Plan Director SGSI para Servicios Públicos

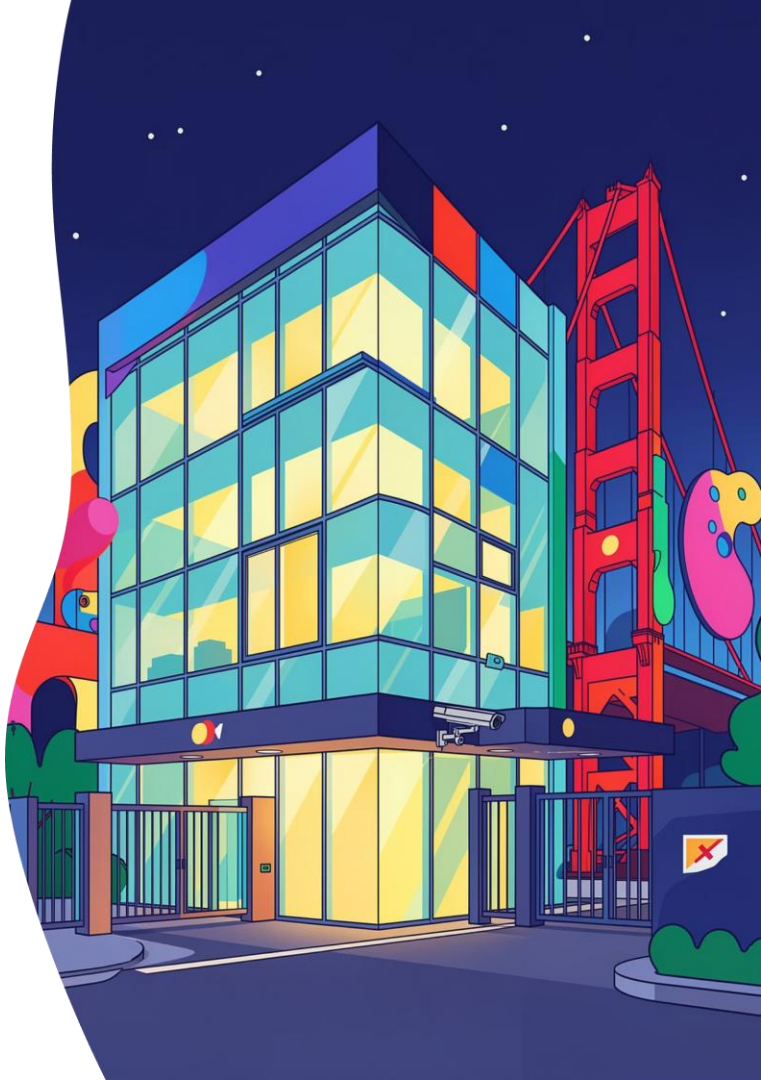
ISO 27001 + 27701 + 22301 | OPSEC | CTI | THREAT HUNTING

Ciberseguridad Real, no de Papel — Protección efectiva de datos personales bajo Ley 21.719 y cumplimiento ANCI bajo Ley 21.663

Preparado por: TTPSEC SpA — Consultoría Especializada en Ciberseguridad Crítica
Director Académico y CEO: Sebastián Vargas Yáñez
Marco Regulatorio: Ley 21.663 | Ley 21.719 | Estatuto Administrativo
Horizonte: 36 meses | **Versión:** 1.0 — 2026

Normas Integradas

- ISO/IEC 27001:2022
- ISO/IEC 27701:2019
- ISO 22301:2019
- NIST CSF 2.0



¿Por Qué Fracasan los SGSI en Servicios Públicos?

DIAGNÓSTICO HONESTO

Cumplimiento Cosmético

Implementaciones centradas en documentación sin capacidades defensivas reales. Se protege contra "amenazas genéricas" sin modelo de adversario explícito.

Conflicto Estructural

CISO subordinado a TI neutraliza la función de seguridad. Rotación de autoridades sin compromiso plurianual sabotea ciclos de mejora continua.

Datos Personales Desprotegidos

Sin ROPA vivo, sin DPIAs, sin minimización real. Logs sin retención adecuada hacen forense post-incidente imposible.

Infraestructura Vulnerable

Backups sin air-gap que ransomware destruye en horas. Capacitaciones anuales que no transforman cultura ni comportamiento.

Resultado: Servicios públicos chilenos siguen siendo objetivo prioritario de APTs, ransomware y hacktivismo regional.

