamente los factores de riesgo (nuevas amenazas, cambios en sistemas).
- Actualizar la evaluación de riesgos basándose en los resultados del monitoreo.

Apéndices y Herramientas

El documento incluye apéndices extensos (D al I) que sirven como "plantillas" y catálogos para facilitar la evaluación, proporcionando:

- Taxonomías de fuentes de amenazas (ej. hackers, errores, fallos estructurales).
- Ejemplos de eventos de amenazas (ej. phishing, inyección SQL, incendios).
- Escalas para medir probabilidad e impacto (ej. Muy Bajo a Muy Alto).
- Tablas para la determinación del nivel de riesgo final.

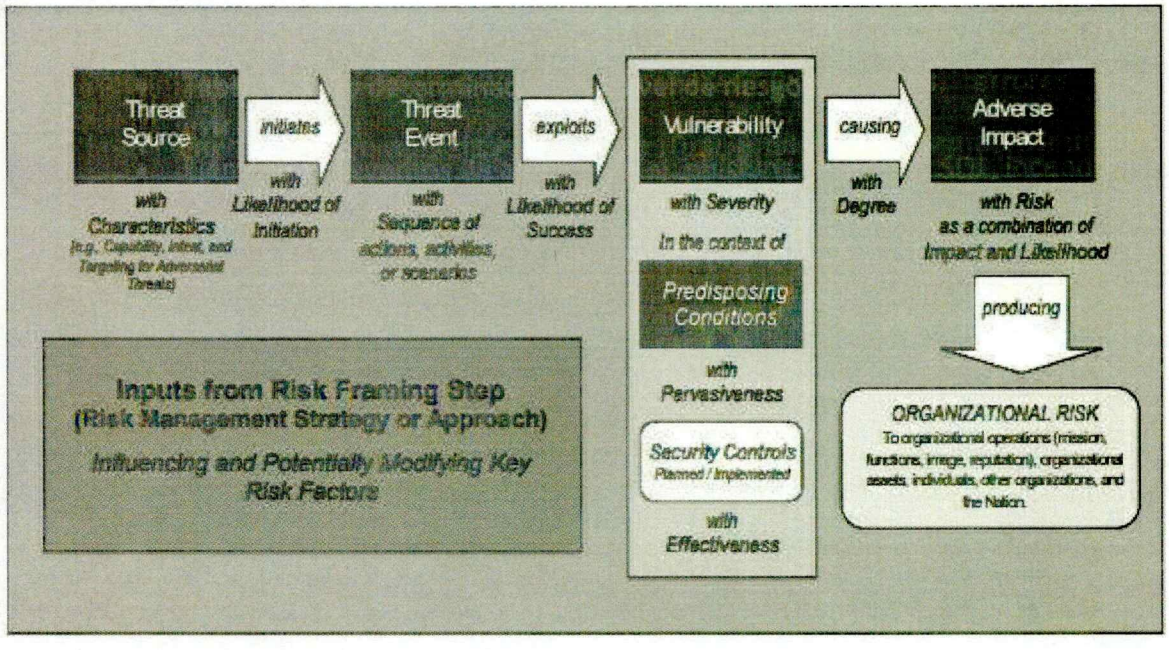


Figura 2: Modelo de riesgos genéricos con indicadores clave. Extraído de NIST SP 800-30 **Rev1.**

2. **COBIT 2019 (Control Objectives for Information and Related Technologies):** Se emplea para evaluar la madurez de la Gobernanza de TI. Específicamente, se analizan

los objetivos de los dominios *Align, Plan and Organize* (APO) para la gestión de riesgos y *Build, Acquire and Implement* (BAI) para la gestión de proyectos de software. COBIT permite determinar si el municipio cuenta con los procesos de toma de decisiones necesarios para alinear la TI con la estrategia comunal.[12]



Figura 3: De Haes, Steven; W. Van Grembergen; Enterprise Governance of Information Technology: Achieving Alignment and Value, Presentando COBIT 5, Springer International Publishing, Switzerland, 2.ª ed. 2015,

COBIT 2019 es un marco de referencia para el gobierno y la gestión de la información y la tecnología (I&T) de la empresa. Su objetivo principal es ayudar a las empresas a crear valor mediante la obtención de beneficios, la optimización de riesgos y la optimización de recursos.

El marco hace una distinción clara entre dos disciplinas:

- Gobierno: Asegura que se evalúen las necesidades de las partes interesadas, se establezca la dirección mediante la priorización y se monitoree el desempeño. Es responsabilidad del consejo de administración.
- Gestión: Planifica, construye, ejecuta y monitorea actividades alineadas con la dirección establecida por el gobierno. Es responsabilidad de la dirección ejecutiva.

Principios de COBIT

COBIT 2019 se basa en dos conjuntos de principios:

1. Principios para un Sistema de Gobierno:

- Proporcionar valor a las partes interesadas.
- Enfoque holístico (creado por distintos componentes que funcionan juntos).
- Sistema de gobierno dinámico (debe considerar el impacto de cambios en la estrategia o tecnología).

- Separar el gobierno de la gestión.
- Adaptar a las necesidades de la empresa (personalización mediante factores de diseño).
- Sistema de gobierno íntegro (cubrir la empresa de principio a fin, no solo el departamento de TI).

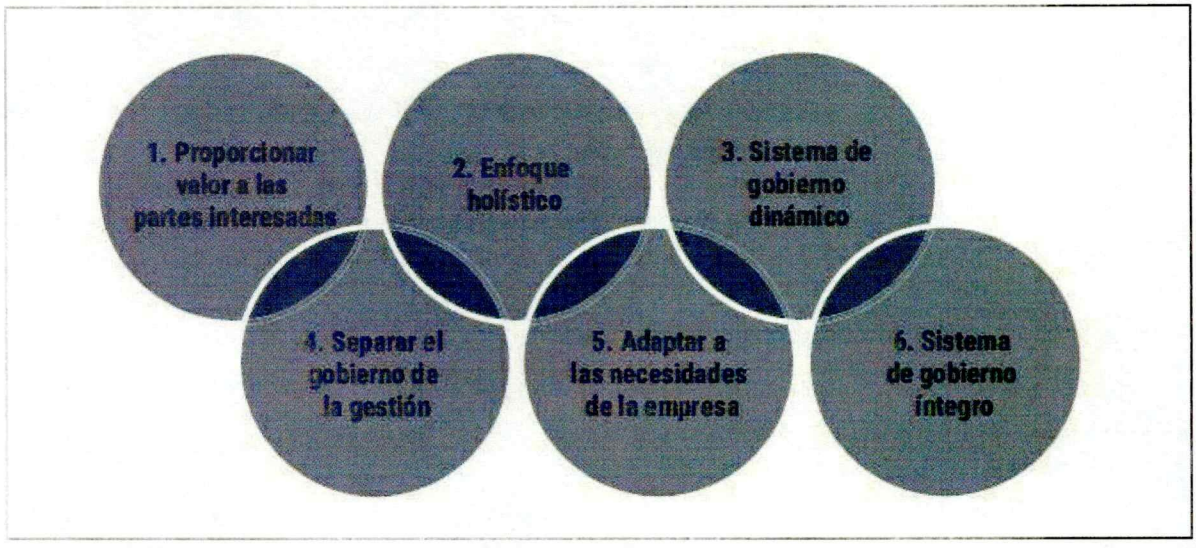


Figura 3: Huygh, T.; S. De Haes; "Using the Viable System Model to Study IT Governance Dynamics: Evidence from a Single Case Study", Actas de la 51.ª Conferencia Internacional de Hawái sobre Ciencias de Sistemas, 2018.

2. Principios para un Marco de Gobierno:

- Basado en un modelo conceptual.
- Abierto y flexible.
- Alineado con las principales normativas y estándares.

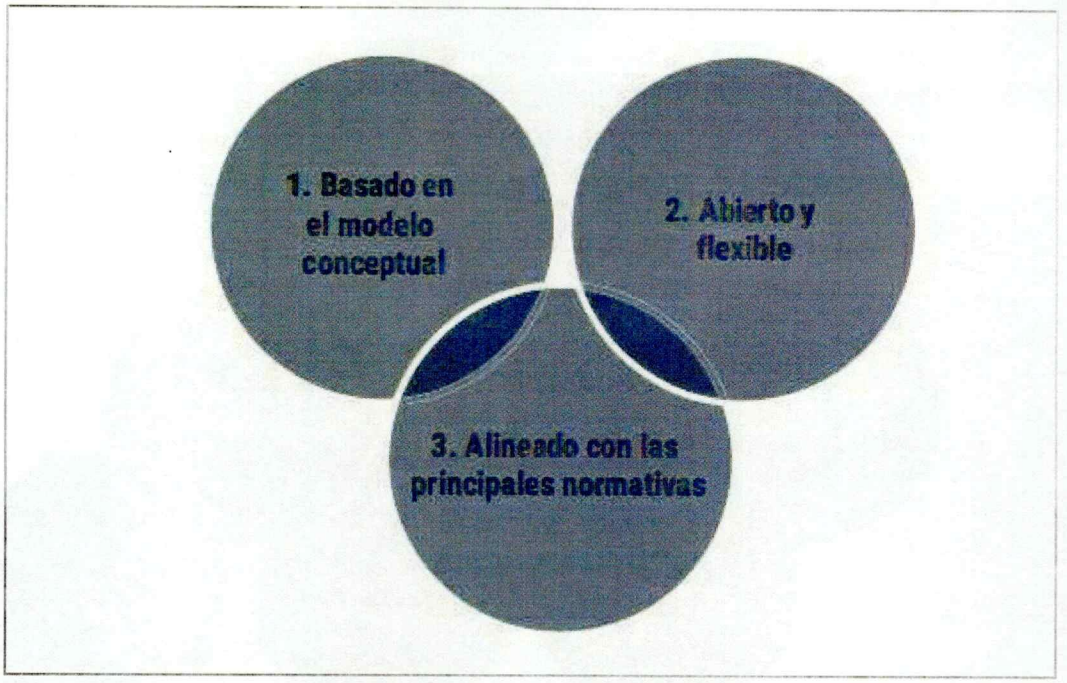


Figura 4: Huygh, T.; S. De Haes; "Using the Viable System Model to Study IT Governance Dynamics: Evidence from a Single Case Study", Actas de la 51.ª Conferencia Internacional de Hawái sobre Ciencias de Sistemas, 2018.

Modelo Core y Objetivos

El modelo central de COBIT organiza los objetivos de gobierno y gestión en cinco dominios:

1. EDM (Evaluar, Dirigir y Monitorizar): Objetivos de gobierno.
2. APO (Alinear, Planificar y Organizar): Estrategia y organización.
3. BAI (Construir, Adquirir e Implementar): Definición y adquisición de soluciones.
4. DSS (Entregar, Dar Servicio y Soporte): Ejecución operativa y seguridad.
5. MEA (Monitorizar, Evaluar y Valorar): Conformidad y desempeño.

En total, existen 40 objetivos de gobierno y gestión distribuidos en estos dominios.

Componentes del Sistema de Gobierno

Para alcanzar los objetivos, el sistema de gobierno se construye a partir de siete tipos de componentes interactivos:

1. Procesos.
2. Estructuras organizativas.
3. Principios, políticas y procedimientos.
4. Información.
5. Cultura, ética y comportamiento.
6. Personas, habilidades y competencias.
7. Servicios, infraestructura y aplicaciones.

Factores de Diseño y Cascada de Metas

COBIT 2019 introduce los Factores de Diseño para personalizar el sistema de gobierno según el contexto de la empresa. Estos incluyen la estrategia empresarial, el perfil de riesgo, el tamaño de la empresa, el rol de TI, el panorama de amenazas, entre otros.

La Cascada de Metas es el mecanismo que traduce las necesidades de las partes interesadas en objetivos accionables:

1. Impulsores y necesidades de las partes interesadas.
2. Metas empresariales (13 metas organizadas en el cuadro de mando integral).
3. Metas de alineamiento (alineación de esfuerzos de TI con el negocio).
4. Objetivos de gobierno y gestión.

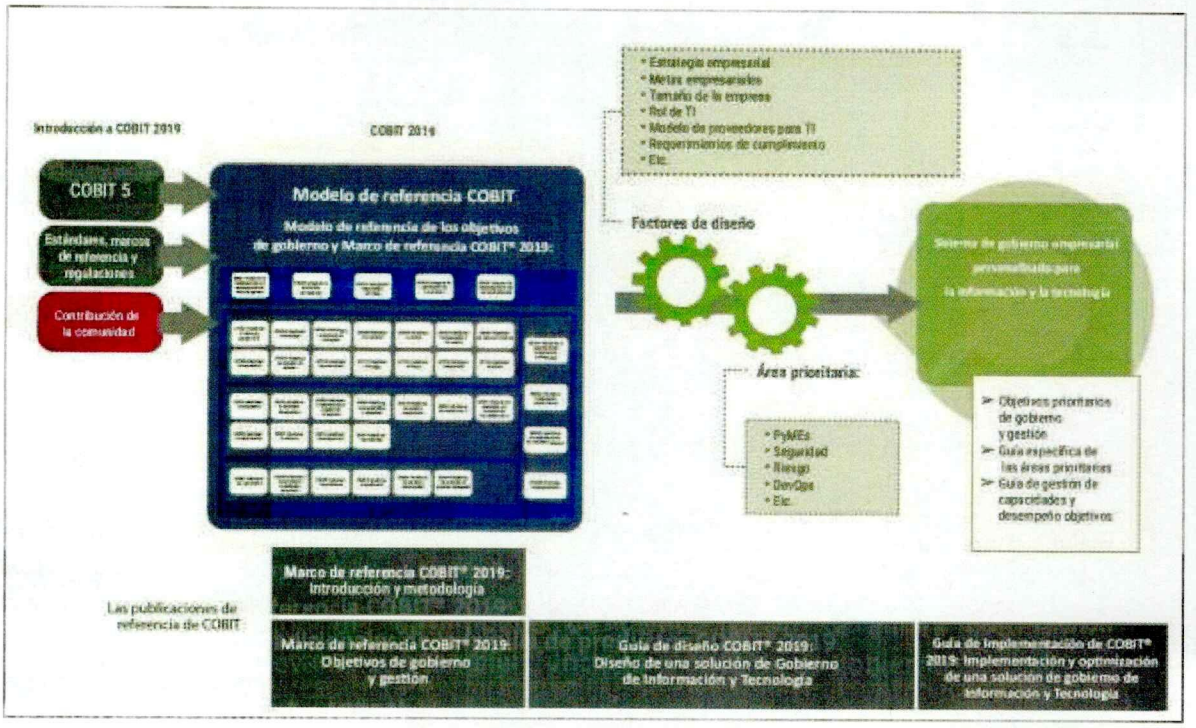


Figura 5: Marco de referencia COBIT® 2019: Introducción y metodología, están previstos títulos adicionales de la familia de productos COBIT® 2019.

Gestión del Desempeño (CPM)

El modelo de gestión del desempeño de COBIT (CPM) se alinea con CMMI Development V2.0 y evalúa qué tan bien funciona el sistema de gobierno.

- Niveles de Capacidad (Procesos): Escala del 0 al 5 que mide qué tan bien se implementa y funciona un proceso.
- Niveles de Madurez (Áreas Prioritarias): Asociados con colecciones de objetivos de gobierno y gestión (áreas prioritarias); se alcanzan si se logran los niveles de capacidad requeridos en los procesos subyacentes.

Diseño e Implementación

El documento describe un flujo de trabajo para diseñar un sistema personalizado en cuatro pasos:

1. Entender el contexto y estrategia de la empresa.

2. Determinar el alcance inicial.
3. Perfeccionar el alcance (considerando factores como amenazas o rol de TI).
4. Finalizar el diseño (resolviendo conflictos de prioridades).

3. **CIS Controls v8.1 (Center for Internet Security):** Utilizado como la lista de verificación técnica para la ciberseguridad defensiva. Se audita el cumplimiento de los controles del Grupo de Implementación 1 (IG1), diseñado para organizaciones con recursos limitados pero que manejan datos sensibles. El foco está en el Control 02 (Inventario de Software) y Control 07 (Gestión de Vulnerabilidades).[15]



Figura 6: Ciber Higiene Esencial. CIS Controls V.8.1.

Los Controles CIS (CIS Critical Security Controls) son un conjunto priorizado de acciones recomendadas para la ciberdefensa, diseñadas para proteger a las organizaciones y sus datos de vectores de ataque conocidos. Esta versión (8.1) es una actualización iterativa que busca mejorar el contexto, la claridad y la consistencia, alineándose con otros marcos de seguridad importantes.

Conceptos Clave

Grupos de Implementación (IGs) Para ayudar a organizaciones de diferentes tamaños a priorizar, los controles se dividen en tres Grupos de Implementación:

- IG1 (Higiene Cibernética Esencial): Diseñado para pequeñas y medianas empresas con experiencia limitada en TI y ciberseguridad. Se enfoca en proteger los activos y el personal contra ataques generales y no dirigidos.

- IG2: Para empresas con infraestructura de TI dedicada y múltiples departamentos con diferentes perfiles de riesgo. A menudo almacenan información sensible y pueden estar sujetas a cumplimiento normativo.
- IG3: Para empresas con expertos en seguridad especializados y que manejan datos o funciones sensibles sujetas a supervisión regulatoria. Deben defenderse contra ataques dirigidos y sofisticados.

