ILUSTRE MUNICIPALIDAD
COMUNA DE
LA LIGUA
ADQUISICIONES

DECRETO ALCALDICIO Nº 2585 /

LA LIGUA, 22 OCT 2026

MAT. Autoriza trato directo inferior a 30 UTM para contratación de servicios Microsoft Azure, respaldo de información.

VISTOS:

- La Ley Nº 18.695 "Orgánica Constitucional de Municipalidades" y sus Modificaciones.
- La Sentencia de Proclamación de fecha 30 de noviembre del 2024, del Tribunal Electoral de Valparaíso.
- La Resolución N°36, de 2024, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón, y su modificación introducida por la Resolución N°3, de 2026, del mismo origen.
- Ley Nº 19.886 y su Reglamento Vigente y sus Modificaciones.
- Decreto de Alcaldía N°10.121/2025, que aprueba subrogancia del Señor Alcalde.
- Decreto de Alcaldía N°1135/2024, que aprueba subrogancia Secretaria Municipal.
- Decreto de Alcaldía N°9753/2025, que aprueba Presupuesto Municipal año 2026.
- Solicitud de Compra de Bienes y Servicios N°0001509/2026, Depto. De Informática.
- Cotización N°4107/ de fecha 15 de agosto de 2026, de Deportes a tu Medida

CONSIDERANDO:

Que, el artículo 60 de la Ley N.º 19.886 regula el procedimiento de trato directo. A su vez, los artículos 71 N.º 6 y 76 del Decreto Supremo N.º 661/2024, del Ministerio de Hacienda, permiten recurrir al trato directo para contrataciones inferiores a 30 UTM que privilegien materias de alto impacto social, entre ellas el impulso a las Empresas de Menor Tamaño, debiendo fundamentarse el cumplimiento de dichos objetivos y que el precio responde a valores de mercado.

Que, mediante Memorándum N.º 60/2026, de fecha 20 de octubre de 2026, y Solicitud de Compra N.º 0001509, el Departamento de Informática solicita la contratación de servicios Microsoft Azure para el alojamiento de servidores virtuales, protección de aplicaciones, respaldo de información y continuidad operativa de los sistemas informáticos municipales, conforme a las especificaciones técnicas adjuntas.

Que, la Municipalidad de La Ligua ha sufrido un incidente de seguridad informática que afectó la continuidad operativa de sus sistemas institucionales, haciendo necesario fortalecer las medidas de seguridad, protección, respaldo y recuperación de información, con el objeto de resguardar el funcionamiento de los servicios municipales y la atención a la comunidad.

Que, la contratación se efectuará por un período de cuatro meses, atendida la necesidad de asegurar la continuidad de los servicios informáticos municipales y la disponibilidad presupuestaria correspondiente al ejercicio 2026.

Que, el proveedor RSCOMPUTACION SpA, RUT N.º 76.601.667-7, se encuentra hábil en el Registro de Proveedores y clasifica como Empresa de Menor Tamaño, según los antecedentes incorporados al expediente administrativo, contribuyendo esta contratación al objetivo de impulsar la participación de dichas empresas en las compras públicas.

ILUSTRE MUNICIPALIDAD
COMUNA DE
LA LIGUA

CONTINUACION DE DECRETO ALCALDICIO Nº 2585 /

Que, el monto referencial de la contratación asciende a US$371,72 mensuales, más IVA, equivalente a US$1.769,39 por los cuatro meses, IVA incluido, debiendo acreditarse que su equivalente en moneda nacional es inferior a 30 UTM y que el precio corresponde a valores de mercado.

DECRETO:

1° Autorícese el trato directo inferior a 30 UTM por materias de alto impacto social, conforme a los artículos 71 N.º 6 y 76 del Decreto Supremo N.º 661/2024, para contratar servicios Microsoft Azure destinados al alojamiento de servidores virtuales, seguridad informática, respaldo de información y continuidad operativa de los sistemas municipales, por un período de cuatro meses.