Marco Regulatorio Chileno Aplicable

Ley 21.663 — Marco de Ciberseguridad

- Crea Agencia Nacional de Ciberseguridad (ANCI)
- Define Servicios Esenciales y Operadores de Importancia Vital (OIV)
- Deberes de reporte de incidentes y compartición con CSIRT de Gobierno
- Sanciones por incumplimiento aplicables a servicios públicos

Ley 21.719 — Protección de Datos Personales

Vigencia plena diciembre 2026

- Agencia de Protección de Datos con potestad sancionatoria
- DPO obligatorio para organismos públicos
- Notificación de brechas en 72 horas
- DPIAs obligatorias para tratamientos de alto riesgo
- Multas significativas y responsabilidad de funcionarios

Estatuto Administrativo

- Régimen disciplinario aplicable a infracciones de seguridad
- Deberes de probidad y reserva

Normas Técnicas Integradas

- ISO/IEC 27001:2022 (SGSI)
- ISO/IEC 27701:2019 (PIMS — extensión privacidad)
- ISO 22301:2019 (continuidad de negocio)
- NIST CSF 2.0 (referencia operacional)

Arquitectura del Plan Director

TRES CAPAS INTEGRADAS | 36 MESES

Capa Normativa — Gobierno

ISO 27001 + 27701 + 22301 como columna vertebral documental y de gestión. Marco de referencia certificable y auditable.

Capa Operacional — Defensa Real

OPSEC + Cyber Threat Intelligence + Threat Hunting + Hardening Continuo. Capacidades defensivas reales contra adversarios reales.

Capa de Privacidad — Protección Efectiva

Cumplimiento real Ley 21.719 con ROPA vivo, DPIAs, derechos ARCOP+, cifrado integral y DPO operativo.

Horizonte Temporal

36 meses divididos en 6 fases secuenciales y transversales con hitos verificables.

Modelo de Madurez

CMMI 0-5. Objetivo nivel 4 al cierre del ciclo de 36 meses.

Cobertura

SGSI completo, certificable y operativo. Alineado con obligaciones ANCI y Ley 21.719.

Fase 0 — Diagnóstico y Línea Base

MES 1–2

Objetivo: Saber exactamente dónde estamos antes de planificar.

Actividades Core

- GAP Assessment triple norma (27001 + 27701 + 22301) con escala CMMI 0-5 por dominio
- Inventario de activos con clasificación por sensibilidad y criticidad
- Mapeo de flujos de datos personales (Data Flow Diagrams) — base obligatoria 27701 y Ley 21.719
- Attack Surface Analysis externo: dominios .gob.cl, subdominios, servicios expuestos, leaks en pastebins y dark web
- Identificación de OIV y Servicios Esenciales según Ley 21.663
- Análisis de Impacto al Negocio (BIA) con RTO/RPO realistas por servicio crítico

Entregables

- Informe de línea base con scoring de madurez
- Matriz de hallazgos priorizados por riesgo
- Registro de tratamientos de datos personales (ROPA inicial)
- Declaración preliminar de aplicabilidad
- Mapa de superficie de ataque externa

Fase 1 — Gobierno y Marco Normativo

MES 2–4

Estructura de Gobierno Propuesta

01

Comité de Seguridad

Presidido por la máxima autoridad del servicio — no delegable.

02

CISO Independiente

Dependencia directa del Jefe de Servicio — nunca bajo TI por conflicto de interés estructural.

03

DPO Obligatorio

Delegado de Protección de Datos — figura obligatoria Ley 21.719 para organismos públicos.

04

Comité de Crisis Cibernética

Activación 24/7 con equipo SOC/CSIRT conectado con CSIRT de Gobierno y ANCI.

Cuerpo Documental Base

Documentación real y operativa — no copy-paste de plantillas genéricas.

- Política General de Seguridad firmada por Jefe de Servicio
- Política de Protección de Datos Personales alineada Ley 21.719 + 27701
- Política de Continuidad de Negocio (22301)
- Procedimientos operativos: gestión de incidentes, accesos, cambios, vulnerabilidades, proveedores, brechas
- Integración con Estatuto Administrativo y régimen disciplinario

Fase 2 — OPSEC Real

MES 3–6

OPSEC no es "no compartas la clave". Es disciplina operacional contra adversarios reales.

Modelo de Adversario Explícito

Mapeo MITRE ATT&CK Enterprise/ICS contra APT-C-36/Blind Eagle, Lazarus, hacktivismo regional y ransomware crews activos en LATAM.

Compartimentación de Información

Principio need-to-know con DLP, etiquetado automático (Microsoft Purview o equivalente), clasificación obligatoria por nivel de sensibilidad.