Clases de Activos El documento define clases de activos para agrupar elementos similares que requieren protección, incluyendo Dispositivos, Software, Datos, Usuarios, Red y Documentación.

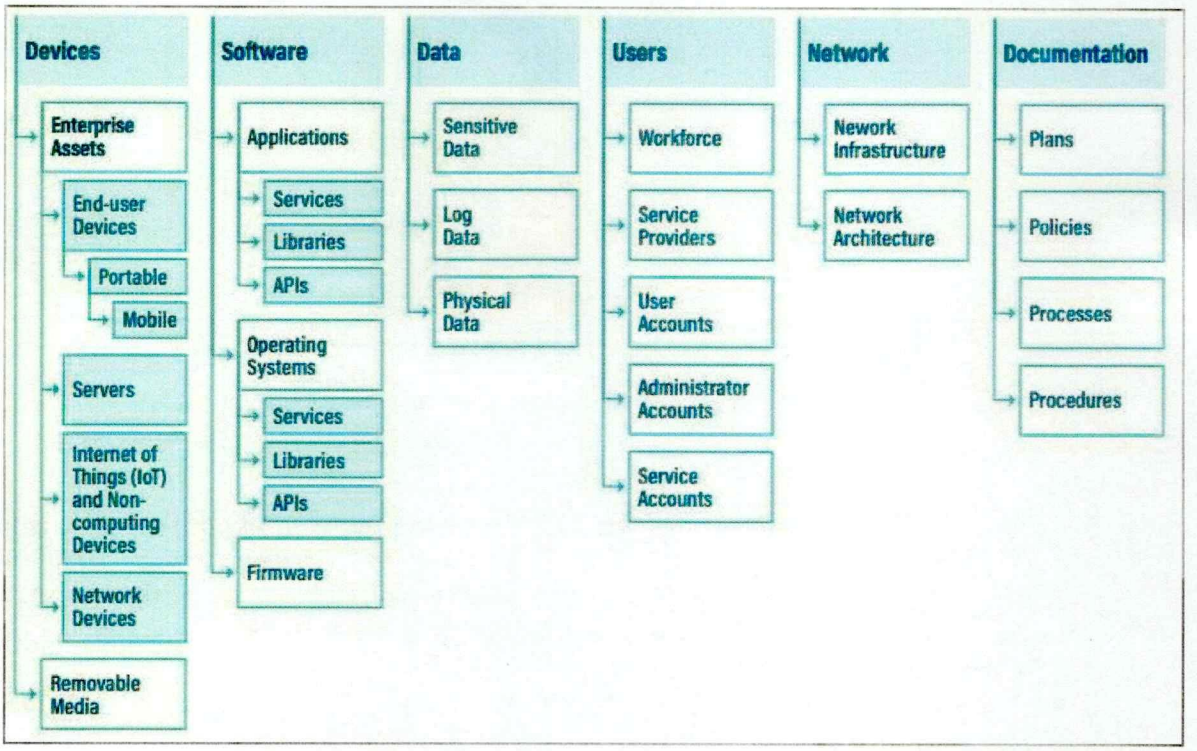


Figura 7: Clases de Activos. CIS Controls V.8.1.

Resumen de los 18 Controles de Seguridad CIS

Los controles se agrupan por funciones lógicas para cubrir todo el espectro de la ciberseguridad:

1. Inventario y Control de Activos Empresariales: Gestionar activamente (rastrear, inventariar y corregir) todos los dispositivos conectados (físicos, virtuales, remotos, nube) para evitar activos no autorizados.
2. Inventario y Control de Activos de Software: Gestionar todo el software en la red para asegurar que solo se instale y ejecute software autorizado, previniendo la ejecución de programas no autorizados o no gestionados.
3. Protección de Datos: Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y eliminar datos de manera segura, protegiéndolos en reposo y en tránsito.
4. Configuración Segura de Activos y Software: Establecer y mantener configuraciones seguras para dispositivos y software (sistemas operativos y aplicaciones) para evitar brechas de seguridad causadas por configuraciones predeterminadas inseguras.
5. Gestión de Cuentas: Gestionar la asignación y autorización de credenciales para cuentas de usuario, administrador y servicio, asegurando que solo los usuarios autorizados tengan acceso.
6. Gestión de Control de Acceso: Crear, asignar, gestionar y revocar credenciales de acceso y privilegios, asegurando que los usuarios solo tengan el acceso necesario para su rol (principio de mínimo privilegio).
7. Gestión Continua de Vulnerabilidades: Evaluar y rastrear continuamente vulnerabilidades en todos los activos empresariales para remediar y minimizar la ventana de oportunidad para los atacantes.
8. Gestión de Registros de Auditoría (Logs): Recopilar, alertar, revisar y retener registros de auditoría de eventos para ayudar a detectar, entender y recuperarse de un ataque.
9. Protecciones de Correo Electrónico y Navegador Web: Mejorar las protecciones contra amenazas provenientes de vectores de correo y web, que son vías comunes para manipular el comportamiento humano (ingeniería social).
10. Defensas contra Malware: Prevenir o controlar la instalación, propagación y ejecución de aplicaciones o códigos maliciosos en los activos empresariales.
11. Recuperación de Datos: Establecer prácticas de recuperación de datos (copias de seguridad) suficientes para restaurar activos a un estado previo al incidente y confiable.
12. Gestión de Infraestructura de Red: Establecer, implementar y gestionar activamente dispositivos de red (físicos y virtuales) para evitar que los atacantes exploten servicios de red vulnerables.

13. Monitoreo y Defensa de Red: Operar procesos y herramientas para mantener un monitoreo integral de la red y defensa contra amenazas de seguridad en toda la infraestructura.
14. Concienciación y Capacitación en Seguridad: Mantener un programa de concienciación para influir en el comportamiento de la fuerza laboral y asegurar que sean conscientes de la seguridad y tengan las habilidades adecuadas.
15. Gestión de Proveedores de Servicios: Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos sensibles o plataformas críticas, asegurando que protejan esos activos adecuadamente.
16. Seguridad del Software de Aplicaciones: Gestionar el ciclo de vida de seguridad del software (desarrollado internamente o adquirido) para prevenir, detectar y remediar debilidades de seguridad.
17. Gestión de Respuesta a Incidentes: Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (políticas, planes, roles definidos) para prepararse y responder rápidamente a un ataque.
18. Pruebas de Penetración: Probar la efectividad y resistencia de los activos mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología), simulando las acciones de un atacante.

4. **ISO/IEC 27001 e ISO 31000:** La norma ISO 31000 proporciona los principios y el marco de trabajo para la gestión de riesgos a nivel organizacional, asegurando que los riesgos TI se integren en la matriz de riesgos global del municipio. La ISO 27001 se utiliza como referencia para los controles de seguridad de la información exigidos por la Ley 21.663.[18]

   El propósito de la norma ISO 31000 es proporcionar directrices para gestionar el riesgo al que se enfrentan las organizaciones. Es un enfoque común aplicable a cualquier tipo de organización, industria o sector, y puede utilizarse a lo largo de la vida de la organización y en cualquier actividad, incluida la toma de decisiones.

   Definiciones Clave

   El documento establece términos fundamentales para entender la gestión del riesgo:

   - Riesgo: Se define como el "efecto de la incertidumbre sobre los objetivos". Este efecto puede ser positivo, negativo o ambos.
   - Gestión del riesgo: Son las actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

- Parte interesada: Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

Principios de la Gestión del Riesgo

El propósito fundamental de la gestión del riesgo es la creación y protección del valor. Los principios que sustentan esto son:

1. Integrada: Es parte de todas las actividades de la organización.
2. Estructurada y exhaustiva: Para obtener resultados coherentes y comparables.
3. Adaptada: Se ajusta a los contextos externo e interno y a los objetivos de la organización.
4. Inclusiva: La participación de las partes interesadas permite considerar sus conocimientos y puntos de vista.
5. Dinámica: Anticipa, detecta, reconoce y responde a los cambios y eventos.
6. Mejor información disponible: Se basa en datos históricos, actualizados y expectativas futuras, considerando sus limitaciones.
7. Factores humanos y culturales: Reconoce la influencia del comportamiento humano y la cultura en la gestión del riesgo.
8. Mejora continua: Mejora mediante el aprendizaje y la experiencia.

Marco de Referencia

El marco de referencia busca asistir a la organización en la integración de la gestión del riesgo en todas sus funciones y actividades significativas.

- Liderazgo y compromiso: La alta dirección debe asegurar que la gestión del riesgo esté integrada y demostrar liderazgo publicando políticas, asignando recursos y estableciendo responsabilidades.
- Componentes: El marco implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo.

Proceso de Gestión del Riesgo

Aunque el documento provisto es una vista parcial, el proceso se ilustra como un ciclo iterativo que incluye los siguientes componentes principales:

1. Comunicación y consulta.
2. Alcance, contexto y criterios.

3. Evaluación del riesgo:
    - Identificación del riesgo.
    - Análisis del riesgo.
    - Valoración del riesgo.
4. Tratamiento del riesgo.
5. Seguimiento y revisión.
6. Registro e informe.

Este proceso debe ser parte integral de la gestión y la toma de decisiones, estructurado para adaptarse a las necesidades específicas de la organización.

En tanto, la norma internacional ISO/IEC 27001:2022. Establece los requisitos para crear, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Objetivo Principal

El propósito de la norma es permitir a las organizaciones de cualquier tamaño o sector proteger su información mediante la gestión de riesgos, asegurando tres pilares fundamentales (la tríada CID):

- Confidencialidad: Que la información no esté disponible ni sea revelada a personas no autorizadas.
- Integridad: Que la información sea exacta y completa.
- Disponibilidad: Que la información esté accesible cuando se necesite.

Introduce cambios significativos para modernizar la seguridad frente a las amenazas digitales actuales:

- Reestructuración de Controles (Anexo A): Se simplificó la lista de controles de seguridad.
    - Antes: 114 controles en 14 dominios.
    - Ahora: 93 controles agrupados en solo 4 temas:
        1. Organizacionales (37 controles).
        2. De Personas (8 controles).
        3. Físicos (14 controles).
        4. Tecnológicos (34 controles).
- 11 Nuevos Controles: Se incorporaron controles modernos que no existían explícitamente en la versión anterior:
    - Inteligencia de amenazas.

- Seguridad de la información para el uso de servicios en la nube.
- Preparación de las TIC para la continuidad del negocio.
- Monitoreo de la seguridad física.
- Gestión de la configuración.
- Eliminación de información.
- Enmascaramiento de datos.
- Prevención de fuga de datos.
- Actividades de monitoreo.
- Filtrado web.
- Codificación segura.

- Cambios en las Cláusulas de Gestión:
  - Planificación de cambios (Cláusula 6.3): Se añade un requisito explícito para que cualquier cambio en el sistema de gestión se planifique adecuadamente.
  - Roles y responsabilidades (Cláusula 5.3): Se enfatiza la comunicación de roles de seguridad dentro de la organización.

Estructura de la Norma

La norma sigue la "Estructura de Alto Nivel" (HLS) para integrarse fácilmente con otras normas ISO (como la ISO 9001). Sus capítulos principales son:

1. Contexto de la organización: Entender las necesidades de las partes interesadas y definir el alcance.
2. Liderazgo: Compromiso de la alta dirección y política de seguridad.
3. Planificación: Evaluación y tratamiento de riesgos
4. Soporte: Recursos, competencias y concientización.
5. Operación: Ejecución de los planes y control operacional.
6. Evaluación del desempeño: Auditoría interna y revisión por la dirección.
7. Mejora: Acciones correctivas y mejora continua.

Importancia para Chile

La adopción de esta norma (NCh 27001:2023) es clave para el cumplimiento de nuevas exigencias en Chile, como la Ley Marco de Ciberseguridad, ya que se perfila como el estándar de referencia para demostrar la debida diligencia en la protección de activos de información en organizaciones tanto públicas como privadas.

5. **ITIL 4 (Information Technology Infrastructure Library):** Empleado para evaluar la "Evaluación Funcional y Satisfacción Usuaria". Se analiza la gestión de servicios, la mesa de ayuda y la entrega de valor desde la perspectiva del usuario funcionario, utilizando el modelo de DeLone & McLean como marco teórico para medir el éxito de los sistemas de información.[20]

Contexto y Propósito

El documento introduce el marco de gestión de servicios ITIL 4, actualizándolo para la Cuarta Revolución Industrial. Se enfoca en cómo las organizaciones modernas deben ser ágiles, colaborativas y centradas en la automatización y la experiencia del cliente.

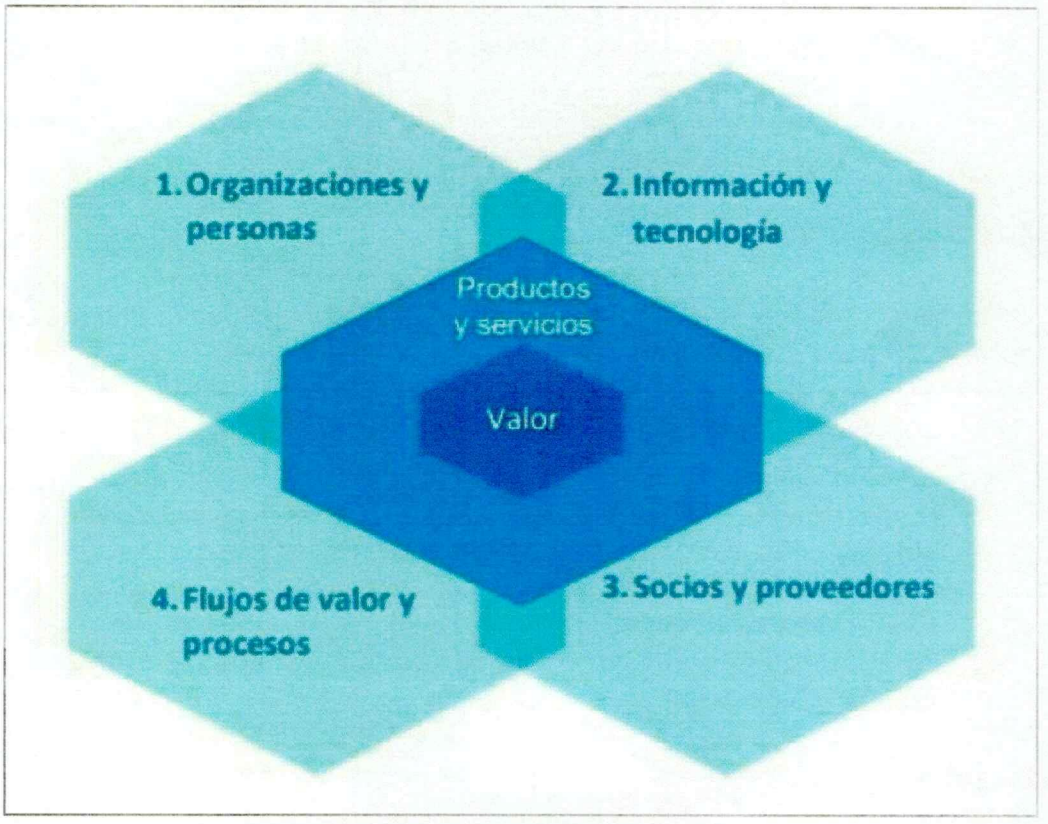


Figura 8: Valor. Itil V4.

Conceptos Fundamentales del Nuevo Modelo ITIL 4

A diferencia de versiones anteriores centradas en procesos, ITIL 4 adopta un enfoque más holístico basado en la creación de valor:

- Sistema de Valor del Servicio (SVS): Es el componente central de ITIL 4. Representa cómo todos los componentes y actividades de la organización trabajan juntos para facilitar la creación de valor.
- Cadena de Valor del Servicio (Service Value Chain): Un modelo operativo flexible que define las actividades clave necesarias para responder a la demanda y facilitar la creación de valor a través de productos y servicios.
- Gestión del Valor: Se enfatiza que el valor no es solo la entrega del servicio, sino la co-creación de beneficios entre el proveedor y el consumidor.

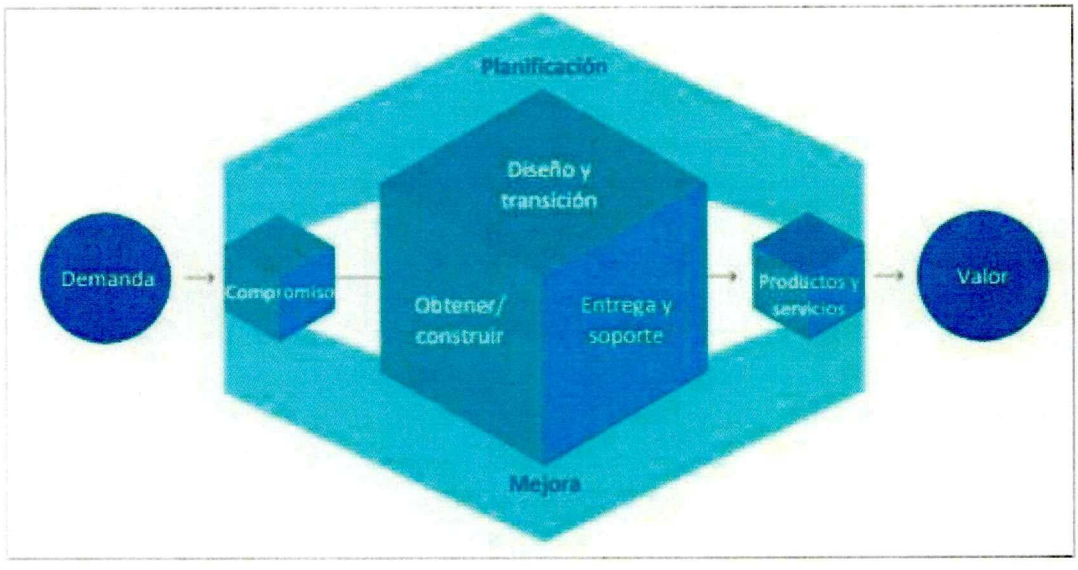


Figura 9: Ciclo fundamental del servicio y mejora continua. Itil V4.