2° Apruébese la contratación con el proveedor **RSCOMPUTACION SpA, RUT N.º 76.601.667-7**, por un período de cuatro (4) meses, a un valor mensual de US$371,72 más IVA, equivalente a un monto total de US$1.769,39, IVA incluido. El pago se efectuará mensualmente, contra presentación de la respectiva factura emitida en pesos chilenos, conforme a la conversión del valor en dólares informada por el proveedor, previa recepción conforme del Departamento de Informática.

3° Contrátense los servicios Microsoft Azure para el alojamiento de dos servidores virtuales destinados al portal web municipal y sus subsitios, y un servidor virtual para sistemas informáticos internos, incluyendo los servicios de seguridad, conectividad, monitoreo, respaldo y recuperación establecidos en el anexo técnico elaborado por el Departamento de Informática, que formará parte integrante de la contratación.

4° El Departamento de Informática será responsable de supervisar la correcta prestación de los servicios contratados, verificar el cumplimiento de las especificaciones técnicas y emitir mensualmente la correspondiente recepción conforme, como requisito previo para la tramitación del pago de cada factura.

5° Publíquense el presente decreto en el Sistema de Información dentro del plazo de 24 horas establecido en el artículo 77 del Decreto Supremo N°661/2024.

Anótese, Comuníquese y Archívese

ILUSTRE MUNICIPALIDAD DE LA LIGUA
SECRETARIA MUNICIPAL(S)
María Alejandra Alvarez Moraga
SECRETARIA(O) MUNICIPAL

I. MUNICIPALIDAD DE LA LIGUA
ALCALDE
PATRICIO PALLARES V.
Patricio Pallares Valenzuela
ALCALDE

RECIBIDO
12:04
22 OCT 2026
SECRETARIA MUNICIPAL
A.M. P.M.

DISTRIBUCIÓN:
- **ADQUISICIONES (prioritario)**
- **ARCHIVO**

PPV/FMO/RIA/lfv

RECIBIDO
28 OCT 2026
A.M. P.M.
16:30

RECIBIDO
11:10
21 OCT 2026
ALCALDIA
A.M. PM.

EXAMINADO
21 OCT 2026
CONTRALORIA
LALIGUA

MUNICIPALIDAD
CONTRALOR
MUNICIPAL
LA LIGUA

ILUSTRE MUNICIPALIDAD
COMUNA DE
LALIGUA

LA LIGUA:.....

N° 0001509

SOLICITUD DE COMPRA DE BIENES Y SERVICIOS

1.IDENTIFICACIÓN DE LA SOLICITUD

Unidad solicitante:...Departamento de Informatica.....

Funcionario Responsable:...Luis Emilio Osorio Pereira..... Tipo: ☐ Bien ☒ Servicio

2.RESPALDO PRESUPUESTARIO

Código presupuestario:.....

Fuente de financiamiento: ☐ Municipal ☐ Programa ☐ Convenio

Nombre del programa: .....

N° Decreto aprueba programa..... fecha decreto...../

Disponibilidad presupuestaria: ☐Sí ☐NO

3.JUSTIFICACIÓN TÉCNICA O DETALLE DE LA COMPRA (Indicar finalidad, necesidad del gasto y vinculación con función municipal)

Contratacion De Servicio De Nube Microsoft Azure Para Alojar Servidores Web y Sistemas Internos Informaticos Referentes A La Seguridad Tras Incidente De Ciberseguridad

4. TIPO DE COMPRA

Tipo ☐Convenio Marco / ☐Licitación Pública / ☐Compra Ágil / ☐Trato Directo / ☐Menor a 3 UTM

5. DETALLE DE LA COMPRA

Cantidad	DETALLE	P. Unitario	Total
1	Suscripcion Mensual Microsoft Azure	US: 371,72	US: 371,72
	(Pago Por Uso Referencial)		
		IVA	US: 70,668
		TOTAL	US: 442,388

La presente solicitud se formula en conformidad a la Ley N° 19.886 y el Decreto N° 661/2024.