Gestión Robusta de Identidades

MFA obligatorio sin excepciones, PAM para cuentas administrativas, JIT access, eliminación de cuentas compartidas.

Segmentación de Red

Zero trust progresivo, microsegmentación de servicios críticos, separación entre redes administrativas, ciudadanas y operacionales.

Higiene Digital de Funcionarios

Capacitación específica para autoridades: huella digital, OSINT defensivo, dispositivos personales y comunicaciones sensibles.

Counter-OSINT

Monitoreo continuo de filtraciones: metadatos en documentos publicados, EXIF en imágenes, exposición LinkedIn de funcionarios sensibles.

Fase 3 — Cyber Threat Intelligence (CTI)

MES 4–8

Inteligencia real, no feeds gratuitos que nadie lee.

CTI Estratégica

Análisis de actores con motivación contra Estado chileno y sector público regional. Fuentes: ANCI, CSIRT Gobierno, MISP comunitarios, ENISA, CISA advisories, reportes Mandiant/CrowdStrike/Recorded Future.

CTI Operacional

TTPs específicas observadas contra servicios públicos similares. Mapeo continuo a MITRE ATT&CK. Integración con D3FEND para contramedidas defensivas.

CTI Táctica

IoCs (hashes, IPs, dominios) enriquecidos e integrados al SIEM/EDR. Plataforma TIP recomendada: OpenCTI (open-source serio), MISP para compartición.

Integración obligatoria: CSIRT de Gobierno + Red de Conectividad del Estado + ANCI. La Ley 21.663 establece deberes de reporte y compartición que pocos cumplen bien.

Fase 4 — Threat Hunting Proactivo

MES 6–10

Aquí se separan los SGSI reales de los de papel.

Modelo: Hypothesis-Driven

Pyramid of Pain + Diamond Model como marcos metodológicos:

- Hunts basados en hipótesis derivadas de CTI
- Hunts basados en TTPs MITRE ATT&CK priorizadas por matriz probabilidad/impacto
- Hunts de anomalías UEBA sobre cuentas privilegiadas y accesos a datos personales masivos
- Búsqueda activa de persistencia: WMI subscriptions, scheduled tasks anómalas, servicios atípicos, GPO modifications

Stack Técnico Mínimo Viable

- EDR/XDR en todos los endpoints y servidores — no antivirus tradicional
- SIEM con retención mínima 12 meses (90 días caliente, resto frío)
- Log sources críticos: AD, DNS, Proxy, EDR, firewalls, aplicaciones con datos personales
- Sysmon con configuración Olaf Hartong o SwiftOnSecurity en todos los Windows
- Plataforma de hunting: Velociraptor (gratis, excelente) o capacidad nativa del XDR

Cadencia Mínima

2 hunts formales por mes con informe, IoCs generados, detecciones nuevas creadas y lecciones documentadas.

Fase 5 — Hardening Sistemático

MES 5–12, CONTINUO

Hardening no es un proyecto, es práctica continua.

Baselines Obligatorias

- CIS Benchmarks Level 1 mínimo, Level 2 para sistemas con datos sensibles
- STIG (DISA) para entornos de alta criticidad
- Microsoft Security Baselines para Windows/M365/Azure
- CIS Controls v8 IG2 mínimo, IG3 para OIV

Frentes de Hardening

- **Sistemas operativos:** Windows Server, Linux, estaciones de trabajo
- **Active Directory:** tier model, eliminación de delegations peligrosas, protección contra Kerberoasting/AS-REP roasting, LAPS, gMSA
- **Cloud:** CSPM continuo, eliminación de buckets públicos, IAM least privilege
- **Aplicaciones web:** OWASP ASVS L2 mínimo, WAF, DAST/SAST en pipelines
- **Bases de datos:** cifrado en reposo y tránsito, masking, auditoría granular
- **Email:** SPF + DKIM + DMARC en reject, anti-phishing avanzado
- **Red:** segmentación, NAC, eliminación de protocolos legacy (SMBv1, NTLMv1, TLS<1.2)

Verificación continua: Scans de vulnerabilidades semanales internos, mensuales externos, pentest anual, red teaming bianual.

Fase 6 — Protección Real de Datos Personales

TRANSVERSAL | LEY 21.719 + ISO/IEC 27701

ROPA Vivo

Registro de tratamientos actualizado automáticamente cuando cambian sistemas, integrado con CMDB. Base obligatoria para cumplimiento Ley 21.719.

DPIA/EIPD Obligatorias

Evaluaciones de impacto en privacidad para tratamientos de alto riesgo: datos sensibles, decisiones automatizadas, tratamiento masivo.