Componentes Clave

1. Principios Guía: Recomendaciones universales que guían a la organización en cualquier circunstancia (ej. "Enfocarse en el valor", "Progresar iterativamente", "Colaborar y promover la visibilidad").
2. Gobierno: Establece que la dirección y el control de las TI son responsabilidad de la alta dirección, asegurando que las TI se alineen con las estrategias del negocio.

3. Prácticas (en lugar de Procesos): ITIL 4 reestructura los antiguos procesos en tres tipos de prácticas:
    - Prácticas de gestión general.
    - Prácticas de gestión de servicios.
    - Prácticas de gestión técnica.

Relación con Otras Metodologías

Se destaca la integración de ITIL 4 con nuevas formas de trabajo como DevOps, Lean y Agile, reconociendo la necesidad de unificar el desarrollo (Dev) y la operación (Ops) en un flujo continuo para ofrecer productos complejos de manera coordinada.

2.2. Procedimientos de Auditoría Ejecutados

La auditoría informática consiste en un examen crítico de los sistemas municipales para verificar su funcionamiento, implementación y pertinencia. El objetivo general es asegurar que los sistemas existentes (ejemplo: Juzgado Local, Activo Fijo, Bodega, Licencias de Conducir, Permisos de Edificación, Contabilidad y Reloj Control) cumplan sus requisitos funcionales, operen de manera segura y eficiente, y respondan a las necesidades actuales del municipio. Además, se verificará el cumplimiento normativo y la gestión adecuada de la seguridad y los datos.

Objetivos de la auditoría

- Evaluar la funcionalidad de cada sistema de la muestra, comprobando que ofrezca los procesos esperados y genere la información requerida. Según definiciones estándar, la auditoría de sistemas "revisa y evalúa los controles y sistemas informáticos existentes" para garantizar su eficacia. Se verificará que cada aplicación cumpla con los requisitos acordados y responda adecuadamente a los procesos municipales.
- Analizar la implementación técnica: esto incluye revisar el código, la configuración de los servidores/aplicaciones, la documentación técnica (manuales de usuario, especificaciones, diagramas de flujos) y la calidad de desarrollo. Se comprobará que hayan existido pruebas de sistema documentadas y que se hayan corregido los errores detectados.
- Medir la pertinencia y utilidad: se evaluará si cada sistema responde efectivamente a las necesidades actuales de la municipalidad (por ejemplo, coherencia con normativa vigente y con otras plataformas oficiales) o si existen duplicidades o

funcionalidades obsoletas. Se entrevistará a los usuarios clave para conocer su percepción de la utilidad real de las aplicaciones.

- Verificar la seguridad y cumplimiento normativo: se analizará la política de acceso, contraseñas y roles definidos en cada sistema, así como la protección de datos personales almacenados. Asimismo, se comprobará el cumplimiento de normativas aplicables, decretos sobre comunicaciones electrónicas, y políticas internas del municipio).

Alcance y cronograma

La auditoría cubre como muestra algunos los sistemas informáticos desarrollados por el prestador para la municipalidad, a saber: *Juzgado de Policía Local, Contabilidad, Tesorería, Patentes Municipales, Gestión de Permisos de Edificación y Remuneraciones*. El trabajo se realiza de la siguiente manera:

- Revisión técnica de sistemas: El auditor inspecciona cada sistema desde el punto de vista técnico. Las actividades incluyen:
  - Revisión de documentación disponible (contratos de desarrollo, manuales). Comprobar que existan especificaciones formales del sistema y registros de versiones.
  - Acceso físico a los equipos/servidores donde operan las aplicaciones. Se solicitan pruebas funcionales representativas para cada sistema (por ejemplo, registrar una nueva multa en el Juzgado Local, gestionar decreto de pago, generar planilla de remuneraciones, etc.). Esto permite validar que las funcionalidades clave operan correctamente.
  - Evaluación de seguridad lógica: verificación de políticas de usuario/rol, contraseñas seguras, mecanismos de autenticación (por ejemplo, si usa firma digital), y registros de eventos (logs de acceso o transacciones). Se examina si los sistemas incluyen control de versiones de los datos (auditorías internas) y cifrado de información sensible.
  - Inspección de las bases de datos asociadas a los sistemas: analiza estructura de tablas y consistencia de datos. También se comprueba que existan copias de seguridad automatizadas y un plan de recuperación, realizando pruebas puntuales de restauración si es posible.
  - Análisis de integración con otros sistemas (por ejemplo, conexión con el SII, Registro Civil o plataforma de pagos si aplica) y cumplimiento de estándares locales.

- Revisión de licencias de software (third-party libraries) y contratos con proveedores, asegurando que no haya incumplimiento de propiedad intelectual.

- Entrevistas y recolección de información: Se destina a reuniones con el personal clave:
  - Usuarios finales y jefes de área: por cada sistema de la muestra se entrevista a funcionarios para indagar sobre la operatividad diaria de la aplicación, su facilidad de uso, problemas comunes, y si el sistema satisface sus necesidades. Se recogerá feedback sobre posibles fallos u oportunidades de mejora.
  - Profesionales responsables o proveedores de TI: se entrevista al desarrollador externo o responsable técnico de cada sistema para comprender las decisiones de diseño, el lenguaje de programación usado, la estructura del código y el mantenimiento realizado. Se requiere evidencia de documentación de desarrollo, bitácoras de cambios y pruebas de calidad ejecutadas.
  - Auditores de control interno (si corresponde): coordinar con la unidad de control interno para comparar hallazgos y obtener políticas internas de TI.

Lista de verificación general (checklist)

La auditoría emplea listas de verificación para asegurar un examen exhaustivo. A continuación, algunos ítems clave agrupados por área:

- **Documentación y procesos de desarrollo:**
  - Existe documentación formal de requisitos funcionales y técnicos para cada sistema.
  - Se disponen de manuales de usuario, diagramas de flujo, manuales de administración y resúmenes de casos de prueba.
  - Se revisaron los contratos con el proveedor: debe quedar claro si el municipio recibió el código fuente (y no solo el ejecutable).
  - Se verificaron bitácoras o registros de control de versiones (por ejemplo, repositorios GIT) y reportes de pruebas realizadas.
- **Seguridad de la información:**
  - Accesos lógicos: Validar que cada usuario tenga rol apropiado y que existan políticas de contraseña (cambio periódico, complejidad). Verificar si se usa autenticación de dos factores o firma digital en procesos críticos.

  - Seguridad física y operativa: Confirmar que los servidores y terminales donde operan los sistemas estén protegidos físicamente (cámaras, cierre con llave, accesos restringidos).
  - Seguridad de base de datos: Corroborar que los accesos a la base de datos estén limitados (solo credenciales encriptadas), y que existan usuarios administrativos separados de los operacionales. Chequear si hay logs de auditoría de la base de datos.
  - Protección de datos personales: Revisar cómo se almacenan RUT y otros datos sensibles, asegurando cifrado o mecanismos de anonimización según normativa de protección de datos.
- **Integridad de datos y operación:**
  - Confirmar existencia de respaldos periódicos de bases de datos y archivos críticos (idealmente automatizados en horario fuera de operación). Probar restauración de al menos una copia.
  - Analizar la integridad referencial: verificar que las tablas principales tengan llaves primarias y foráneas que eviten registros huérfanos. Buscar duplicados o registros incongruentes mediante consultas de prueba.
  - Revisar índices y rendimiento: comprobar que las consultas de uso frecuente estén indexadas adecuadamente para evitar lentitud. Monitorear tiempos de respuesta básicos del sistema.
  - Chequear sincronización entre sistemas (por ejemplo, si el sistema de Activo Fijo envía información a Finanzas) y consistencia entre módulos.
- **Cumplimiento legal y administrativo:**
  - Verificar que los desarrollos cumplen con decretos presidenciales que exigen formatos estándar de intercambio (DS 77/2004, DS 93/2006), uso de RFC correcto y conservación de documentos electrónicos.
  - Asegurar que los sistemas consideren la Ley de Transparencia (p. ej. históricos de roles/altas/bajas que puedan requerirse en informes).
  - Comprobar contratos de licencia de software de terceros incluidos (deben tener copia de licencias vigentes).
- **Propiedad intelectual y registro de software:**
  - Confirmar en el contrato que los derechos de autor fueron cedidos al municipio. De acuerdo con la ley de derechos de autor chilena, los programas producidos "por encargo de un tercero" se reputan cedidos a dicho tercero (en este caso el municipio) salvo estipulación en contrario. Es decir, legalmente el municipio es titular de los sistemas desarrollados.
- **Verificación con usuarios:**

- Evaluar nivel de satisfacción de los usuarios clave: preguntarse si los tiempos de respuesta son adecuados, si conocen los procedimientos, y si existe capacitación suficiente.
- Comprobar que no haya resistencias o "soluciones informales" paralelas (por ejemplo, registros en Excel externos a la aplicación) que indiquen falta de fiabilidad del sistema.

Revisión de las bases de datos

- Backups y recuperación: validar que exista una política de respaldo (por ejemplo, copias diarias o diferenciales) y que estas copias sean recuperables. Se intentará restaurar al menos parte de una base a un servidor de prueba para confirmar la viabilidad de recuperación ante desastres.
- Controles de auditoría: comprobar si la base de datos registra auditoría de transacciones (por ejemplo, triggers o logs de auditoría de cambios) para operaciones sensibles. Esto complementa la revisión de logs del propio sistema.

Entrevistas y compilación de evidencias

Se consolida la información obtenida. Se documentan las impresiones de los usuarios sobre cada sistema (usabilidad, principales problemas) y se contrastan con lo observado técnicamente. Las entrevistas con los desarrolladores/responsables permiten aclarar dudas técnicas (por ejemplo, por qué no se incluyó una función X, o cómo se aborda la continuidad del sistema). Además, se recopilan evidencias adicionales: pantallazos de configuraciones, reportes de bases de datos, registros de auditoría, contratos completos y cualquier información relevante entregada en el momento. Todo hallazgo (fortaleza o debilidad) se registra con su evidencia.

Adicionalmente, el despliegue de la auditoría se realizó mediante procedimientos de validación cruzada:

- **Revisión Documental Forense:** Se analizaron las Bases Administrativas, Especificaciones Técnicas y Decretos de Adjudicación de las licitaciones ID 2783-74-LE24 y ID 2784-23-LE24. Se buscaron inconsistencias, cláusulas abusivas, requisitos limitantes de la competencia y definiciones de propiedad intelectual contrarias a la jurisprudencia de la CGR.[23]
- **Entrevistas en Profundidad:** La evaluación se fundamenta en un levantamiento de información detallado que incluyó entrevistas en profundidad con los actores clave de la gestión tecnológica municipal: el Sr. Edison Maldonado, desarrollador externo y proveedor histórico de los sistemas, y el Sr. Luis Valenzuela, encargado del

Departamento de Informática Municipal. Asimismo, se incorporó la perspectiva de los usuarios finales de las unidades críticas de negocio —Rentas, Finanzas, Adquisiciones, Recursos Humanos y Salud— para contrastar la visión técnica con la realidad operativa diaria.

- **Análisis de Brechas (Gap Analysis):** Se comparó la arquitectura actual (VB6/SQL Legacy) contra los requisitos de interoperabilidad del Decreto 12/2023 del MINSEGPRES, determinando la factibilidad técnica de cumplimiento.

3. Análisis Forense de Contratos Tecnológicos 2025

La revisión exhaustiva de los procesos de contratación pública para el año 2025 expone una estrategia de adquisición de tecnología que contraviene los principios de eficiencia, modernización y libre competencia. A continuación, se detalla el análisis forense de los actos administrativos y contratos.

3.1. Licitación ID 2783-74-LE24: "Servicio de Mantención de Hardware y Software"

Este contrato, adjudicado mediante el Decreto Alcaldicio N° 10218 de fecha 31 de diciembre de 2024, compromete un monto de **$33.600.000** anuales al proveedor **Edison Mauricio Maldonado Villagra** (RUT 11.348.957-k). El análisis revela hallazgos críticos:

A. Simulación de Competencia y Dependencia Absoluta:
El acta de evaluación 25 confirma que el Sr. Maldonado fue el único oferente. En el mercado tecnológico chileno, donde existen cientos de empresas de desarrollo y soporte, la ausencia de competencia para un contrato de esta envergadura es anómala.

- *Causa Raíz:* Las Bases Técnicas exigen experiencia específica en tecnologías obsoletas (Visual Basic 6.0, SQL Server 6.5/7.0, Crystal Report 6.0). Al solicitar conocimientos sobre herramientas que el mercado abandonó hace 15 años, el municipio *de facto* excluye a cualquier proveedor moderno, diseñando una licitación a la medida del incumbente.
- *Implicancia Legal:* Esto podría vulnerar el principio de libre concurrencia de la Ley 19.886. La CGR ha dictaminado reiteradamente que las bases no pueden contener cláusulas que dirijan la adjudicación a un proveedor específico salvo justificación técnica fundada, la cual no se sostiene cuando la "necesidad técnica" es mantener obsolescencia.[26]

B. Perpetuación de la Deuda Técnica:
El contrato tiene por objeto la "mantención" de sistemas legados. Sin embargo, no incluye cláusulas de modernización, migración o refactorización del código. El municipio está

pagando por mantener con vida artificial sistemas que Microsoft declaró "End of Life" (EOL) en 2008.

- *Impacto Financiero:* El costo de oportunidad es inmenso. Por $33.6M anuales, el municipio podría suscribir licencias SaaS (Software as a Service) de ERPs municipales modernos (como CAS Chile, SMC, o similares) que incluyen soporte, actualizaciones legales y seguridad por diseño, eliminando la carga de mantenimiento de infraestructura.

3.2. Licitación ID 2784-23-LE24: "Adquisición e Implementación de Plataforma de Software"

Adjudicada por Decreto N° 9574 el 05 de diciembre de 2024 por un monto de **$50.000.000** al mismo proveedor, Edison Maldonado.[25]

A. Conflicto de Interés Estructural:
El mismo proveedor encargado de "mantener" los sistemas antiguos (y que, según las entrevistas, controla el acceso al código y base de datos) es contratado para desarrollar el "nuevo" sistema.

- *Riesgo de Captura:* El proveedor tiene el incentivo perverso de hacer que la migración sea lenta o incompleta para asegurar la renovación del contrato de mantención de los sistemas legados. No existe un tercero independiente (QA o Auditoría) que valide que el nuevo software cumpla con los estándares modernos y no sea simplemente una "lavada de cara" (porting) del código antiguo con las mismas vulnerabilidades.

B. Propiedad Intelectual y Código Fuente:
Las bases mencionan "Desarrollo y Mantención (Sin Copia de Códigos Fuentes)" en secciones de los TDR antiguos, aunque el nuevo contrato habla de adquisición. Existe una ambigüedad contractual crítica.

- *Análisis Jurídico:* Si el municipio paga por el desarrollo de una obra por encargo ("work for hire"), los derechos patrimoniales deben pertenecer al municipio según la Ley 17.336 de Propiedad Intelectual y dictámenes de la CGR.[24] Si el proveedor retiene el código fuente, el municipio queda secuestrado: no puede licitar la mantención a otro proveedor en el futuro, no puede auditar la seguridad del código y no puede integrarlo libremente con el Estado. El proveedor declaró en entrevista que "el desarrollo es de él", lo que constituye una alerta roja de apropiación de patrimonio público.

C. Carencia de Garantías Técnicas:
El contrato no especifica estándares de seguridad (OWASP ASVS), pruebas de carga o cumplimiento de la Norma Técnica de Ciberseguridad (Decreto 7). Se está adquiriendo un "caja negra" sin certificar que sea segura para procesar datos de los vecinos.

4. Análisis de Gobernanza TI y Cumplimiento del Reglamento Interno

La Gobernanza de TI en la I. Municipalidad de La Ligua se encuentra en un estado de **madurez incipiente (Nivel 0-1 según escala COBIT)**, caracterizado por la dependencia de personas ("héroes") en lugar de procesos institucionalizados.