ILUSTRE MUNICIPALIDAD DE LA LIGUA
INFORMATICA

FIRMA SOLICITANTE

V° B° ALCALDE Y/O ADMINISTRADOR

>>05007

RSCOMPUTACION SPA

Actividades de consultoria de informatica y gestion de instalaciones
Dr. Manuel Barros Borgono 71 Of 1105 , PROVIDENCIA
Teléfono: 56988542978
Email: contacto@rscomputacion.com

R.U.T: 76601667-7

Cotización

Folio N° 4107

Señor (es)	Ciudad	Giro	R.U.T
I MUNICIPALIDAD DE LA LIGUA	LA LIGUA	ADMINISTRACION PUBLICA Y DEFENSA	69.050.100-7
Dirección	**Condición de pago**	**Vendedor**	**Tipo de Cambio**
DIEGO PORTALES 555	CREDITO 30 DIAS	Yamilet Samaca ysamaca@rscomputacion.com	USD
Comuna	**Fecha Documento**	**Fecha de Vencimiento**	**Tasa de Cambio**
VALPARAISO	16-10-2026	31-10-2026	1

Item	Código	Detalle	Cant	P. Unitario	Rec/Desc	Total
1	RSCL000031	Azure Subscription with Billing Type Monthly	1 CS	US$ 371.72	US$ 0.00	US$ 371.72

Comentario: SUSCRIPCION MENSUAL - CONSUMO PAGO POR USO
CONSIDERAR QUE ES UNA ESTIMACIÓN, EL MONTO A PAGAR ES
VARIABLE DE ACUERDO A CONSUMO MENSUAL

Comentario

- TRANSFERENCIA AL DÍA, DOCUMENTO 0, 30 (PREVIA EVALUACIÓN CREDITICIA).
- PLAZO DE ENTREGA EN SOFTWARE 02 DÍAS HÁBILES UNA VEZ RECIBIDA LA ORDEN DE COMPRA
- TIPO DE CAMBIO: DÓLAR AMERICANO OBSERVADO + $ 5 AL DÍA DE FACTURACIÓN.

Recargo/Dscto.	US$ 0.00
Afecto	US$ 371.72
Exento	US$ 0.00
19% IVA	US$ 70.64

COMUNA DE LA LIGUA | **INFORMATICA**

MEMORANDUM N°60 /2026-

DE:	LUIS EMILIO OSORIO PEREIRA, ENCARGADO DE INFORMATICA
A:	SR. FELIPE MORALES OSSIO, ADMINISTRADOR MUNICIPAL ILUSTRE MUNICIPALIDAD DE LA LIGUA.
MAT:	SOLICITA CONTRATACIÓN DE SERVICIOS MICROSOFT AZURE PARA ALOJAMIENTO DE SERVIDORES Y CONTINUIDAD OPERATIVA MUNICIPAL.
FECHA:	MARTES 20 OCTUBRE DEL 2026.

Solicitud
Solicito autorizar el inicio de las gestiones técnicas, presupuestarias y administrativas para contratar servicios Microsoft Azure, su implementación segura y su operación, destinados a alojar dos máquinas virtuales para el portal web municipal, sus servicios y subsitios, y una máquina virtual para los sistemas municipales utilizados por funcionarios internos. La contratación deberá incorporar las protecciones y servicios complementarios descritos en el anexo técnico, y no limitarse al arriendo de capacidad de cómputo.

Fundamento
La Municipalidad informó haber sufrido un ataque cibernético. Este antecedente hace necesario reforzar la continuidad de sus servicios digitales, reducir su exposición y disponer de mecanismos verificables de detección y recuperación. No se cuenta en este documento con evidencia forense que permita afirmar la causa, el alcance, la existencia de filtración o la integridad de los respaldos; dichas materias deberán determinarse mediante la investigación correspondiente.

Se propone una arquitectura con separación entre servicios públicos e internos, protección de aplicaciones web, acceso administrativo restringido, gestión de identidades, detección de amenazas, respaldos protegidos y monitoreo. Azure aporta capacidades de plataforma, pero la seguridad de los sistemas operativos, las aplicaciones, los datos y los accesos requiere configuración y gestión permanente por parte de la Municipalidad y del proveedor contratado [1].