Privacy by Design y by Default

Integrado en SDLC y compras de software. La privacidad no es un parche posterior, es un requisito de diseño.

Derechos ARCOP+

Procesos automatizados para Acceso, Rectificación, Cancelación, Oposición, Portabilidad y Bloqueo con SLA conforme Ley 21.719.

Cifrado Integral

AES-256 en reposo, TLS 1.3 en tránsito, tokenización para identificadores. Gestión de brechas con notificación a Agencia en 72h.

Encargados de Tratamiento

Contratos DPA conformes Art. 15 ter Ley 19.628 con todos los proveedores. Transferencias internacionales con cláusulas tipo y evaluación de país receptor.

Continuidad de Negocio — ISO 22301

INTEGRADA CON TODO EL PLAN, NO ANEXA

Componentes Operativos

- BIA detallado por proceso crítico de servicio público
- Estrategias de continuidad documentadas con RTO/RPO por sistema
- Planes de Continuidad (BCP) y Recuperación ante Desastres (DRP)
- Backups con regla 3-2-1-1-0 — incluye copia inmutable air-gapped (clave anti-ransomware)
- Centro de Operaciones Alterno (sitio físico o cloud) para servicios críticos
- Pruebas de restauración con métricas objetivas — no "el backup existe" sino "se restauró exitosamente"

Ejercicios con Escalada Progresiva

01

Tabletop

Trimestral — discusión de escenarios con equipo directivo.

02

Walkthrough

Semestral — revisión paso a paso de procedimientos.

03

Simulación Parcial

Semestral — activación de componentes específicos del BCP.

04

Simulación Completa

Anual — activación integral con métricas objetivas.

Cronograma Maestro — 36 Meses

1

Mes 1–2

Diagnóstico, GAP triple norma, ROPA inicial, attack surface analysis, BIA documentado.

2

Mes 3–6

Gobierno establecido, políticas firmadas, OPSEC base operativo, hardening crítico iniciado, primer ROPA completo.

3

Mes 7–12

CTI operativa con feeds integrados, primer ciclo Threat Hunting (2 hunts/mes), DPIAs prioritarias, BCP/DRP probados.

4

Mes 13–18

Primera auditoría interna integrada, ejercicios de continuidad maduros, CTI estratégica, hardening cobertura ≥90%.

5

Mes 19–24

Certificación ISO 27001:2022 + ISO/IEC 27701:2019, alineación plena Ley 21.719, madurez CMMI nivel 3.

6

Mes 25–36

Certificación ISO 22301:2019, programa red teaming establecido, madurez CMMI nivel 4, mejora continua institucionalizada.

KPIs Operativos — No de Vanidad

MÉTRICAS QUE IMPORTAN

Indicadores objetivos y medibles para evaluar el avance real del SGSI en cada etapa del plan director.

Indicador	Objetivo Año 1	Objetivo Año 3
MTTD (Mean Time to Detect)	< 24 horas	< 4 horas
MTTR (Mean Time to Respond)	< 72 horas	< 12 horas
% cuentas privilegiadas con PAM + MFA	100% (mes 6)	100% sostenido
Cobertura EDR/XDR	100% (mes 4)	100% sostenido
Hunts ejecutados por mes	≥ 2 (desde mes 8)	≥ 4 mensuales
Vulnerabilidades críticas con SLA cumplido	≥ 95%	≥ 99%
DPIAs sobre tratamientos de alto riesgo	100% antes dic-2026	100% sostenido
Tiempo respuesta solicitudes ARCOP	< 20 días hábiles	< 10 días hábiles
Ejercicios de continuidad anuales	≥ 4	≥ 6
Brechas notificadas dentro de 72h	100%	100%

Stack Tecnológico Recomendado

Capa de Visibilidad

- SIEM: Microsoft Sentinel / Splunk / Elastic Security
- EDR/XDR: Microsoft Defender XDR / CrowdStrike Falcon / SentinelOne
- Sysmon configuración hardened (Olaf Hartong)
- NDR para zonas críticas

Capa de Identidad

- IAM: Microsoft Entra ID / Okta
- PAM: CyberArk / BeyondTrust / Delinea
- MFA obligatorio: FIDO2 hardware tokens para administradores

Capa de Datos

- DLP: Microsoft Purview / Forcepoint
- Cifrado: BitLocker, LUKS, Always Encrypted, TDE
- DAM para bases con datos personales

Capa de Inteligencia

- TIP: OpenCTI (open-source) o MISP
- Threat Hunting: Velociraptor, KQL queries, Sigma rules