4.1. Evaluación de Madurez COBIT 2019

Utilizando los objetivos de gestión de COBIT 2019, se identifican las siguientes brechas críticas:

1. **APO12 - Gestionar el Riesgo:**
   - *Estado:* Inexistente. No hay una matriz de riesgos de TI formalizada ni un apetito de riesgo definido por el Alcalde o el Concejo. Los riesgos de ciberseguridad (Ransomware) y operativos (caída de sistemas) se gestionan de manera reactiva ("apagar incendios") una vez que ocurren.
   - *Impacto:* El municipio es ciego a su propia exposición. La falta de evaluación de riesgos impide justificar presupuestos para seguridad o modernización ante el Concejo.[12]
2. **BAI03 - Gestionar la Identificación y Construcción de Soluciones:**
   - *Estado:* Deficiente. La decisión de "construir" (desarrollo propio externalizado) vs "comprar" (SaaS de mercado) no se basó en un caso de negocio formal o estudio de TCO (Total Cost of Ownership). Se optó por la inercia de continuar con el proveedor conocido, ignorando las soluciones de mercado que ya resuelven la problemática municipal de forma estandarizada.[14]
3. **DSS05 - Gestionar los Servicios de Seguridad:**
   - *Estado:* Crítico. La seguridad depende de un firewall perimetral (Unifi) y antivirus básicos (Avast/Defender). No hay gestión de parches (Patch Management), no hay SIEM (monitoreo de eventos), ni SOC. La "seguridad" se delega en un proveedor externo que accede vía AnyDesk, una práctica de alto riesgo que viola los principios de acceso seguro y trazabilidad.[16]

4.2. Análisis de Estructura Organizacional

Uno de los hallazgos más relevantes de esta auditoría es la dependencia extrema y estructural de un único proveedor externo. El concepto de "Bus Factor" (Factor de Autobús) refiere al número de miembros clave de un equipo que, si fueran atropellados por un autobús (o dejaran de estar disponibles por cualquier razón), causarían el colapso del proyecto. En el caso de La Ligua, el Bus Factor es 1.

Según lo recabado, "El proyecto Visual Basic solo está el desarrollador y prestador de servicio como responsable y contraparte técnica, sin considerar el soporte técnico que también residen en el mismo prestador". Tanto el sistema legado, que sostiene la operación crítica de ingresos (Rentas) y permisos de circulación, como el nuevo desarrollo web, residen intelectual y operativamente en la figura de Edison Maldonado. Esta situación contraviene directamente el principio de segregación de funciones y continuidad del negocio. COBIT 2019, en su objetivo APO07 (Gestionar los Recursos Humanos), enfatiza la necesidad de minimizar la dependencia de individuos clave mediante la gestión del conocimiento y la documentación.

La realidad operativa descrita es precaria: "En periodos peak no hay respuesta en el momento porque depende de la disponibilidad del prestador de servicios". Esto implica que durante los periodos críticos de recaudación (Marzo y Agosto para Permisos de Circulación, Julio y Enero para Patentes Comerciales), el municipio queda expuesto a un riesgo de denegación de servicio operativo. Si el proveedor sufre una emergencia médica o decide unilateralmente cesar el servicio, el municipio carece de capacidad interna para mantener, reparar o incluso reiniciar los sistemas complejos que dependen de su intervención manual.

Además, la estructura interna del Departamento de Informática es débil. El encargado, Luis Valenzuela, "depende del administrador" y no se identifican roles claros de especialización. No existe un Encargado de Ciberseguridad o similar, ni un Encargado de Transformación Digital formalmente empoderado y con conocimientos específicos ("Encargado de Td: no sabe", "Encargado de Ciberseguridad: no saben, Luis parece"). Esta indefinición de roles incumple los requisitos de la Ley Marco de Ciberseguridad, que exige a los organismos del Estado designar contrapartes técnicas responsables ante la ANCI para la gestión de crisis.

ARTICULO 12°: El Departamento de Informática dependerá del Administrador/a Municipal y estará a cargo de un(a) Encargad(a) de Informática, y tendrá las siguientes funciones:

a) Administrar, coordinar y controlar el funcionamiento del equipamiento informático de la Municipalidad;
b) Administrar los sistemas y programas computacionales de la Municipalidad, adoptando las normas técnicas y de seguridad para su adecuado uso;
c) Instruir y capacitar al personal municipal sobre el adecuado uso del equipamiento y programas computacionales;
d) Mantener un catastro actualizado de todo el equipamiento y programas informáticos de la Municipalidad;
e) Efectuar tareas de mantención y todas las demás necesarias para el adecuado funcionamiento de los equipos y programas computacionales; y,
f) Otras funciones que le sean encomendadas por su superior, o conforme a la reglamentación vigente.

Figura 10: Funciones Departamento de Informática. Decreto Alcaldicio N°1315 de fecha 16 de febrero 2021. I Municipalidad de La Ligua.

4.3. Gestión de la Propiedad Intelectual y Riesgo Contractual

La auditoría identificó un vacío legal significativo respecto a la propiedad de los activos de software. Aunque se indica que "el desarrollo dice que es de él pero que no tiene problema con dejárselo a la muni", se admite explícitamente que "no aparece en el contrato".

Esta ambigüedad representa un riesgo patrimonial mayor. Según la Ley N° 17.336 de Propiedad Intelectual en Chile, la titularidad del software desarrollado por un externo no se transfiere automáticamente al mandante (el municipio) a menos que exista una cláusula de cesión de derechos expresa y por escrito. En el escenario actual, el municipio ha financiado durante años el desarrollo de un activo sobre el cual no tiene control legal.

Desde la perspectiva de los estándares de seguridad, esto viola el control SA-4 (Acquisition Process) de NIST SP 800-53 , que exige a las organizaciones incluir requisitos de seguridad y propiedad en los contratos de adquisición. La falta de acceso al código fuente ("Administran documentación bbdd, no hay código") coloca al municipio en una situación de "secuestro tecnológico" o Vendor Lock-in. Sin el código fuente, es imposible realizar auditorías de seguridad independientes (SAST), corregir vulnerabilidades críticas o migrar los datos hacia otra plataforma sin la cooperación voluntaria del proveedor actual.

4.4. Ausencia de Documentación Técnica

La gestión del conocimiento es inexistente. Se reporta: "Documentación bases de datos: no hay documentación", "Documentación código: no hay". Solo existen manuales de usuario, los cuales son insuficientes para la administración técnica del sistema.

Esta carencia incumple el control SA-5 (System Documentation) de NIST y hace inviable cualquier plan de continuidad que no involucre al desarrollador actual. Si el municipio decidiera contratar a un nuevo equipo de ingenieros para mantener el sistema actual, estos se enfrentarían a una "caja negra" indescifrable, elevando los costos y tiempos de cualquier intervención a niveles prohibitivos. La falta de un diccionario de datos o modelo entidad-relación documentado explica, en parte, los problemas de integridad de datos reportados por los usuarios (duplicidad de registros, inconsistencias en reportes), ya que no existe una "fuente de verdad" arquitectónica que guíe el desarrollo y mantenimiento.

5. Auditoría Técnica: Sistemas Legados y Riesgos

La inspección técnica de los activos de información confirma un escenario de obsolescencia tecnológica que compromete la seguridad nacional y la continuidad del servicio. El núcleo transaccional del municipio opera sobre una plataforma tecnológica que ha sido mantenida por más de 15 años, donde su mantención, soporte y proyección esta ligada a un único proveedor.

5.1. Riesgo Sistémico

El sistema principal e implementado totalmente fue desarrollado en 2001 utilizando Microsoft Visual Basic 6.0. Es imperativo señalar que Microsoft declaró el fin del soporte extendido para VB6 el 8 de abril de 2008. Esto significa que la plataforma base sobre la que recauda el municipio lleva 17 años sin recibir actualizaciones de seguridad, parches de corrección de errores o mejoras de compatibilidad por parte del fabricante.

- Vulnerabilidades: Microsoft cesó el soporte de VB6 en 2008. El *runtime* no recibe parches de seguridad. Las aplicaciones VB6 dependen de librerías COM/ActiveX que son vectores frecuentes de ataques de desbordamiento de memoria (Buffer Overflow) y ejecución remota de código (RCE).
- Riesgos de Seguridad Intrínsecos: El uso de software no soportado (End-of-Life, EOL) es una violación directa del control SA-22 (Unsupported System Components) de NIST SP 800-53, que prohíbe explícitamente el uso de componentes sin soporte en sistemas conectados a redes, salvo que existan medidas de aislamiento extremo (Air Gap) que aquí no se aplican. Las aplicaciones VB6 dependen de librerías COM (Component Object Model) y controles ActiveX que poseen vulnerabilidades conocidas y explotables. Un atacante con acceso a la red interna podría aprovechar estas vulnerabilidades para ejecutar código arbitrario en los servidores o estaciones de trabajo, comprometiendo la totalidad de la base de datos municipal. Las soluciones antivirus mencionadas (Windows Defender, Avast) actúan a nivel de sistema operativo y firmas de archivos, pero son ineficaces para detectar explotación de vulnerabilidades lógicas dentro del código de una aplicación legado personalizada.
- Incompatibilidad con Estándares Modernos: VB6 carece de soporte nativo para protocolos de criptografía modernos como TLS 1.2 o 1.3, necesarios para establecer comunicaciones seguras con servicios web de terceros (TGR, Previred, Registro Civil, CONASET). Cualquier integración actual se realiza mediante "parches" o componentes intermedios no estandarizados, lo que añade fragilidad y puntos de fallo a la arquitectura. Además, la ejecución de aplicaciones VB6 en sistemas operativos modernos (Windows 10/11) depende de una capa de compatibilidad que Microsoft no garantiza a perpetuidad, poniendo en riesgo la operatividad futura

ante cualquier actualización de Windows y posiblemente vulnerando la integridad de los datos.[29]

5.2. Infraestructura de Redes y Seguridad Perimetral

La auditoría de la infraestructura de comunicaciones revela debilidades críticas en la defensa en profundidad.

- Segmentación y Firewall: Si bien se indica que "Este año se hizo segmentación de redes" y se utiliza un firewall, la efectividad de estas medidas se ve comprometida por las prácticas de acceso. Los equipos, aunque robustos para entornos PYME, carecen de las capacidades avanzadas de Prevención de Intrusiones (IPS) y de inspección profunda de paquetes (DPI) necesarias para proteger datos sensibles de gobierno al nivel que ofrecerían soluciones *Enterprise*.
- Acceso Remoto No Seguro (AnyDesk): El hallazgo de que "Se conectan por anydesk no licenciado" para labores de soporte y administración es crítico. AnyDesk es una herramienta de acceso remoto de escritorio, no una solución de gestión de acceso privilegiado (PAM). Su uso en entornos corporativos, especialmente sin controles estrictos (como sí lo permitiría una VPN con autenticación multifactor), es desaconsejado por todos los marcos de ciberseguridad (NIST AC-17). AnyDesk ha sido utilizado frecuentemente como vector de entrada por grupos de Ransomware para desplegar ataques, ya que permite al atacante tomar control total de la sesión del usuario, eludiendo controles de red perimetrales. La falta de bitácoras centralizadas de quién se conecta, cuándo y qué hace durante la sesión de AnyDesk impide cualquier trazabilidad forense en caso de incidente.
- Ausencia de Directorio Activo (Active Directory): Se confirma que "Active directory, no existe". Esta es una carencia fundacional en la arquitectura de seguridad. Sin un Directorio Activo (AD), la gestión de usuarios es descentralizada y manual ("Se preparan los equipos por parte del informático").
- Gestión de Identidades: No hay forma de aplicar políticas de contraseñas robustas (complejidad, rotación) de manera centralizada.
- Ciclo de Vida de Usuarios: Cuando un funcionario deja el municipio, no existe un "botón único" para revocar todos sus accesos. Es altamente probable que existan cuentas "zombies" de exfuncionarios con acceso a los sistemas.
- Permisos: La falta de AD fomenta el uso de cuentas locales con privilegios administrativos en los PC, facilitando la instalación de malware y software no autorizado.

5.3. Integridad y Respaldo de Datos (Backup & Recovery)

La estrategia de continuidad de negocio es deficiente y expone al municipio a la pérdida total de información.

- **Respaldos:** "El respaldo no está contemplado en NAS". Almacenar los respaldos en un disco duro y no en hardware especializado como un dispositivo NAS (Network Attached Storage) conectado a la misma red local (LAN) que los servidores de producción viola el principio de separación de entornos y la regla 3-2-1 de backups (3 copias, 2 medios, 1 fuera de sitio). En un ataque de Ransomware moderno, el malware escanea la red en busca de dispositivos y cifra los respaldos antes de cifrar los servidores. Sin una copia "inmutable" o desconectada (Air-gapped) o en la nube (Off-site), la recuperación es imposible.
- **Gestión de Base de Datos:** Se indica que se usa SQL Server actualizado a 2022, pero "se modificó la estructura de la bbdd en el servidor porque se adaptó para el sistema nuevo. No se duplicó". Esto revela una práctica temeraria: realizar cambios estructurales en la base de datos de producción sin un entorno de pruebas (*Staging*) y sin mantener la integridad del esquema original. Esto explica los problemas de "cruce de datos" reportados por los usuarios, ya que el sistema antiguo (VB6) y el nuevo (Web) estarían compitiendo o escribiendo incorrectamente sobre tablas modificadas sin control de versiones.

- **Riesgo de Datos**

  Los antecedentes indican el uso y migración no controlada según mejores prácticas de desarrollo seguro.

  - ENV expuesto: Tiene vulnerabilidades críticas conocidas como mantener este motor en una red conectada y expuesta públicamente conlleva a una invitación abierta a ciberataques.
  - Falta de Encriptación: Estas versiones antiguas no soportan *Transparent Data Encryption* (TDE) ni encriptación de columnas. Los datos sensibles (RUT, direcciones, deudas) residen en texto plano en el disco. Si un atacante roba el servidor o una copia de seguridad (backup), accede a toda la información sin barreras.[32]

5.4. Desarrollo Web (Laravel/PHP): Riesgos de Implementación

El municipio ha intentado abordar la obsolescencia mediante el desarrollo de "Sistemas Web Nuevos" (Laravel/PHP). Sin embargo, la auditoría de este proyecto muestra que se están repitiendo los errores de gobernanza:

Gestión del Proyecto y Retrasos

El proyecto presenta desviaciones significativas en su cronograma: "Se mostró el sistema nuevo agosto. En noviembre se iba a entregar". A la fecha del reporte, la implementación plena no se ha concretado. En el desarrollo de software, los retrasos crónicos sin una gestión de alcance clara suelen ser síntoma de problemas profundos en la definición de requerimientos o en la capacidad técnica del equipo ejecutor. La falta de hitos de entrega cumplidos erosiona la confianza de los usuarios ("Sistema nuevo no se usa") y genera resistencia al cambio.

Calidad del Software y Seguridad (AppSec)

- Falta de Entorno de Calidad (QA): La modificación directa de la base de datos de producción sugiere que no existe un ciclo de vida de desarrollo de software (SDLC) seguro y formal. No hay evidencia de entornos separados para Desarrollo, Pruebas (QA) y Producción, lo cual es un estándar básico en ingeniería de software para prevenir caídas de servicio por errores de programación.

- Vulnerabilidades de Código: El uso del framework Laravel es positivo por ser un estándar de industria, pero requiere un mantenimiento riguroso de sus dependencias. Sin un proceso de análisis de composición de software (SCA) o escaneo de vulnerabilidades estático (SAST) —prácticas exigidas por NIST SA-11 — es probable que el nuevo sistema nazca con vulnerabilidades conocidas en sus librerías de terceros (riesgo de cadena de suministro). Además, al no haber documentación del código, el municipio queda nuevamente cautivo del desarrollador para realizar las actualizaciones de seguridad del framework (ej. pasar de Laravel 9 a 10), proceso que suele ser complejo y romper funcionalidades.

La "nueva plataforma" se desarrolla en una tecnología moderna, su seguridad depende de la implementación.

- **Riesgo OWASP:** Sin una auditoría de código (SAST), es altamente probable que el desarrollo a medida contenga vulnerabilidades del **OWASP Top 10**, como Inyección SQL (si no se usa Eloquent ORM correctamente), *Broken Access Control* (fallas en la validación de roles) o *Cross-Site Scripting* (XSS).
- **Hardening:** Existe evidencia de que el servidor web (Apache/Nginx) no tiene una configuración endurecida (*hardening*) según benchmarks CIS (deshabilitar versiones viejas de PHP, ocultar cabeceras, configurar CSP).[34]

Evidencias de Seguridad

Muestra: munialigua.cl/api/public/login



Figura 11: Sistema Admin Reloj Control, 29 de Diciembre 2025. I Municipalidad de La Ligua.

El portal de "Admin. Reloj Control" muestra un formulario de inicio de sesión para el módulo de asistencia. Aunque la interfaz no carga completamente en todos los navegadores, al revisar el código fuente se detectó un objeto Ziggy de Laravel que expone la lista completa de rutas de la aplicación. Estas rutas incluyen endpoints de depuración (_ignition/health-check, execute-solution, update-config) y numerosas API internas para gestionar funcionarios, registros y permisos. La exposición de estas rutas podría ayudar a un atacante a mapear la funcionalidad de la aplicación y buscar vulnerabilidades.

No se identificó un archivo. env accesible en este subdirectorio ni un repositorio. git; sin embargo, la exposición de rutas y endpoints de depuración sugiere que la aplicación se ejecuta en modo de desarrollo.

Recomendaciones:

- Desactivar o eliminar Ziggy en producción o limitar la información que expone a las rutas necesarias para el frontend.
- Deshabilitar los endpoints de *Ignition* y asegurarse de que APP_DEBUG esté configurado en false en producción.
- Revisar que los endpoints api/* requieran autenticación y que las entradas se validen correctamente.