Decisión requerida
Se solicita disponer el levantamiento técnico y la cotización desglosada, designar una contraparte municipal y tramitar la disponibilidad presupuestaria. La adjudicación y el inicio del servicio quedarán sujetos al procedimiento de compra que corresponda, a la revisión jurídica y a la aprobación de costos y condiciones. Se propone evaluar un período inicial de 12 meses, sujeto a confirmación administrativa. El anexo forma parte de los requisitos técnicos de esta solicitud.



LUIS EMILIO OSORIO PEREIRA

Departamento De Informatica
Ilustre Municipalidad de La Ligua

DISTRIBUCIÓN:

- Adquisiciones.
- Archivo Informática.

Anexo técnico y condiciones del servicio

1 Alcance y antecedentes que deben verificarse

El alcance base comprende tres máquinas virtuales productivas y los servicios de red, seguridad, respaldo, observabilidad y soporte necesarios para su funcionamiento. Las dos máquinas web deberán operar como nodos redundantes cuando las aplicaciones lo permitan. Si alojan servicios diferentes sin duplicación, no existirá alta disponibilidad para cada servicio y el proveedor deberá indicarlo expresamente.

Antes de definir tamaños o migrar, se deberá inventariar cada dominio, subdominio, subsitio, API, certificado, integración, tarea programada, base de datos y repositorio de archivos. El inventario incluirá propietario funcional, criticidad, clasificación de información, dependencias, sistema operativo, versiones y soporte del fabricante. Se deberán identificar servicios externos, correo transaccional, autenticación y eventuales conexiones con Power Apps o Power Automate, solo si existen.

El levantamiento deberá medir CPU, memoria, almacenamiento, IOPS, latencia, conexiones y tráfico, incluyendo períodos de mayor demanda. Se exigirá validar licencias, compatibilidad con virtualización, derechos de traslado y necesidad de acceso a proveedores de sistemas municipales. No se dispone de estos datos, por lo que las capacidades de este anexo son referencias de cotización y no un dimensionamiento definitivo.

2 Objetivos y límites

Los objetivos son restablecer o fortalecer la prestación digital municipal en un entorno controlado; impedir el acceso directo a servidores de origen; reducir el movimiento lateral; detectar acciones sospechosas; y recuperar aplicaciones y datos mediante procedimientos probados. Ninguna arquitectura elimina por completo el riesgo de ataque y ninguna migración sustituye la investigación del incidente o la corrección de vulnerabilidades del software.

El servidor interno único constituye un punto único de falla. Sus respaldos y un procedimiento de recuperación reducen el impacto, pero no equivalen a continuidad sin interrupciones. Una segunda instancia interna, redundancia de base de datos o recuperación regional se cotizarán como ampliaciones separadas si la evaluación de impacto las exige.

3 Entregables de diseño

El proveedor deberá entregar diagramas de red y de flujos, inventario de recursos y costos, matriz de puertos y permisos, análisis de dependencias, políticas de identidad y respaldo, plan de migración y reversa, y matriz de riesgos. Se deberán documentar región, zonas disponibles, ubicación de datos y respaldos, servicios con procesamiento global y restricciones regulatorias o contractuales. No se presumirá que todos los servicios están disponibles en una región específica.

Arquitectura de infraestructura y conectividad

4 Arquitectura base propuesta

Para el frente público se propone Azure Application Gateway WAF_v2 como entrada HTTPS, con reglas por nombre de host y rutas hacia WEB01 y WEB02, alojadas en subredes privadas. El balanceador solo deberá utilizar nodos saludables. Application Gateway permite distribuir tráfico de aplicaciones y su WAF proporciona una capa de inspección de solicitudes web [2][3].

Flujo público: Internet → DNS municipal → Application Gateway WAF_v2 → WEB01 y WEB02 por direcciones privadas → servicios de datos autorizados. Los servidores web no tendrán direcciones IP públicas. Se mantendrá cifrado HTTPS desde el cliente hasta el servidor de origen, validando certificados y nombres de host.