Capa de Continuidad

- Backup inmutable: Veeam con immutability / Rubrik / Cohesity
- DRP cloud: Azure Site Recovery / AWS Disaster Recovery

Presupuesto Estimado Referencial

SERVICIO PÚBLICO MEDIANO: 500–2.000 FUNCIONARIOS

Período	Rango USD	Componentes Principales
Año 1	USD 400K – 700K	Consultoría e implementación, herramientas core (EDR/XDR, SIEM, PAM, DLP), capacitación especializada, primer ciclo de hardening, GAP Assessment triple norma profesional
Año 2	USD 250K – 450K	Operación continua y licenciamiento sostenido, certificación ISO 27001 + ISO/IEC 27701, programa de mejora continua, auditorías internas y externas
Año 3	USD 200K – 350K	Operación madura y mejora incremental, certificación ISO 22301, programa de red teaming, renovaciones de certificación

Variables Fuertes de Costo

EDR/XDR
USD 40–80 por endpoint/año

SIEM
Depende de volumen de logs ingestados (GB/día)

PAM
USD 80–150K licenciamiento típico

Modelo de Adversario para Servicios Públicos Chilenos

ACTORES PRIORIZADOS CON BASE EN INTELIGENCIA DISPONIBLE

APTs Estatales

- APT-C-36 (Blind Eagle) — activo en LATAM contra gobiernos
- Lazarus Group — interés en sectores estratégicos
- Actores asociados a tensiones geopolíticas regionales

Crimen Organizado

- Ransomware crews: LockBit (residual), BlackCat/ALPHV, BlackSuit, Akira, Play
- Initial Access Brokers que venden accesos a redes gubernamentales

Hacktivismo

- Grupos regionales con motivación política contra gobiernos
- Defacement y data leaks como tácticas principales

Insiders

- Funcionarios descontentos con acceso privilegiado
- Riesgo elevado en periodos de cambio de autoridades
- Negligencia más frecuente que malicia

Vector más explotado en sector público LATAM: Phishing → ejecución de payload → escalada en AD → exfiltración → cifrado. El SGSI debe romper esta cadena en múltiples puntos.

Mapeo MITRE ATT&CK Priorizado

TOP 15 TÉCNICAS CRÍTICAS PARA SERVICIOS PÚBLICOS

Cada técnica debe tener detección Sigma/KQL implementada y hunt asociado.

Acceso Inicial

T1566 Phishing
Spearphishing Attachment / Link

T1190 Exploit
Public-Facing Application

T1078 Valid Accounts
Credenciales legítimas comprometidas

Ejecución y Persistencia

T1059 Scripting
PowerShell, cmd

T1053 Scheduled Task
Persistencia vía tareas programadas

T1547 Boot Autostart
Logon Autostart Execution

Escalada y Movimiento Lateral

T1068 Privilege Escalation
Exploitation for Privilege Escalation

T1003 Credential Dumping
LSASS, NTDS.dit

T1021 Remote Services
SMB, RDP, WMI

T1558 Kerberoasting
Steal or Forge Kerberos Tickets

C2, Exfiltración e Impacto

T1071 App Layer Protocol
HTTPS C2

T1572 Protocol Tunneling
Evasión de controles de red

T1567 Exfiltración Web
Exfiltration Over Web Service

T1486 Ransomware
Data Encrypted for Impact

T1485 Data Destruction
Destrucción de datos y evidencia

Riesgos del Propio Plan y Mitigaciones

HONESTIDAD CONSULTIVA — CINCO SABOTEADORES TÍPICOS

1 Rotación de Autoridades

Mitigación: Compromiso documentado en acto administrativo plurianual, métricas públicas de avance, integración con metas presidenciales.

2 Presupuesto Plurianual No Asegurado

Mitigación: Financiamiento por fases con casos de negocio sólidos, vinculación a multas potenciales bajo Ley 21.719 y obligaciones ANCI.

3 Resistencia Cultural

Mitigación: Quick wins visibles en primeros 90 días (MFA universal, EDR desplegado, PAM en cuentas críticas), comunicación ejecutiva mensual, programa de embajadores internos.

4 Vendor Lock-in en Herramientas

Mitigación: Arquitectura abierta, preferencia por estándares (Sigma, STIX/TAXII, SCAP), cláusulas de portabilidad de datos en contratos.

5 Equipo Insuficiente o Sin Perfil

Mitigación: Modelo híbrido SOC interno + MSSP especializado, programa de formación con certificaciones (GCIH, GCFA, GCTI, GCIA).