Muestra: munlaligua.cl/dom/tramitegeneral

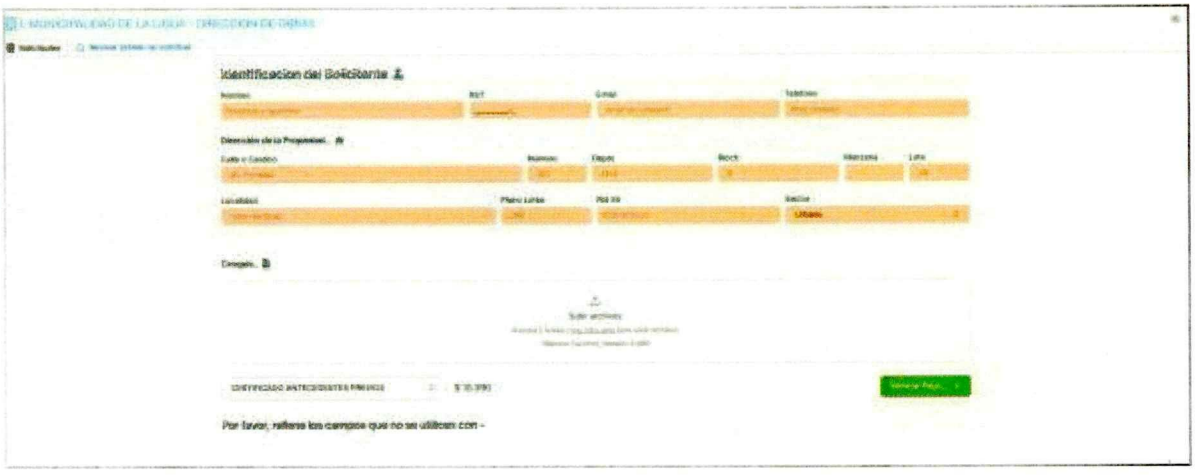


Figura 12: Sistema DOM, 29 de Diciembre 2025. I **Municipalidad de La Ligua.**

Esta página de la **Dirección de Obras Municipales (DOM)** ofrece un formulario para solicitar certificados y subir archivos. Al inspeccionar el código fuente se confirmó la presencia de Ziggy con decenas de rutas internas, incluidas funciones de estado de solicitudes y de la API DOM. Al igual que en el módulo de asistencia, esto revela detalles de la arquitectura de la aplicación.

Exposición del archivo .env: El archivo de configuración del entorno /.env dentro de este módulo es público y contiene información sensible: nombre y clave de la aplicación, claves secretas (APP_KEY), credenciales para un servicio de folios (PASS_WEBSERVICE), parámetros de base de datos SQL Server e indicadores de que la aplicación se ejecuta con APP_DEBUG=true. Esta información permite comprometer completamente el sistema.

```
NOMBRE DE LA APLICACIÓN=DOM
APP_ENV=local
CLAVE DE APLICACIÓN=base64:9S4jZ6ilVThRLNzqNqBqz5PDGvrzxMVBrf1cGcDjHyw=
APP_DEBUG=verdadero
APP_TIMEZONE=América/Santiago
URL_DE_LA_APLICACIÓN=http://localhost

PASS_WEBSERVICE=DOMMunLaligua596
PASE_RECIBIR_FOLIO=DOMMunLaligua596

MUNI_NAME="Ilustre Municipalidad de La Ligua"
MUNI_RUT="69.050.100-7"

APP_LOCALE=es
APP_FALLBACK_LOCALE=es
APP_FAKER_LOCALE=es_ES

APP_MAINTENANCE_DRIVER=archivo
APP_MAINTENANCE_STORE=base de datos

BCRYPT_RONDAS=12

LOG_CHANNEL=pila
LOG_STACK=único
LOG_DEPRECATIONS_CHANNEL=nulo
LOG_LEVEL=depuración

CONEXIÓN_BD=sqlsrv
HOST_DE_BASE=WIN-JGU9MQ5MQLC
PUERTO_DB=1433
BASE DE DATOS DB=dom
DB_NOMBRE_USUARIO=
CONTRASEÑA DE LA BASE DE DATOS=

#CONEXIÓN_BD=sqlite
#DB_HOST=127.0.0.1
# PUERTO_DB=3306
# BASE DE DATOS DB=laravel
# DB_USERNAME=raíz
# CONTRASEÑA_DB=
```

Figura 13: Exposición .env Sistema DOM, 29 de Diciembre 2025. I Municipalidad de La Ligua.

Exposición de Git: El repositorio Git también está accesible. El fichero .git/HEAD muestra que la rama principal es main, y los registros de commits (.git/logs/refs/heads/main) enumeran todos los cambios con fechas, hashes y datos del autor. A partir de estos archivos un atacante puede reconstruir el código fuente completo.

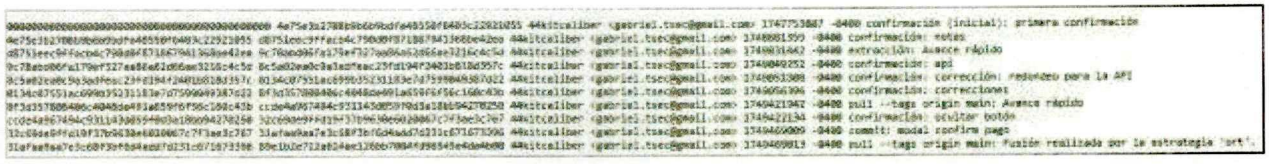


Figura 14: Exposición commits Sistema DOM, 29 de Diciembre 2025. I Municipalidad de La Ligua.

Recomendaciones:

- Mover el archivo .env y todo el directorio .git fuera del directorio público o configurar el servidor para que devuelva un 404/403 ante solicitudes que comiencen por /.env o /.git.
- Rotar inmediatamente todas las claves y contraseñas expuestas en el .env (APP_KEY, credenciales de servicios y base de datos).
- Desactivar el modo debug (APP_DEBUG=false) y agregar cabeceras de seguridad (ServerTokens Prod, ServerSignature Off).
- Revisar la validación del formulario y las restricciones de subida de archivos (actualmente se permiten archivos de hasta 5 MB sin validación, lo que puede introducir malware).

Muestra: munlaligua.cl/domadm/public/login

Aunque el acceso al login devuelve un error 502, el archivo /.env de este módulo es accesible y expone correos y credenciales SMTP (tramitelaligua@gmail.com con su contraseña de aplicación), claves de API (ABLY_KEY_PUB, ABLY_KEY_SUB) y parámetros de base de datos, además de ejecutarse en modo local con APP_DEBUG=true.

```
CORREO_POSTAL=smtp
MAIL_HOST=smtp.gmail.com
PUERTO DE CORREO=465
MAIL_USERNAME=tramitelaligua@gmail.com
CONTRASEÑA DE CORREO="hyfh ocat sxvc nxyf"
CIFRADO DE CORREO=tls
MAIL_FROM_ADDRESS="tramitelaligua@gmail.com"

# CORREO_CORREO=smtp
# MAIL_HOST=sandbox.smtp.mailtrap.io
# PUERTO_DE_CORREO=2525
# NOMBRE_USUARIO_DE_CORREO=879d1c64310216
# CONTRASEÑA DE CORREO ELECTRÓNICO=203e19aac85c47
# MAIL_SCHEME=nulo
# DIRECCIÓN_DE_CORREO="hola@ejemplo.com"
MAIL_FROM_NAME="Dirección de Obras - La Ligua"

MUNI_RUT="69.050.100-7"
MUNI_NOMBRE="Ilustre Municipalidad de La Ligua"

PASS_WEBSERVICE="DOMMunLaligua596"

NOMBRE DE LA APLICACIÓN=DOMADM
APP_ENV=local
CLAVE DE APLICACIÓN=base64:ITCT+Ubo1dRvy4K1xKy0vdFA6NRQYjDmZzmOBXvdDxg=
APP_DEBUG=verdadero
APP_TIMEZONE=América/Santiago
URL_DE_LA_APLICACIÓN=http://localhost
```

Figura 15: Exposición .env Sistema DOM, 29 de Diciembre 2025. I Municipalidad de La Ligua.

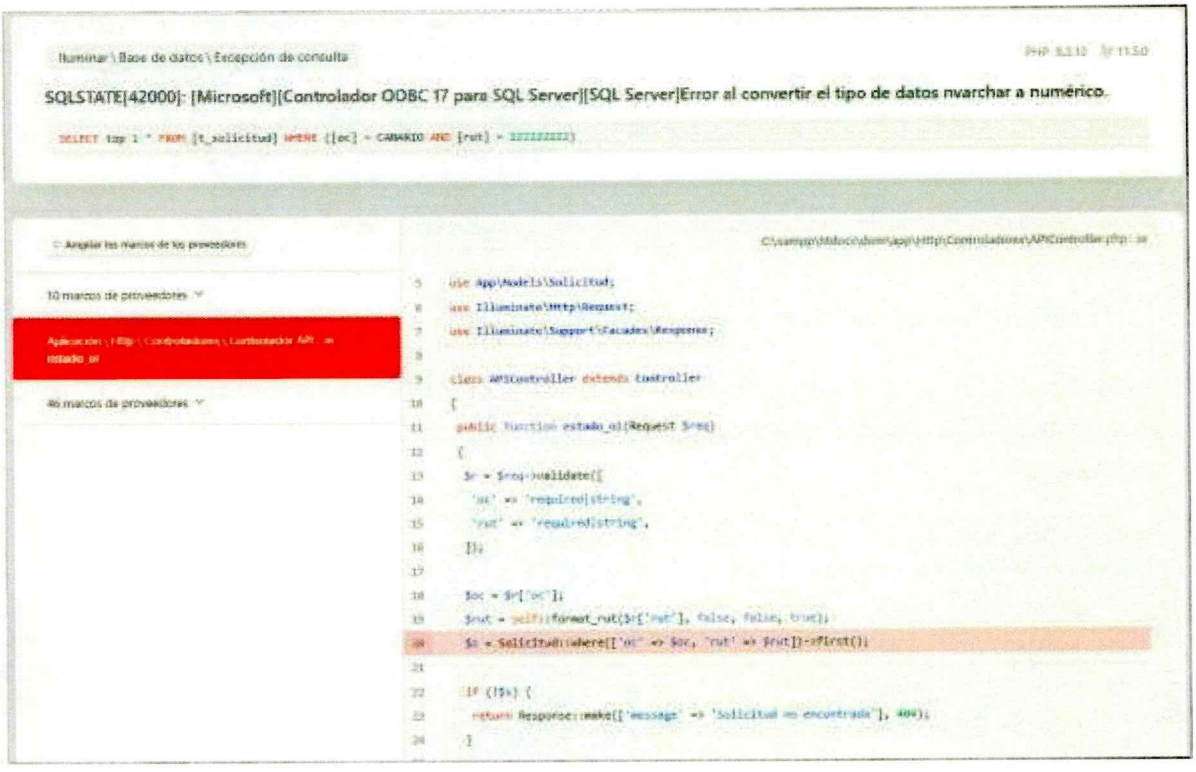


Figura 15: Exposición SQL Sistema DOM, 29 de Diciembre 2025. I Municipalidad de La Ligua.

No se pudo verificar el acceso al repositorio .git, ya que devuelve un error 502, pero es probable que esté disponible al igual que en el módulo anterior.

Recomendaciones:

- Proteger el archivo .env y el directorio .git mediante reglas del servidor (RedirectMatch 404 \.env, \/.git), y reubicar dichos archivos fuera del árbol público.
- Rotar las credenciales de correo y de API divulgadas, activar autenticación multifactor en la cuenta de Gmail y configurar variables seguras.
- Asegurar que el módulo se ejecute en modo de producción (APP_DEBUG=false).

Muestra: munlaligua.cl/licencias/login

La página de licencias de conducir muestra un formulario de inicio de sesión. El código fuente incluye un objeto Ziggy con más de un centenar de rutas internas para gestión de licencias, usuarios, listados de trámites, mantenimiento de tipos de licencias y varios endpoints API (api/buscar_solicitudes, api/desplegar_solicitud, etc.). La cantidad de rutas expuestas brinda información valiosa sobre la estructura del sistema.

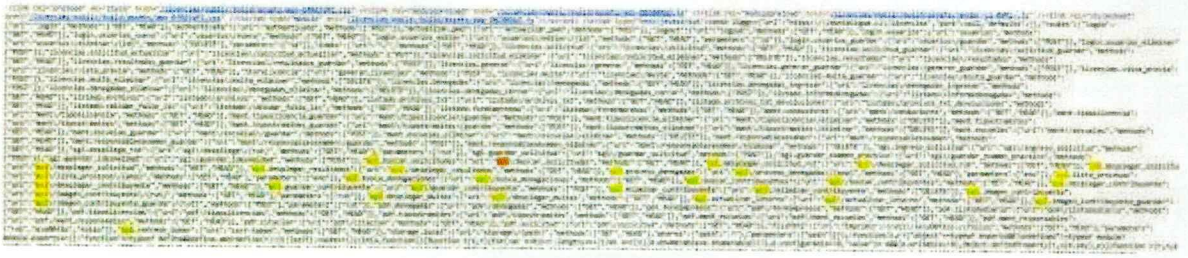


Figura 16: Exposición rutas API Sistema Licencias, 29 de Diciembre 2025. I Municipalidad de La Ligua.

No se observó acceso al archivo .env ni al repositorio .git (las solicitudes devolvieron 502), pero conviene comprobar la configuración del servidor para garantizar que no estén accesibles.

Recomendaciones:

- Restringir la enumeración de rutas de Ziggy en producción para evitar que los atacantes conozcan la API completa.
- Revisar la autenticación y autorización de todos los endpoints api/* y asegurar que no devuelvan información sin las credenciales adecuadas.
- Verificar manualmente que los archivos .env y .git no sean accesibles y que APP_DEBUG esté desactivado.

Muestra: softed.cl/bodega/public/login

El portal de **Bodega** muestra un formulario simple para ingresar usuario y contraseña. El código fuente utiliza Ziggy y expone numerosas rutas internas para administrar productos, empresas, facturas y funciones de mantenimiento. Esto puede facilitar la enumeración de funciones sensibles.

Se intentó acceder a /.env y al repositorio .git y se obtuvo un error 404 o 502, por lo que aparentemente no están expuestos.



Figura 17: Exposición ziggy Sistema Bodegas, 29 de Diciembre 2025. I Municipalidad de La Ligua.

Recomendaciones:

- Limitar la información del objeto Ziggy en producción; solo deben publicarse las rutas necesarias para la interfaz.
- Implementar controles de acceso y autenticación robusta para los endpoints de gestión de inventario y facturas.
- Realizar pruebas de fuga de información para confirmar que no existan archivos ocultos u otras configuraciones inseguras.

Muestra: softed.cl/activofijo/public/login

La página de Activo Fijo no permitió cargar su código fuente (502), pero el archivo /.env del módulo es públicamente accesible y contiene el nombre de la aplicación, clave secreta (APP_KEY), parámetros de base de datos activofijo, servidor SQL y configuración SMTP, todo con APP_DEBUG=true. Esto representa un riesgo de alto impacto.

```
NOMBRE_DE_LA_APP=activofijo
APP_ENV=local
CLAVE DE APLICACIÓN=base64:V7V9GI6k1qTz8l0GLRvh+jaEop6Kb3PtTI0KwBTR9jM=
APP_DEBUG=verdadero
URL_DE_LA_APLICACIÓN=http://localhost
APP_TIMEZONE=América/Santiago

LOG_CHANNEL=pila
LOG_DEPRECATIONS_CHANNEL=nulo
LOG_LEVEL=depuración

CONEXIÓN_BD=sqlsrv
DB_HOST=WIN-DD6KJ83LSCR
PUERTO_DB=1433
DB_DATABASE=activofijo
DB_NOMBRE_USUARIO=
CONTRASEÑA DE LA BASE DE DATOS=
```

Figura 18: Exposición .env Sistema Activo Fijo, 29 de Diciembre 2025. I Municipalidad de La Ligua.

```
HOST DE MEMCACHED=127.0.0.1

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=nulo
PUERTO REDIS=6379

CORREO_POSTAL=smtp
MAIL_HOST=mailpit
PUERTO DE CORREO=1025
MAIL_USERNAME=nulo
MAIL_PASSWORD=nulo
MAIL_ENCRYPTION=nulo
MAIL_FROM_ADDRESS="hola@ejemplo.com"
CORREO_DESDE_NOMBRE="${NOMBRE_DE_LA_APLICACIÓN}"
```

Figura 19: Exposición SMTP Sistema Activo Fijo, 29 de Diciembre 2025. I Municipalidad de La Ligua.

Recomendaciones:

- Proteger el archivo .env y eliminarlo del directorio público; trasladarlo fuera de public y denegar su acceso mediante reglas del servidor.
- Configurar el entorno de producción (APP_DEBUG=false) y ocultar la URL base (APP_URL apunta a localhost), sustituyéndola por el dominio correcto.
- Revisar la configuración de la base de datos y del correo: las contraseñas deben cambiarse y almacenarse de forma segura.

Muestra: softed.cl/jpl/public/login

El módulo JPL presenta un formulario de login desarrollado con Bootstrap. No se encontró un objeto Ziggy, pero el código fuente muestra un formulario con token CSRF y llamadas a genealabs/laravel-caffeine/drip para mantener la sesión activa.