Flujo interno: red municipal → VPN de sitio a sitio → segmento privado de aplicaciones → INT01. El acceso remoto de funcionarios, si se requiere, deberá utilizar una solución autenticada con MFA y permisos por perfil. No se publicarán directamente en Internet los sistemas internos. La autenticación de cada aplicación deberá validarse; la VPN no reemplaza sus controles de acceso.

Flujo de administración: estación autorizada → identidad administrativa con MFA → Azure Bastion o canal privado aprobado → servidor. Se prohíbe exponer RDP, SSH o consolas de administración a Internet. Los puertos de base de datos quedarán accesibles exclusivamente desde las aplicaciones autorizadas.

5 Separación y protección de red

Se implementarán segmentos diferenciados para entrada web, servidores públicos, aplicaciones internas, administración y servicios compartidos. Las reglas NSG y los cortafuegos del sistema operativo permitirán únicamente los flujos documentados. Se denegará la comunicación entre el segmento público y el interno salvo dependencias aprobadas. El egreso se controlará mediante Azure Firewall o una solución equivalente justificada, incorporando su costo, trazabilidad y listas de destinos necesarios.

La VPN se cotizará con las condiciones del equipo municipal, direccionamiento sin superposición, resolución DNS y rutas necesarias. La redundancia del gateway, del equipo local y de los enlaces deberá evaluarse conjuntamente; una VPN en la nube no elimina la dependencia del acceso a Internet de la Municipalidad.

6 Alternativas que requieren evaluación económica

Azure Front Door Premium con WAF y conectividad privada al origen podrá cotizarse como alternativa para necesidades de distribución global o una arquitectura de entrada distinta. Private Link depende de orígenes y regiones compatibles [4]. No se exigirá simultáneamente Front Door y Application Gateway sin un beneficio técnico documentado. La protección DDoS adicional para IP públicas se evaluará según la topología elegida, exposición y costo; un WAF y un servicio DDoS cubren amenazas diferentes.

Servidores y disponibilidad de las aplicaciones

7 Capacidades iniciales para comparar ofertas

Recurso	Referencia por instancia	Condición de validación
WEB01 y WEB02	2 VM; cada una con 4 vCPU, 16 GiB RAM; disco SO 128 GiB; datos 256 GiB SSD administrado.	Confirmar consumo, IOPS y espacio; cada nodo deberá soportar la carga de contingencia definida.
INT01	1 VM con 8 vCPU, 32 GiB RAM; disco SO 128 GiB; datos 512 GiB SSD administrado.	Confirmar usuarios concurrentes, aplicaciones y requisitos del fabricante.
Bases de datos y archivos	Capacidad y modalidad por determinar.	Cotizar por separado motor, licencias, almacenamiento compartido y protección cuando correspondan.

Estas cifras son supuestos de trabajo para obtener una cotización comparable, no capacidades acreditadas. El proveedor deberá proponer SKU y discos equivalentes o superiores según mediciones, justificar cualquier variación y detallar el costo incremental. Se evitarán compromisos de reserva antes de validar la carga y estabilizar el consumo.

8 Diseño de las dos máquinas web

Cuando la región y el servicio lo permitan, WEB01 y WEB02 se distribuirán en zonas distintas. La disponibilidad exige que ambos nodos puedan servir los mismos dominios, aplicaciones y contenidos. Se deberá resolver la sincronización de despliegues, sesiones, archivos cargados y configuraciones. Los discos locales no constituyen almacenamiento compartido; el proveedor deberá cotizar un repositorio apropiado o un mecanismo consistente y probado.

Las comprobaciones de salud evaluarán una ruta representativa y no solo la respuesta del puerto. Se deberá probar la retirada de un nodo, la atención del tráfico con el restante y el retorno controlado. Se validarán cargas de archivos, inicio de sesión, formularios, tareas programadas y operaciones que no deben ejecutarse duplicadas. Los límites de tamaño de solicitudes y tiempos de espera del WAF se ajustarán a las necesidades municipales.