Roadmap de Certificaciones y Aseguramiento

Año 1 — Preparación

- Auditoría interna ISO 27001:2022 — final año 1
- Pre-auditoría ISO/IEC 27701:2019
- Cumplimiento documental Ley 21.719 listo para diciembre 2026

Año 2 — Certificación

- Certificación ISO 27001:2022 (etapa 1 + etapa 2)
- Certificación ISO/IEC 27701:2019 integrada
- Primer pentest externo formal
- Primera prueba de continuidad completa

Año 3 — Madurez

- Certificación ISO 22301:2019
- Red Team exercise anual
- Auditoría de cumplimiento Ley 21.663 ante ANCI
- Reevaluación de madurez CMMI — objetivo nivel 4

Mantenimiento continuo: Auditorías de seguimiento anuales por organismo certificador acreditado, recertificación trianual, auditorías ANCI según calendario regulatorio.

Gobierno de Datos Personales — Arquitectura DPO

DELEGADO DE PROTECCIÓN DE DATOS | LEY 21.719

Perfil Requerido

- Conocimiento experto en marco normativo de protección de datos
- Independencia funcional — no puede ser reemplazado por instrucciones sobre sus tareas
- Reporte directo a máxima autoridad
- Recursos asignados para el ejercicio efectivo del cargo

Responsabilidades Operativas

- Mantenimiento del ROPA actualizado
- Asesoría en DPIAs
- Punto de contacto con Agencia de Protección de Datos
- Atención de derechos ARCOP+
- Investigación interna de brechas y reporte regulatorio
- Capacitación continua de funcionarios

Integración con SGSI

Co-presidencia

DPO co-preside Comité de Privacidad junto al CISO.

Firma Conjunta

CISO y DPO firman conjuntamente todas las DPIAs.

Reporte Coordinado

Notificación coordinada a ANCI (Ley 21.663) y Agencia de Protección de Datos (Ley 21.719).

Gestión de Incidentes — Doble Notificación

PROCEDIMIENTO INTEGRADO BAJO DOS MARCOS LEGALES

Notificación Obligatoria (24–72 horas)

- CSIRT de Gobierno y ANCI bajo Ley 21.663 (plazos según reglamento)
- Agencia de Protección de Datos Personales en 72h máximo bajo Ley 21.719
- Titulares de datos cuando aplique riesgo alto

Post-Incidente

- Reporte ejecutivo a máxima autoridad
- Lecciones aprendidas integradas a mejora continua
- Actualización de detecciones y hunts
- Revisión de controles fallidos

Cultura de Seguridad — Más que Capacitaciones

PROGRAMA DE CULTURA SOSTENIBLE

Capacitación Segmentada por Rol

Autoridades

OPSEC personal, gestión de comunicaciones sensibles, riesgo reputacional.

Personal con Datos Sensibles

Privacidad, minimización, derechos de titulares.

TI/Operaciones

Hardening, gestión segura de cambios, respuesta a incidentes.

Funcionarios Generales

Phishing, ingeniería social, higiene digital.

Componentes del Programa

- Onboarding obligatorio con evaluación
- Refresco anual obligatorio con contenidos actualizados
- Campañas mensuales de phishing simulado con métricas y refuerzo dirigido
- Comunicados breves quincenales sobre amenazas actuales
- Reconocimiento público de comportamientos seguros
- Canal anónimo de reporte de incidentes y conductas sospechosas

Métrica de éxito: Reducción sostenida de tasa de clicks en phishing simulado y aumento de reportes proactivos por parte de funcionarios.

Gestión de Proveedores y Cadena de Suministro

RIESGO CRÍTICO SUBESTIMADO EN SERVICIOS PÚBLICOS

Cláusulas Tipo Recomendadas para Proveedores Críticos

Confidencialidad Reforzada
Obligaciones contractuales de reserva con régimen de responsabilidad.