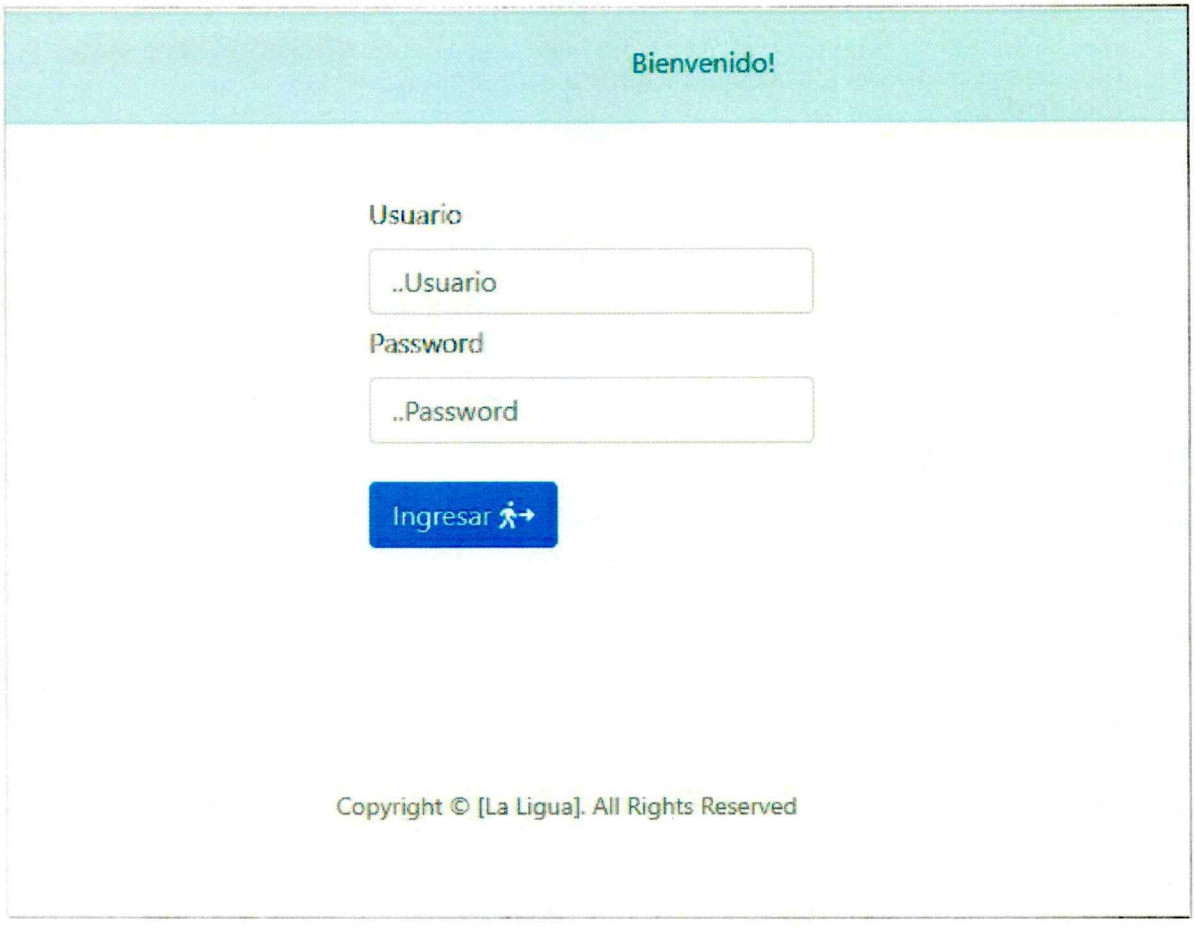


Figura 20: Inicio sesión Sistema JPL, 29 de Diciembre 2025. I Municipalidad de La Ligua.

```
ajax.open('GET', 'https://softed.cl/jpl/public/genealabs/laravel-caffeine/drip');
ajax.setRequestHeader('X-Requested-With', 'XMLHttpRequest');
ajax.send();


tInterval(function () {
  caffeineSendDrip();
300000);

(2000 > 0) {
 setInterval(
     function () {
         if (new Date() - lastCheck >= 31355882000) {
             location.reload(true);
             setTimeout(
                 function () {
                     location.reload(true);
                 },
                 Math.max(0, 2000 - 500),
             );
         }
     },
     2000,
 );
```

Figura 21: Llamada sesión activa Sistema JPL, 29 de Diciembre 2025. I Municipalidad de La Ligua.

```
<!---traspaso de variables formularios -->
<div class="conteiner">
 <div class="col md-6">
  <form action="https://softed.cl/jpl/public/authenticate" method="POST" class="row g-1">
   <input type="hidden" name="_token" value="4LydFRNjvzH62CtXpxuwP8Z7oaIUSRmI7TlqR7Ea">       <div class="col-md-8">
    <label for="Usuario" class="form-label">Usuario
           </label>
    <input type="text" class="form-control" value="" name="usuario" id="usuario" placeholder="..Usuario">

   </div>
   <div class="col-8" style="height: 4rem;">
    <label for="password" class="form-label">Password
           </label>
    <input type="password" class="form-control" value="" name="password" id="password" placeholder="..Password"
     aria-describedby="passwordHelpBlock">
```

Figura 22: Token CSRF Sistema JPL, 29 de Diciembre 2025. I Municipalidad de La Ligua.

El archivo /.env del módulo está expuesto y revela la clave de la aplicación (APP_KEY), configuración de base de datos gijpl, tiempos de sesión y parámetros de correo, todo con APP_DEBUG=true[softed.cl](). La base de datos se ejecuta en un servidor WIN-DD6KJ83LSCR sin usuario ni contraseña definidos, lo que podría indicar uso de autenticación integrada de Windows.

```
NOMBRE DE LA APLICACIÓN=JPLLL
TIEMPO DE VIDA DE LA SESIÓN=522600
APP_ENV=local
CLAVE DE APLICACIÓN=base64:DxwQPTDFsipFANBxgGwBiOXwUg0lDkgmk9sheVmDeMc=
APP_DEBUG=verdadero
URL_DE_LA_APLICACIÓN=http://localhost

LOG_CHANNEL=pila
LOG_DEPRECATIONS_CHANNEL=nulo
LOG_LEVEL=depuración

CONEXIÓN_BD=sqlsrv
DB_HOST=WIN-DD6KJ83LSCR
PUERTO_DB=1433
BASE DE DATOS DB=gijpl
DB_NOMBRE_USUARIO=
CONTRASEÑA DE LA BASE DE DATOS=

CONTROLADOR DE TRANSMISIÓN=registro
CACHE_DRIVER=archivo
DISCO DEL SISTEMA DE ARCHIVOS=local
CONEXIÓN_DE_COLA=sincronización
SESSION_DRIVER=archivo

HOST DE MEMCACHED=127.0.0.1

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=nulo
PUERTO REDIS=6379

CORREO_POSTAL=smtp
MAIL_HOST=mailpit
PUERTO DE CORREO=1025
MAIL_USERNAME=nulo
MAIL_PASSWORD=nulo
MAIL_ENCRYPTION=nulo
MAIL_FROM_ADDRESS="hola@ejemplo.com"
CORREO_DESDE_NOMBRE="${NOMBRE_DE_LA_APLICACIÓN}"
```

Figura 23: Exposición .env Sistema JPL, 29 de Diciembre 2025. I Municipalidad de La Ligua.

Recomendaciones:

- Bloquear el acceso a /.env en el servidor y mover el archivo fuera del directorio público. Rotar la APP_KEY y las credenciales de la base de datos.
- Revisar las rutas definidas en routes/web.php y asegurar que todas requieran autenticación adecuada.

- Deshabilitar el modo de depuración en producción para evitar fugas de información en mensajes de error.

Conclusiones generales

- **Archivos .env expuestos:** Los módulos *DOM*, *DOMADM*, *Activo Fijo* y *JPL* publican sus archivos .env, revelando claves secretas, credenciales de correo, parámetros de base de datos y datos de configuración. Esto es una vulnerabilidad crítica que permite la toma de control de los sistemas.
- **Repositorios Git accesibles:** En dom/tramitegeneral se puede navegar por .git/HEAD y logs, obteniendo el historial de commits y la identidad de los desarrolladores. Es probable que otros módulos también tengan el repositorio expuesto.
- **Modo de depuración activo:** Varias aplicaciones están configuradas con APP_ENV=local y APP_DEBUG=true, lo que se refleja en la exposición de endpoints de Ignition y una mayor verbosidad de errores. Esto debe desactivarse en producción.
- **Enumeración de rutas mediante Ziggy:** Los proyectos basados en Laravel utilizan Ziggy para pasar rutas al frontend. En los entornos analizados, Ziggy expone todas las rutas del backend, incluidos endpoints de depuración y APIs internas. En producción, Ziggy debería limitarse a las rutas necesarias para la aplicación cliente.
- **Falta buenas prácticas de desarrollo:** Lo anterior expone que el desarrollo que se enuncia como concluido no cuenta con buenas prácticas de desarrollo de software como estándar, exponiendo a vulnerabilidades de la institución por parte de ciberdelincuentes.

6. Evaluación Funcional y Satisfacción Usuaria

La tecnología debe servir a las personas. Utilizando el **Modelo de Éxito de Sistemas de Información de DeLone & McLean**, se evaluó la percepción de los funcionarios, revelando una desconexión crítica entre la TI y la operación municipal.

6.1. Dimensiones de Evaluación (Resultados de Entrevistas)

- Departamento de Rentas y Patentes (Nivel de Satisfacción: 0/Inexistente)
    - Esta es el área más crítica debido a su impacto en los ingresos municipales. Los hallazgos son devastadores para la integridad financiera del municipio:

- Integridad de Datos: "La información no corresponde a lo deseado. Salen otros datos... se pisan los atributos". Esto indica problemas graves de concurrencia o diseño de base de datos.
- Error de Cálculo Financiero: "El sistema no toma el capital negativo. Los toma como positivos". Este error algorítmico es gravísimo. Si un IPC negativo o un factor de corrección no se aplica correctamente, el municipio está cobrando montos erróneos a los contribuyentes. Esto expone al alcalde y al concejo a acusaciones de notable abandono de deberes y a juicios de cuentas por parte de la Contraloría General de la República (CGR).
- Duplicidad: "Se duplican interés en patentes comerciales". Cobrar intereses duplicados es ilegal y genera un pasivo contingente por devoluciones masivas.
- Ineficiencia Operativa: "Enrolar una patente es difícil... Los convenios no se pueden liquidar". Esto obliga a procesos manuales lentos, reduciendo la recaudación efectiva.

- 6.2 Recursos Humanos y Remuneraciones (Nivel de Satisfacción: 3/Bajo)

  - Riesgo de Integridad y Fraude: "Todo el proceso se hace manual, los descuentos, las planillas, etc... Contabilidad, la remuneración se hace en excel". El cálculo de remuneraciones en planillas Excel para una planta municipal es una práctica de alto riesgo inaceptable bajo estándares modernos de control interno. Excel no ofrece pistas de auditoría (*Audit Trail*): no se puede saber quién modificó una fórmula o un monto, ni cuándo. Esto facilita tanto el error humano involuntario como la manipulación maliciosa de datos para generar pagos indebidos.
  - Pérdida de Historia: "No tiene asientos contables de 2018 por sistema". Existe un agujero negro de información histórica que impide análisis de tendencias o auditorías retrospectivas.
  - Validación Externa: "Se valida con PreviRed para ver si los valores realizados por Excel son los adecuados ya que no confío en el sistema". El sistema debería ser la fuente de verdad, no PreviRed. Que el sistema dependa de una validación externa para saber si está correcto demuestra su falta de confiabilidad lógica.

- 6.3 Adquisiciones y Abastecimiento (Nivel de Satisfacción: 4/Bajo)
    - Falta de Interoperabilidad: "Se hace todo manual, no se conecta a mercadopúblico". La gestión de compras públicas exige integración con la plataforma de la Dirección de Compras y Contratación Pública (DCCP). Realizar la gestión desconectada duplica el trabajo administrativo y aumenta el riesgo de inconsistencias entre la Orden de Compra (OC) en el portal y la contabilidad interna.
    - Ineficiencia: "Para visar las Órdenes de Compra se hace una a una". La falta de procesos de aprobación por lotes o flujos de trabajo automatizados genera cuellos de botella burocráticos.

- 6.4 Salud y Atención al Público
    - Soporte Deficiente: "El soporte se hace en días y horarios en que el proveedor tiene disponibilidad para dar una solución". En un área sensible como Salud, donde la atención de pacientes puede depender del sistema, tiempos de respuesta de días son inaceptables.
    - Insatisfacción con Mesa de Ayuda: Se reporta consistentemente que el soporte técnico "No es el más adecuado y con enfoque al usuario". Según ITIL 4, el *Service Desk* es la cara de TI ante la organización. Un trato deficiente desincentiva el reporte de incidentes, llevando a los usuarios a ocultar problemas o crear soluciones alternativas fuera del control de TI (*Shadow IT*), lo que incrementa el riesgo global.

6.2. Análisis de Usabilidad

La interfaz de los sistemas legados (VB6) requiere una curva de aprendizaje alta y no es intuitiva. La falta de manuales actualizados y capacitación formal ("no hubo jornada de capacitación") agrava el problema. El sistema no guía al usuario, sino que permite errores (ej. ingresar RUTs inválidos), lo que contamina la base de datos.[37]

7. Análisis de Brechas Normativas (Gap Analysis)

7.1 Ley N° 21.180 de Transformación Digital del Estado

- **Estado: Incumplimiento Alto.**

- **Análisis:** La ley mandata que para 2027 todos los procedimientos administrativos deben ser electrónicos. La realidad de I Municipalidad de La Ligua, con procesos manuales en RRHH, Adquisiciones y Rentas, y sistemas desconectados (silos), está lejos de cumplir este objetivo.
- **Brecha Específica:** No hay evidencia de integración operativa con las plataformas habilitantes del Estado:
    - **DocDigital** (comunicaciones oficiales), **ClaveÚnica** (identidad digital) y **FirmaGob** (firma electrónica avanzada). Actualmente existe una barrera contractural administrativa para continuar con un proveedor externo de firmas electrónicas avanzadas, adicionalmente el argumento de que FirmaGob "cae mucho" no considera datos reales para una evaluación objetiva; como entidad pública, el municipio debe alinearse con los estándares de la SEGPRES y Gobierno Digital, no crear islas tecnológicas. Este producto ofrecido para los servicios públicos mediante la formalización de convenios está integrado a todas las herramientas actuales del Estado como Sistema de Gestión de Licencias de Conducir, Sistema de Gestión Social, Doc Digital, entre otros.

7.2 Ley N° 21.663 Marco de Ciberseguridad

- **Estado: Incumplimiento Crítico.**
- **Análisis:** La ley obliga a los organismos del Estado a aplicar medidas técnicas para gestionar riesgos y reportar incidentes a la ANCI (CSIRT Nacional).
- **Brecha Específica:**
    - **Identificación de Activos:** No hay un inventario claro de activos de información (hardware y software) actualizado, requisito base de CIS Controls v8.1 (Control 1 y 2).
    - **Detección y Respuesta:** La falta de logs centralizados y la dependencia de antivirus básicos (Windows Defender/Avast) sin una consola de administración central (EDR/XDR) deja al municipio ciego ante ataques. No podrían detectar ni reportar un incidente dentro del plazo legal (3 horas para incidentes de impacto significativo).
    - **Gobernanza:** La falta de un responsable de seguridad identificado impide la coordinación con la autoridad nacional o al menos un mediador institucional.

7.3 Protección de Datos Personales (Ley 19.628 / Proyecto Ley)

- **Estado: Riesgo Alto.**
- **Análisis:** Las áreas de Salud y "Ayudas Sociales" tratan Datos Sensibles (diagnósticos, situación socioeconómica).
- **Brecha Específica:**
  - **Principio de Seguridad:** La Ley exige medidas de seguridad acordes al riesgo. Almacenar datos sensibles en sistemas inestables, accesibles vía AnyDesk inseguro y sin cifrado de base de datos, constituye una negligencia en el deber de custodia.
  - **Trazabilidad:** Al compartir cuentas de administrador o no tener logs de acceso claros, es imposible saber qué funcionario accedió a la ficha médica o social de un vecino, violando el principio de confidencialidad. Se evidencia del registro en base de datos por parte del nuevo desarrollo, pero al no estar implementado sigue existiendo la brecha.

8. Matriz de Hallazgos y Clasificación de Riesgos (Consolidada)

A continuación, se presenta la Matriz de Riesgos consolidada, elaborada bajo la metodología NIST SP 800-30, utilizando una escala cualitativa/cuantitativa de 5x5.

8.1. Marco Metodológico de la Matriz

- **Nivel de Riesgo (R) = Probabilidad (P) x Impacto (I)**
- **Probabilidad (1-5):**
  - 5: Frecuente (Ocurre mensualmente o la vulnerabilidad es explotable trivialmente).
  - 4: Probable.
  - 1: Raro.
- **Impacto (1-5):**
  - 5: Catastrófico (Paralización total, multas legales masivas, daño reputacional nacional).
  - 4: Mayor (Pérdida financiera significativa, interrupción de servicios críticos).
  - 1: Insignificante.
- **Clasificación:**
  - **Crítico (20-25):** Acción inmediata ineludible.
  - **Alto (12-19):** Atención urgente requerida.
  - **Medio (6-11):** Gestionar y monitorear.