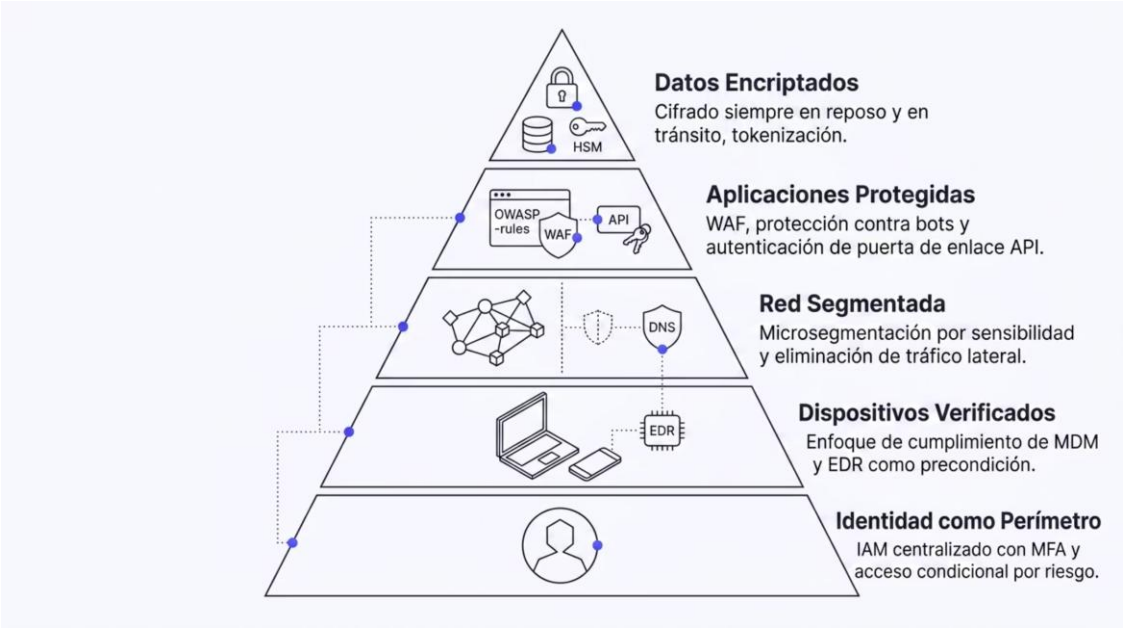
Subprocesadores
Autorización previa obligatoria para cualquier subcontratación.

Localización de Datos
Chile/región autorizada con restricciones de transferencia internacional.

Plan de Salida
Continuidad de servicio garantizada y eliminación verificada al término.

Arquitectura Técnica Objetivo — Zero Trust Progresivo

NUNCA CONFIAR, SIEMPRE VERIFICAR | ASUMIR BRECHA | PRIVILEGIO MÍNIMO



Entregables del Plan por Fase

Fase 0 (Mes 1–2)

Informe GAP Assessment triple norma con scoring CMMI, ROPA inicial completo, mapa de superficie de ataque externa, BIA documentado.

Fase 1 (Mes 2–4)

Política General de Seguridad firmada, 12+ procedimientos operativos, estructura de gobierno formalizada, SoA inicial.

Fase 2 (Mes 3–6)

Modelo de adversario documentado, programa OPSEC operativo, segmentación de red implementada, PAM y MFA universal desplegados.

Fase 3 (Mes 4–8)

Plataforma CTI operativa (OpenCTI/MISP), feeds integrados al SIEM, reportes CTI mensuales.

Fase 4 (Mes 6–10)

Programa formal de Threat Hunting, stack de detección desplegado, 2 hunts/mes con reportes.

Fase 5 (Mes 5–12)

Cobertura hardening ≥90%, reportes de cumplimiento CIS/STIG, pentest externo.

Fase 6 (Transversal): DPIAs de tratamientos críticos, procesos ARCOP+ automatizados, plan de respuesta a brechas operativo.

Quick Wins en Primeros 90 Días

ACCIONES DE ALTO IMPACTO PARA CONSTRUIR MOMENTUM

1

Días 1–30

- MFA obligatorio en todas las cuentas administrativas
- EDR desplegado en servidores críticos
- Backup inmutable configurado y probado en sistemas Tier 1
- Inventario inicial de activos críticos completado
- Comité de Seguridad constituido formalmente

2

Días 31–60

- MFA universal extendido a todos los funcionarios
- PAM en producción para cuentas administrativas top
- Sysmon desplegado en servidores Windows
- Política General de Seguridad firmada
- ROPA inicial publicado

3

Días 61–90

- Primera campaña de phishing simulado ejecutada
- Hardening AD básico aplicado (LAPS, eliminación SMBv1)
- Primer hunt formal completado y documentado
- Procedimiento de incidentes activado y probado en tabletop
- DPO designado y operativo

Resultado: Postura de seguridad medible y visible en 90 días que sostiene la inversión de los siguientes 33 meses.