8.2. Matriz Detallada

ID	Hallazgo	Descripción Detallada	Impacto	Probabilidad	Nivel de Riesgo	Estándar Afectado
H-01	Dependencia Unipersonal (Bus Factor)	La operación tecnológica total depende de un solo proveedor externo sin respaldo ni documentación.	Catastrófico	Alta	CRÍTICO	COBIT APO07
H-02	Obsolescencia VB6	Uso de plataforma EOL (2001) vulnerable a exploits y sin capacidad de cifrado moderno.	Alto	Muy Alta	CRÍTICO	NIST SA-22
H-03	Indefinición de Propiedad Intelectual	El municipio no posee legalmente el código fuente ni derechos claros sobre el software que financia.	Alto	Alta	CRÍTICO	NIST SA-4
H-04	Cálculo Manual de Remuneraciones	Proceso crítico de pago de sueldos realizado en Excel sin controles de integridad ni auditoría.	Alto	Media	CRÍTICO	CGR / Probidad
H-05	Errores Financieros en Rentas	Sistema calcula erróneamente capitales negativos y duplica intereses, generando daño patrimonial.	Alto	Alta	CRÍTICO	Integridad Financiera Escalable
H-06	Ausencia de Active Directory	Gestión de usuarios manual y descentralizada. Cuentas locales con privilegios administrador.	Alto	Alta	CRÍTICO	NIST AC-2, AC-6
H-07	Respaldos Inseguros	Backups almacenados en dispositivos de discos duros.	Catastrófico	Media	ALTO	NIST CP-9
H-08	Acceso Remoto	Uso de herramientas de escritorio remoto no gestionadas ni licenciadas para administración de sistemas.	Alto	Alta	ALTO	NIST AC-17
H-09	Incumplimiento Ley Transformación Digital	Procesos manuales predominantes y falta de integración con plataformas del Estado.	Medio	Muy Alta	ALTO	Ley 21.180
H-10	Falta de QA en Desarrollo Web	Modificación directa de base de datos en producción y falta de entorno de pruebas.	Medio	Alta	MEDIO	NIST SA-11
H-11	Insatisfacción Usuaria	Mesa de ayuda informal con reportes de baja resolución de problemas.	Medio	Alta	MEDIO	ITIL (Service Desk)

9. Propuesta de Líneas de Trabajo Críticas

Ante la criticidad del diagnóstico, se propone un plan de estabilización y modernización estructurado en 5 líneas de trabajo, fundamentadas en PMBOK y **COBIT 2019**.

Línea 1: Aseguramiento de la Continuidad y Propiedad (Inmediato - Mes 1)

- Acción:
  - Exigir formalmente la entrega de la última versión del código fuente compilable y las credenciales administrativas ("sa") y técnicas de todas las bases de datos, asimismo su documentación formal.
  - Proyectar mantención temporal finita del sistema existente con el fin de dar continuidad operativa al municipio. Considerar el plazo de licitación y puesta en marcha de los sistemas adjudicados.
  - Evaluar implementación paralela de sistemas y portales provistos por SUBDERE en materia de Pagos en Línea (patentes comerciales, permisos de circulación, multas, etc) a través de su plataforma SEM.
- Fundamento: Recuperar la soberanía sobre los activos de información municipales. Sin esto, cualquier otro plan es inviable.
- Referencia: Cláusulas de Propiedad Intelectual de las Bases Tipo de ChileCompra y Ley 17.336 de Propiedad Intelectual.

Línea 2: Mitigación de Ciberseguridad de Emergencia (Corto Plazo - Mes 1-3)

- Acción:
  - Eliminar accesos remotos no controlados (AnyDesk, RDP). Implementar VPN con autenticación de doble factor (MFA) en los casos que sea necesario.
  - Licitar servicio de asistencia remota (ej: AnyDesk, Teamviewer o similares) para cumplir con la normativa legal vigente sobre el uso irregular de estas aplicaciones evitando la exposición a multas o demandas legales.
  - Aislar (segmentar) los servidores legados en una VLAN apropiada, sin exposición a total a internet, accesible solo desde dispositivos específicos.
  - Implementar una estrategia de respaldos se sugiere la básica "3-2-1" (3 copias, 2 medios, 1 fuera de sitio/nube inmutable) para protegerse contra ataques como Ransomware. Para luego transitar a otras más robustas.
- Fundamento: CIS Controls v8 (Controles 12, 11 y 3).[16]

Línea 3: Blindaje de Infraestructura e Identidad (Corto Plazo - Mes 1 a 3)

- Objetivo: Reducir la superficie de ataque y controlar accesos.
- Acciones:

- Implementación de Directorio Activo: Desplegar un controlador de dominio (Windows Server AD o solución LDAP basada en Linux como FreeIPA) para centralizar usuarios y aplicar políticas de bloqueo de cuentas y complejidad de contraseñas.
- Configurar VLAN existente: Desplegar una solución que configure adecuadamente las VLAN existentes, evitando el uso de doble computador.
- Seguridad Perimetral y VPN: Configurar una VPN corporativa (utilizando el hardware existente) con autenticación de doble factor (2FA) para todo acceso de soporte externo. Bloquear el puerto y uso de Escritorios Remotos a nivel de firewall.
- Respaldo Inmutable: Contratar un servicio de almacenamiento en nube (ej. Azure, AWS, Google Cloud, Google Workspace) y configurar la replicación automática de los respaldos críticos fuera de la red municipal.
- Licitar o contratar servicio de diagnóstico de infraestructura y redes del municipio: Según lo constatado en terreno fue identificado que las categorías de cableado generan detrimento a la calidad del internet contratado afectando el normal funcionamiento del municipio.

Línea 4: Licitar Alternativas de Mercado (Corto Plazo - Mes 2-4)

- Acción: Realizar proceso licitatorio para contratar soluciones ERP Municipales existentes (ej. CAS Chile, SMC, etc.).
- Fundamento: Según análisis expuesto por este informe. Es altamente probable que el costo de suscripción a un servicio maduro sea igual o menor que el costo de mantener, arreglar y operar sistemas propios obsoletos.

Línea 5: Auditoría y Saneamiento Financiero (Corto Plazo - Mes 2 a 4)

- Objetivo: Detectar y corregir ítems financieros en Rentas, Tesorería, Conciliaciones Bancarias, Tránsito, Contabilidad, RRHH, entre otras.
- Acciones:
  - Auditoría Externa Contable: Contratar una auditoría forense específica para revisar los cálculos de patentes y remuneraciones de los últimos 2 años, cuantificando el impacto de los errores de "capital negativo" y "duplicidad de intereses".
  - Controles Compensatorios: Establecer un procedimiento manual obligatorio de doble verificación para la nómina de sueldos y la emisión de patentes de

altos montos, hasta que se implemente el nuevo sistema. Prohibir el uso de Excel como "sistema maestro".

Línea 6: Plan de Migración y Modernización (Mediano Plazo - Mes 4-12)

- Acción: Diseñar y licitar la implementación de un nuevo sistema de gestión integral (ERP) que reemplace los sistemas legados. La licitación debe exigir:
  - Cumplimiento de Ley 21.180.
  - Cumplimiento Ley 21.719 (Privacidad).
  - Certificación ISO 27001 del proveedor.
  - Mesa de ayuda en horario municipal.
  - Actualizaciones legales sin costos adicionales.
  - Migración de datos históricos garantizada.
- **Fundamento:** Ley 21.634 y Ley 21.180.[1]

Línea 7: Gestión del Cambio y Capacitación (Transversal)

- Acción: Implementar un programa de alfabetización digital y capacitación funcional para los funcionarios, acompañado de una mesa de ayuda (Service Desk) formalizada con SLAs claros.
- Fundamento: ITIL 4 (Service Value System). La tecnología no funciona si las personas no saben usarla o la rechazan.[20]

Línea 8: Reestructuración del Gobierno TI (Mediano Plazo - Mes 3 a 6)

- Objetivo: Profesionalizar la gestión y cumplir la Transformación Digital y Segura del Estado.
- Acciones:
  - Definición de Roles: Designar formalmente (por decreto) un Encargado de Seguridad de la Información y un Encargado de Transformación Digital, con asignación de responsabilidad y capacitación específica.
  - Comité de TI: Crear un Comité de Tecnología presidido por el Administrador Municipal para alinear las decisiones tecnológicas con la estrategia comunal y supervisar el plan de modernización.
  - Comité Incidentes Ciberseguridad / Protección de datos: Crear un Comité de Tecnología presidido por el Administrador Municipal para alinear las decisiones sobre ciberseguridad e incidentes de información.

- Licitar o contratar un servicio que diagnostique el estado del municipio en la materia y genere un plan de trabajo ajustado a la realidad institucional para dar un adecuado complimiento y tránsito en la materia.

10. Evaluación Estratégica: ¿Desarrollo Propio o Software de Mercado?

Esta es la decisión estratégica más importante para l Municipalidad de La Ligua.

10.1. Análisis de Costo Total de Propiedad (TCO) y Riesgo

Opción A: Desarrollo Propio (Status Quo / Modelo actual)

- Ventajas:
  - Software a la medida: si son identificados correctamente los requerimientos, el software se ajusta a la realidad institucional y a sus funcionarios.
  - Propiedad: si es realizado un adecuado contrato el software desarrollado forma parte íntegra del activo municipal.
- Desventajas:
  - Altos costos: Los costos para el desarrollo propio y mantención de software son superiores a los de arriendo.
  - Costos Ocultos: Infraestructura (servidores, electricidad), licencias de S.O. y SQL (si se regularizan), horas hombre de personal interno para soporte nivel 1, costo de fallas, costo de riesgo legal adquirido (multas Ciberseguridad/Datos).
  - Planificación: existe un alto nivel de riesgo al no cumplimiento de los plazos estipulados y la calidad de sus entregables si no cuentan con una contraparte técnica resolutiva.
  - Evaluación: Este proyecto requiere mantener un equipo de desarrollo de alto nivel ("Software Factory") donde el municipio debe iniciar un proceso de revisión del código, revisión del software, documentación, pruebas funcionales, trabajo paralelo, transición de software y capacitaciones. La dependencia de un proveedor con niveles de servicios limitados, adicionalmente, la imposibilidad técnica de contar con una contraparte efectiva del desarrollo y los demás antecedentes expuestos se vuelve una opción riesgosa que afectará continuamente al municipio y a sus vecinos y vecinas.

Opción B: Software de Mercado

Modelo: Suscripción mensual/anual por servicio. El proveedor se encarga de la infraestructura (a convenir), seguridad, actualizaciones legales y mantenimiento evolutivo.

- *Ventajas:*

- Economía de Escala: El proveedor prorratea los costos de desarrollo de nuevas leyes (ej. cambios en IPC, nuevas exenciones) entre 50-100 o n clientes municipales. La I Municipalidad de la Ligua recibe la actualización a bajo costo.
- Seguridad: Proveedores establecidos operan en plataformas certificadas (AWS, Azure) con SOC y cumplimiento ISO 27001.
- Interoperabilidad: Cuentan con conectores plataformas del servicio público.
- Capacitación: Estos proveedores tienen manuales de usuarios, jornadas de aprendizajes en el uso de los sistemas a demanda.
- Mesas de ayuda: Los proveedores cuentan con equipos dedicados para atender consultas, identificar fallas y gestionar su pronta respuesta.

- *Desventajas:*
  - Menor personalización ("traje a la medida"). Requiere adaptar procesos municipales al estándar del software (lo cual suele ser positivo para la eficiencia).
  - Propiedad: El municipio no es dueño del software, su uso está supeditado a la relación contractual entre ambos.

Evaluación: Actualmente la I Municipalidad de La Ligua no posee la capacidad y maduración tecnológica para gestionar un equipo de tecnología de desarrollo. El desarrollo propio en este contexto es ineficiente, de alto costo y riesgoso. La recomendación es licitar un servicio integral que contemple la totalidad de sistemas que requieran para gestionar el municipio y que entregue un soporte técnico estable durante el horario de funcionamiento normal de la municipalidad. Asimismo, es altamente recomendado ejecutar el plan de trabajo propuesto para mitigar los hallazgos identificados durante esta visita de auditoría ya que existen problemas como la duplicidad de equipos computacionales que genera una ineficiencia del gasto público y de igual manera afectan a los funcionarios/as municipales para cumplir con sus labores diarias y entregar el valor esperado por la comunidad.

11. Conclusiones

El diagnóstico general revela una situación de Riesgo Sistémico Crítico. La municipalidad opera bajo un modelo de "monodependencia tecnológica" extremadamente frágil, donde la continuidad operativa de servicios esenciales depende casi exclusivamente del conocimiento tácito de un único proveedor externo, sin el respaldo de contratos de propiedad intelectual adecuados, documentación técnica o planes de sucesión. Los sistemas legados, desarrollados en tecnologías obsoletas (Visual Basic 6.0) hace más de dos décadas, presentan vulnerabilidades de seguridad no mitigables y limitaciones funcionales severas que obligan a los funcionarios a realizar cálculos financieros críticos —como remuneraciones y patentes— de manera manual o en planillas de cálculo paralelas, incrementando exponencialmente el riesgo de fraude y error administrativo.

A pesar de los esfuerzos recientes por iniciar un proceso de modernización mediante el desarrollo de nuevos sistemas web en tecnologías más actuales (Laravel/PHP), la auditoría detectó que este proyecto replica los vicios estructurales del pasado: ausencia de metodologías de aseguramiento de calidad (QA), falta de documentación de código y una gestión de proyecto laxa que ha derivado en incumplimientos de plazos y baja adopción usuaria. La insatisfacción en departamentos clave como Rentas es total, reportándose errores graves en el cálculo de capitales y duplicidad de registros tributarios.

En materia de cumplimiento normativo, la brecha detectada es alarmante. La infraestructura actual carece de los controles básicos exigidos por el Marco de Ciberseguridad y la Ley de Protección de Datos Personales, tales como la gestión centralizada de identidades (Active Directory), la segregación de funciones y la trazabilidad de accesos a datos sensibles. La inexistencia de interoperabilidad real con plataformas del Estado (DocDigital, ClaveÚnica, Mercado Público) posiciona al municipio en una situación de incumplimiento ante los plazos fatales de la Ley de Transformación Digital.

Este informe concluye con una recomendación estratégica categórica: la suspensión controlada del desarrollo de software interno y la transición hacia la adquisición de soluciones de gestión municipal de mercado (ERP). Se fundamenta que la complejidad regulatoria y tecnológica actual excede las capacidades de un equipo de desarrollo unipersonal o reducido. Se propone un plan de acción de cinco ejes críticos para mitigar los riesgos inmediatos de seguridad y preparar a la institución para una licitación pública que permita modernizar su gestión bajo estándares de industria, garantizando así la probidad administrativa y la calidad del servicio al ciudadano.

La auditoría técnica realizada a la I. Municipalidad de La Ligua evidencia una situación de **emergencia tecnológica y administrativa**. La institución opera sobre una plataforma obsoleta, insegura y legalmente no conforme, sostenida únicamente por la dependencia precaria de un proveedor único.

1. **Riesgo de Colapso Operacional:** La dependencia de Visual Basic 6.0 y bases de datos sin soporte no es un "problema técnico", es una bomba de tiempo. Una falla de hardware o un ciberataque moderno podría dejar al municipio sin capacidad de recaudar ni pagar sueldos por semanas, ya que no existen capacidades de recuperación ante desastres (DRP) validadas.
2. **Incumplimiento Legal Flagrante:** La actual infraestructura impide materialmente el cumplimiento de la Ley de Transformación Digital y la Ley Marco de Ciberseguridad. Mantener esta situación expone al Alcalde a acusaciones de notable abandono de deberes, al no salvaguardar el patrimonio documental y digital de la comuna.
3. **Ineficiencia del Gasto:** Se están destinando más de $80 millones anuales a mantener sistemas que los propios usuarios califican con nota "0" y que requieren trabajo manual paralelo en Excel. Esto vulnera el principio de eficiencia y eficacia de la administración del Estado.

El camino a seguir es claro: La I. Municipalidad de La Ligua debe abandonar el paradigma del desarrollo propio artesanal y transitar, mediante una licitación pública competitiva y transparente, hacia soluciones de gestión municipal de mercado (SaaS) que garanticen seguridad, modernidad y cumplimiento normativo inmediato.

12. Anexo

Este anexo estructura las notas de los hallazgos críticos de la auditoría realizada a la I. Municipalidad de La Ligua, organizados estrictamente bajo el marco metodológico proporcionado en la sección "2.2. Procedimientos de Auditoría Ejecutados".

1. Objetivos de la Auditoría: Resultados de la Evaluación

A continuación, se detallan los resultados obtenidos al aplicar los objetivos fundamentales de la auditoría sobre la muestra de sistemas (Rentas, Remuneraciones, DOM, JPL, etc.):

A. Evaluación de Funcionalidad

- Contraste con procesos esperados: Se detectó que el sistema de Rentas y Patentes presenta fallas críticas en la lógica de negocio, calculando erróneamente capitales negativos como positivos y duplicando el cobro de intereses en patentes comerciales.
- Eficacia de los controles: En el área de Remuneraciones y Contabilidad, la funcionalidad del sistema es considerada nula por los usuarios, quienes deben realizar todo el proceso de cálculo de sueldos y descuentos de manera manual en planillas Excel externas por falta de confianza en el software.

B. Análisis de la Implementación Técnica

- Revisión de Código y Configuración:
  - Sistemas Legados: El núcleo transaccional opera sobre Visual Basic 6.0, una tecnología cuyo soporte finalizó en 2008 (EOL), lo que implica vulnerabilidades de seguridad intrínsecas y dependencia de componentes obsoletos.
  - Sistemas Web Nuevos (Laravel): Se encontraron exposiciones graves de configuración. Los archivos .env (que contienen credenciales de bases de datos y claves de API) son accesibles públicamente en los módulos de DOM, Activo Fijo y JPL. Además, las aplicaciones se ejecutan en modo de depuración (APP_DEBUG=true) en producción.
- Documentación: Se confirmó la inexistencia absoluta de documentación técnica del código o de las bases de datos; solo existen manuales de usuario insuficientes para la administración técnica.