Estado Actual vs. Estado Objetivo — Mes 36

Dimensión	Estado Típico Actual	Estado Objetivo Mes 36
Madurez CMMI	Nivel 0-1 (ad hoc)	Nivel 4 (gestionado cuantitativamente)
Certificaciones	Ninguna	ISO 27001 + 27701 + 22301
MTTD	Días a semanas	<4 horas
Cobertura EDR	Antivirus básico parcial	XDR 100% endpoints
Threat Hunting	Inexistente	Programa formal, 2+ hunts/mes
CTI	Ninguna o feeds gratuitos	TIP operativa con análisis tres niveles
Protección Datos	Política genérica	ROPA vivo + DPIAs + ARCOP+ automatizado
Backup	Sin air-gap	Inmutable, probado, restauración medida
MFA	Parcial o inexistente	Universal con FIDO2 para admins
PAM	Sin gestión	PAM con sesiones grabadas
Hardening	Inconsistente	CIS L1/L2 + STIG verificado
Continuidad	Plan en papel	Probado trimestralmente con métricas
Cumplimiento ANCI	Reactivo	Proactivo con reporte integrado
Cumplimiento Ley 21.719	Insuficiente	Pleno con DPO operativo

Factores Críticos de Éxito

SIN ESTOS ELEMENTOS EL PLAN FRACASA

1

Patrocinio Ejecutivo Real

Máxima autoridad como sponsor activo, no figura decorativa. Participación visible en Comité de Seguridad.

2

Independencia del CISO y DPO

Reporte directo a Jefe de Servicio. Sin subordinación a TI. Recursos asegurados para el ejercicio efectivo.

3

Presupuesto Plurianual Comprometido

Acto administrativo que vincule los 36 meses. Cláusulas de continuidad ante cambios de autoridad.

4

Equipo con Perfil Adecuado

Contratación o capacitación con certificaciones reconocidas. Retención con planes de carrera definidos.

5

Métricas Públicas Internas

Dashboard mensual visible a alta dirección. Indicadores objetivos, no narrativos ni cualitativos.

6

Cultura de Aprendizaje Sin Sanción

Post-mortem sin culpabilización. Reporte de errores fomentado. Mejora continua real e institucionalizada.

7

Integración con Auditoría Interna

Coordinación con Contraloría Interna y, cuando aplique, con Contraloría General de la República.

8

Vinculación Interagencial

Participación activa en CSIRT de Gobierno, ANCI, mesas sectoriales y redes de compartición de inteligencia.

Siguiente Paso — Inicio Inmediato

PARA ACTIVAR EL PLAN

Decisión Ejecutiva Inmediata (Semana 1)

- Aprobación formal del Plan Director por máxima autoridad
- Asignación presupuestaria inicial para Fase 0
- Designación de CISO y DPO con dependencia directa
- Constitución formal del Comité de Seguridad

Arranque Operativo (Semanas 2–4)

- Contratación de GAP Assessment triple norma
- Activación de equipo de implementación
- Comunicación organizacional del Plan
- Identificación de quick wins prioritarios

Hitos Visibles (Mes 1–3)

- GAP Assessment entregado con scoring CMMI
- Política General de Seguridad firmada y publicada
- MFA universal activado
- EDR en servidores críticos
- Primer informe ejecutivo mensual

Compromiso TTPSEC SpA: Acompañamiento técnico end-to-end con metodología validada en sector público, energético, portuario, minero y banca a lo largo de Chile y LATAM. Equipo senior certificado en C|CISO, CCSK, CCZT, ISA/IEC 62443, ISO/IEC 42001, ISO 27001 LA/LI.

TTPSEC SpA — Contacto y Cierre

CONSULTORÍA ESPECIALIZADA EN CIBERSEGURIDAD PARA INFRAESTRUCTURA CRÍTICA Y SERVICIOS PÚBLICOS

Sebastián Vargas Yáñez

CEO & Founder — TTPSEC SpA

sebastian@ttpsec.com
www.ttpsec.com
Coquimbo, Chile | Operación LATAM

Especialización

- Ciberseguridad OT/ICS y TI integrada
- SGSI ISO 27001/27701/22301
- Cumplimiento Ley 21.663 y Ley 21.719
- Threat Intelligence y Threat Hunting
- Hardening sistemático y Zero Trust
- Continuidad operativa de servicios críticos

Modelo de Servicio

> Consultoría senior, sin junior shadowing. Entregables ejecutables, no PowerPoints de adorno. Compromiso con resultados medibles.

Certificaciones del Equipo

C|CISO
Certified Chief Information Security Officer

CCSK / CCZT
Cloud Security & Zero Trust

ISO 27001 LA/LI
Lead Auditor / Lead Implementer

ISA/IEC 62443
Ciberseguridad Industrial OT/ICS

Plan Director SGSI para Servicios Públicos | Versión 1.0 — 2026 | Confidencial