C. Medición de Pertinencia y Utilidad

- Obsolescencia y Duplicidades: Los sistemas actúan como "silos" desconectados, obligando a la duplicidad de trabajo manual en áreas como Adquisiciones, que no se integra con Mercado Público.
- Percepción de Utilidad: El sistema de Rentas tiene un nivel de satisfacción de "0/Inexistente" debido a errores financieros, mientras que Salud reporta tiempos de respuesta de soporte inadecuados.

D. Verificación de Seguridad y Cumplimiento Normativo

- Políticas de Acceso: No existe un Directorio Activo (Active Directory), lo que resulta en una gestión de usuarios manual, descentralizada y con cuentas locales con privilegios administrativos.
- Protección de Datos: Se identificó el uso de herramientas de acceso remoto no seguras (AnyDesk no licenciado) para soporte, sin trazabilidad ni autenticación robusta.
- Cumplimiento Normativo: Existe un incumplimiento crítico de la Ley N° 21.663 (Marco de Ciberseguridad) y la Ley N° 21.180 (Transformación Digital), debido a la falta de inventario de activos, monitoreo de incidentes e interoperabilidad con el Estado.

2. Alcance y Cronograma: Ejecución del Trabajo

La auditoría cubrió la muestra estipulada (Juzgado de Policía Local, Contabilidad, Tesorería, Patentes, DOM, Remuneraciones) mediante las siguientes actividades ejecutadas:

Revisión Técnica de Sistemas

- Revisión de documentación: Se verificaron los contratos de las licitaciones ID 2783-74-LE24 y ID 2784-23-LE24, confirmando la ausencia de cláusulas claras de propiedad intelectual y especificaciones técnicas modernas.
- Evaluación de seguridad lógica: Se comprobó la exposición de rutas internas del sistema mediante la librería "Ziggy" en los desarrollos web, permitiendo a atacantes mapear la API completa.
- Inspección de bases de datos: Se detectó que la estructura de la base de datos en producción fue modificada directamente para adaptar el sistema nuevo, sin duplicación previa ni entorno de pruebas, afectando la integridad de los datos.
- Integración: Se constató la falta de integración con plataformas gubernamentales clave como DocDigital, ClaveÚnica y FirmaGob.

Entrevistas y Recolección de Información

- Usuarios Finales: Se entrevistó a personal de Rentas, Finanzas, Tesorería, RRHH y Salud, confirmando la dependencia de procesos manuales y la desconfianza en los datos del sistema.
- Responsable TI: Se realizaron entrevistas con el proveedor externo (Edison Maldonado) y el encargado de informática (Luis Valenzuela), revelando una dependencia unipersonal extrema ("Bus Factor = 1") donde el conocimiento reside exclusivamente en el proveedor externo.

3. Lista de Verificación General (Checklist de Hallazgos)

A continuación, se documentan los hallazgos según los ítems de control definidos en el procedimiento:

Documentación y Procesos de Desarrollo

- Requisitos y Manuales: [NO CUMPLE] Ausencia total de documentación técnica, diccionarios de datos o modelos entidad-relación.
- Código Fuente: [NO CUMPLE] El municipio no posee el código fuente. El contrato es ambiguo y el proveedor retiene el control, impidiendo auditorías o migraciones independientes.
- Control de Versiones: [RIESGO CRÍTICO] Se encontraron repositorios .git expuestos públicamente en los sistemas web, permitiendo la descarga del historial de cambios y código fuente por terceros no autorizados.

Seguridad de la Información

- Accesos Lógicos: [DEFICIENTE] Falta de segregación de funciones; usuarios comparten credenciales o utilizan cuentas con privilegios excesivos por falta de administración centralizada.
- Seguridad de Base de Datos: [CRÍTICO] Las credenciales de conexión a la base de datos (usuario y contraseña) están expuestas en texto plano en archivos .env accesibles vía web.
- Protección de Datos Personales: [ALTO RIESGO] Datos sensibles de salud y fichas sociales se manejan en sistemas sin cifrado y con controles de acceso vulnerables, incumpliendo la Ley 19.628.

Integridad de Datos y Operación

- Integridad Referencial: [FALLA] Se reportan problemas de "cruce de datos" y duplicidad de registros debido a modificaciones estructurales en la base de datos productiva sin control de calidad.
- Sincronización: [MANUAL] No existe sincronización automática efectiva; procesos críticos como el paso de información a contabilidad se realizan manualmente o mediante validaciones en Excel.

Cumplimiento Legal y Administrativo

- Normativa Digital: [INCUMPLIMIENTO] Los sistemas actuales son una barrera para la implementación de la Ley de Transformación Digital, al no soportar tramitación electrónica nativa ni interoperabilidad.
- Licencias de Terceros: [IRREGULAR] Se utiliza software de acceso remoto (AnyDesk) sin el licenciamiento corporativo adecuado.

Propiedad Intelectual y Registro de Software

- Cesión de Derechos: [NO EXISTE] A pesar de ser un desarrollo financiado por el municipio, el proveedor declara que "el desarrollo es de él", y los contratos no estipulan explícitamente la cesión del código fuente, contraviniendo la jurisprudencia de la CGR sobre obras por encargo.

Verificación con Usuarios

- Satisfacción: [BAJA/NULA] Existe resistencia al uso del "Sistema Nuevo" debido a retrasos y falta de funcionalidad. Se detectaron "soluciones informales" paralelas en Excel para suplir las carencias del sistema oficial en áreas críticas.

4. Revisión de las Bases de Datos

Backups y Recuperación:

- Política de Respaldo: [INSEGURA] Los respaldos no se realizan en dispositivos especializados (NAS) ni en la nube, sino en discos duros locales, violando la regla de seguridad básica 3-2-1 y exponiendo los datos a destrucción por Ransomware.
- Pruebas de Restauración: No hay evidencia de pruebas de restauración exitosas ni de un entorno de *Staging* para validar la integridad de los datos antes de realizar cambios estructurales.

Controles de Auditoría:

- Logs: Si bien existe a nivel de base de datos un log que permite identificar quién modificó un registro sensible, no existe trazabilidad clara ni auditoría de transacciones como modelo de políticas que permita verificar su correcto funcionamiento.

5. Entrevistas y Compilación de Evidencias (Consolidación)

La contrastación entre las entrevistas y la inspección técnica confirma un escenario de Riesgo Sistémico Crítico.

- Evidencia Consolidada:
  - Los usuarios reportan errores de cálculo (Rentas) que fueron validados técnicamente por la obsolescencia del motor de base de datos y la falta de integridad referencial.
  - La dependencia del proveedor (mencionada en entrevistas) se comprobó con la falta de documentación y el acceso exclusivo al código fuente.
  - La inseguridad percibida se materializó en el hallazgo técnico de credenciales expuestas y puertos de depuración abiertos.

13. Bibliografía

- Biblioteca del Congreso Nacional de Chile. (2019). *Ley N° 21.180: Transformación Digital del Estado.* [1]
- Biblioteca del Congreso Nacional de Chile. (2024). *Ley N° 21.663: Ley Marco de Ciberseguridad.* [3]
- Biblioteca del Congreso Nacional de Chile. (2024). *Ley N° 21.719: Protección de Datos Personales.* [6]
- Biblioteca del Congreso Nacional de Chile. (2023). *Ley N° 21.634: Moderniza la Ley de Compras Públicas.* [39]
- Center for Internet Security (CIS). (2021). *CIS Controls Version 8.* [15]
- Contraloría General de la República. (2019). *Informe Final N° 1.097-18: Auditoría a Tecnologías de la Información.* [40]
- DeLone, W. H., & McLean, E. R. (2003). *The DeLone and McLean Model of Information Systems Success: A Ten-Year Update*. Journal of Management Information Systems. [41]
- ISACA. (2018). *COBIT 2019 Framework: Governance and Management Objectives.* [12]
- ISO. (2018). *ISO 31000:2018 Risk management — Guidelines.* [18]
- Ministerio Secretaría General de la Presidencia. (2023). *Decreto N° 12: Norma Técnica de Interoperabilidad.* [42]
- NIST. (2012). *Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments.* [11]
- OWASP. (2021). *OWASP Top 10:2021.* [36]

Obras citadas

1. Gestión municipal en Chile y entrada en régimen de la Ley 21.180. El desafío de la transformación digital - Dialnet, fecha de acceso: diciembre 30, 2025, https://dialnet.unirioja.es/descarga/articulo/9540138.pdf
2. Transformación Digital del Estado - Implementación de la Ley Nº 21.180 a nivel municipal - BCN, fecha de acceso: diciembre 30, 2025, https://www.bcn.cl/obtienearchivo?id=repositorio/10221/37193/1/BCN_Implementacion_de_la_Ley_No_21.180_Transformacion_digital_del_Estado_a_nivel_de_los_municipios_final.pdf
3. Ley 21663, fecha de acceso: diciembre 30, 2025, https://nuevo.leychile.cl/servicios/Consulta/Exportar?radioExportar=Normas&exportar_formato=pdf&nombrearchivo=Ley-21663_08-ABR-2024&exportar_con_notas_bcn=False&exportar_con_notas_originales=False&exportar_con_notas_al_pie=False&hddResultadoExportar=1202434.2222-02-02.0.0%23

4. Guía práctica de la Ley Marco de Ciberseguridad en Chile (Ley 21.663) - ManageEngine, fecha de acceso: diciembre 30, 2025, https://www.manageengine.com/latam/images/chile-cybersecurity-law-ebook.pdf
5. The Dangers of End-of-Life Software | Property & Casualty - CBIZ, fecha de acceso: diciembre 30, 2025, https://www.cbiz.com/insights/article/the-dangers-of-end-of-life-software-property-casualty
6. Ley Chile - Ley 21719 - Biblioteca del Congreso Nacional - BCN, fecha de acceso: diciembre 30, 2025, https://www.bcn.cl/leychile/Navegar?idNorma=1209272
7. Guía Práctica para facilitar la implementación de la nueva Ley de Protección de Datos Personales en la Administración, fecha de acceso: diciembre 30, 2025, https://wikiguias.digital.gob.cl/datos-personales/guia-practica-implementacion-nueva-ley-datos-personales
8. Presidente Boric promulgó ley que moderniza las compras públicas y destacó que fortalecerá la transparencia, a las Mipymes e impulsará la innovación - Ministerio de Hacienda, fecha de acceso: diciembre 30, 2025, https://www.hacienda.cl/subsecretaria/noticias/presidente-boric-promulgo-ley-que-moderniza-las-compras-publicas-y-destaco-que
9. Ley Chile - Ley 21634 - Biblioteca del Congreso Nacional - BCN, fecha de acceso: diciembre 30, 2025, https://www.bcn.cl/leychile/navegar/imprimir?idNorma=1198903&idVersion=2024-12-12
10. What is NIST SP 800-30 - CyberSaint, fecha de acceso: diciembre 30, 2025, https://www.cybersaint.io/blog/what-is-nist-sp-800-30
11. NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, fecha de acceso: diciembre 30, 2025, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
12. COBIT® | Control Objectives for Information Technologies® - ISACA, fecha de acceso: diciembre 30, 2025, https://www.isaca.org/resources/cobit
13. What Is the COBIT Framework? IT Governance and Management - Legit Security, fecha de acceso: diciembre 30, 2025, https://www.legitsecurity.com/aspm-knowledge-base/what-is-cobit-framework
14. What is COBIT? A framework for alignment and governance - CIO, fecha de acceso: diciembre 30, 2025, https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html
15. CIS Critical Security Controls Version 8, fecha de acceso: diciembre 30, 2025, https://www.cisecurity.org/controls/v8
16. CIS Critical Security Controls Version 8.1, fecha de acceso: diciembre 30, 2025, https://www.cisecurity.org/controls/v8-1

17. Implementation Guide - CIS Center for Internet Security, fecha de acceso: diciembre 30, 2025, https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf
18. ISO 31000 Risk Management Framework: Your Complete Guide USA - Protecht, fecha de acceso: diciembre 30, 2025, https://www.protechtgroup.com/en-us/blog/iso-31000-risk-management-framework-your-complete-guide
19. The Basics of ISO 31000 – Risk Management - Riskonnect, fecha de acceso: diciembre 30, 2025, https://riskonnect.com/business-continuity-resilience/the-basics-of-iso-31000-risk-management/
20. Service desk KPIs & dashboards: from SLA to time-to-value - SMC Consulting, fecha de acceso: diciembre 30, 2025, https://www.smcconsulting.be/service-desk-kpis-complete-guide/
21. 17 help desk and service desk metrics to measure support performance - Zendesk, fecha de acceso: diciembre 30, 2025, https://www.zendesk.com/blog/top-10-help-desk-metrics/
22. Validation of the DeLone and McLean Information Systems Success Model - PMC - NIH, fecha de acceso: diciembre 30, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC5334133/
23. Municipalidades de Lo Prado y La Reina - ChileCompra, fecha de acceso: diciembre 30, 2025, http://www.chilecompra.cl/wp-content/uploads/2025/05/Municipalidades-de-Lo-Prado-y-La-Reina.pdf
24. DIRECTIVA DE CONTRATACIÓN PÚBLICA N° 8 - Escritorio de Alejandro Barros, fecha de acceso: diciembre 30, 2025, https://www.alejandrobarros.com/wp-content/uploads/old/Directiva_N_8_Contratacion_TICs.pdf
25. 2783-74-LE24.pdf
26. Contraloría General de la República - ChileCompra, fecha de acceso: diciembre 30, 2025, https://www.chilecompra.cl/wp-content/uploads/2016/11/dictamen-n-24685.pdf
27. Contraloría advierte improcedencia de invocar propiedad intelectual para justificar trato directo en capacitaciones municipales - DOE | Actualidad Jurídica, fecha de acceso: diciembre 30, 2025, https://actualidadjuridica.doe.cl/contraloria-advierte-improcedencia-de-invocar-propiedad-intelectual-para-justificar-trato-directo-en-capacitaciones-municipales/
28. IT governance implementation framework in small and medium enterprise - ResearchGate, fecha de acceso: diciembre 30, 2025, https://www.researchgate.net/publication/260480612_IT_governance_implementation_framework_in_small_and_medium_enterprise

29. VB6 Migration Guide: Risks, Strategies & Best Practices - softacom, fecha de acceso: diciembre 30, 2025, https://www.softacom.com/blog/migration-from-vb6-challenges-strategies-and-best-practices/
30. VB6 Is Still Alive in 2025 - But Should You Keep It? | ModLogix, fecha de acceso: diciembre 30, 2025, https://modlogix.com/blog/vb6-is-still-alive-in-2025-but-should-you-keep-it/
31. HIPAA / HITECH Compliance Risks with Visual Basic 6.0 | Mobilize.Net, fecha de acceso: diciembre 30, 2025, https://www.gapvelocity.ai/resources/guides/hipaa-risks-vb6
32. SQL Server 2022 - Microsoft Lifecycle, fecha de acceso: diciembre 30, 2025, https://learn.microsoft.com/en-us/lifecycle/products/sql-server-2022
33. SQL Server End of Life: All You Need To Know - Lansweeper.com, fecha de acceso: diciembre 30, 2025, https://www.lansweeper.com/blog/eol/a-comprehensive-guide-to-sql-server-end-of-life/
34. 12 Top Security Best Practices for Your Laravel Application | SaaSykit, fecha de acceso: diciembre 30, 2025, https://saasykit.com/blog/12-top-security-best-practices-for-your-laravel-application
35. Laravel - OWASP Cheat Sheet Series, fecha de acceso: diciembre 30, 2025, https://cheatsheetseries.owasp.org/cheatsheets/Laravel_Cheat_Sheet.html
36. OWASP Top 10:2025, fecha de acceso: diciembre 30, 2025, https://owasp.org/Top10/2025/en/
37. Guía práctica de la Escala de Usabilidad del Sistema (SUS) para el año 2025 - UXtweak, fecha de acceso: diciembre 30, 2025, https://blog.uxtweak.com/es/escala-de-usabilidad-del-sistema/
38. SUS - A quick and dirty usability scale - AHRQ Digital Healthcare Research, fecha de acceso: diciembre 30, 2025, https://digital.ahrq.gov/sites/default/files/docs/survey/systemusabilityscale%2528sus%2529_comp%255B1%255D.pdf
39. Ley 21634 - Biblioteca del Congreso Nacional de Chile, fecha de acceso: diciembre 30, 2025, https://nuevo.leychile.cl/navegar?idNorma=1198903&idParte=10475275&idVersion=2024-12-12
40. INFORME FINAL - Maho.cl, fecha de acceso: diciembre 30, 2025, https://www.maho.cl/categorias2025/21-Resultado%20auditoria%20al%20ejercicio%20presupuestario/INFORME%20FINAL%20N%C2%B0%201.097-18%20AH%20FISC%20A%20TECN%20DE%20LA%20INFORM%20-%20JULIO%202019.pdf

41. The DeLone and McLean Model of Information Systems Success: A Ten-Year Update, fecha de acceso: diciembre 30, 2025, https://www.researchgate.net/publication/220591866_The_DeLone_and_McLean_Model_of_Information_Systems_Success_A_Ten-Year_Update
42. Decreto 12 | Interoperabilidad | Wiki Guías | Secretaría de Gobierno Digital, fecha de acceso: diciembre 30, 2025, https://wikiguias.digital.gob.cl/Normas/Decreto12