9 Sistemas operativos y datos

Se instalarán versiones con soporte vigente y configuración reforzada conforme a guías del fabricante y una línea base documentada. Se deshabilitarán servicios innecesarios y autenticación obsoleta, se activarán registros de auditoría y cifrado de discos, y se

separarán cuentas de servicio de las administrativas. Secure Boot y vTPM se habilitarán cuando sean compatibles con la generación y el sistema seleccionados.

La base de datos se ubicará en un servicio administrado o en una instancia privada según compatibilidad. El diseño de tres VM no presupone que todas las bases de datos puedan alojarse en INT01: si se requiere otro recurso, debe identificarse y cotizarse. La disponibilidad del portal dependerá también de la base de datos, DNS, archivos y autenticación; la redundancia del cómputo por sí sola no asegura la disponibilidad integral.

Controles de seguridad y gestión de accesos

10 Identidades y privilegios

La suscripción y los recursos deberán estar bajo control de la Municipalidad, con acceso a facturación, inventario y registros. El proveedor recibirá permisos delegados y revocables. Se utilizarán cuentas nominativas, MFA para accesos administrativos, roles de mínimo privilegio y separación entre administración, auditoría y gestión de respaldos. Se evitarán cuentas compartidas y asignaciones permanentes de propietario.

Se evaluará Microsoft Entra Conditional Access y Privileged Identity Management según licenciamiento, cotizando explícitamente sus requisitos. Se mantendrán cuentas de emergencia protegidas, monitoreadas y probadas. Las aplicaciones usarán identidades administradas cuando sean compatibles; secretos y certificados se almacenarán en Azure Key Vault o un repositorio seguro equivalente, con rotación y acceso auditado.

11 Protección web y de servidores

El WAF se configurará con reglas administradas vigentes compatibles y controles específicos para los dominios municipales. Se ajustará primero con tráfico representativo y posteriormente se habilitará el modo de prevención antes de la aceptación productiva. Toda exclusión deberá tener justificación, alcance mínimo, responsable y revisión. El WAF reduce ataques comunes, pero no corrige código vulnerable ni reemplaza autenticación, validación de datos o pruebas de aplicaciones [3].

Las tres VM deberán contar con protección de endpoint y capacidad EDR, por ejemplo mediante Microsoft Defender for Servers con el plan que cumpla las funciones ofertadas. Se exigirá verificar incorporación, comunicación de agentes, recepción de alertas y procedimiento de investigación [5]. Se gestionarán vulnerabilidades de sistemas operativos, motores web, extensiones, bibliotecas y CMS; la oferta identificará expresamente quién corrige cada capa.

Se propone evaluar vulnerabilidades críticas explotadas activamente en un máximo de 24 horas desde su detección y aplicar mitigación o corrección en 72 horas, sujeto a pruebas y compatibilidad. Las excepciones deberán documentar riesgo, control compensatorio y fecha de resolución. Estos son objetivos contractuales propuestos, no plazos normativos ni garantías del fabricante.

12 Configuración y cambios

Se aplicarán políticas para restringir regiones aprobadas, impedir exposición pública no autorizada, exigir etiquetado y auditar configuraciones. Se conservará la infraestructura como código o un mecanismo reproducible equivalente, con control de versiones y sin secretos en los archivos. Los cambios productivos requerirán respaldo, validación, ventana autorizada y procedimiento de reversa. El entorno temporal de pruebas o migración deberá cotizarse y retirarse de forma controlada al finalizar.

Respaldo y recuperación ante incidentes

13 Política de protección de datos

Se contratará Azure Backup o una solución compatible con la carga, incluyendo las tres VM y la protección consistente de bases de datos y archivos. La oferta describirá frecuencia, retención, crecimiento y costos de restauración. Como referencia inicial se propone respaldo diario de VM con 30 puntos diarios y 12 puntos mensuales, sujeto a clasificación de información y capacidad presupuestaria. La periodicidad efectiva se validará mediante la política concreta del servicio.

Se exigirán controles de inmutabilidad, borrado reversible y autorización separada para operaciones sensibles donde el tipo de bóveda y la carga los soporten. Azure Backup dispone de estas capacidades, cuya habilitación y alcance deben acreditarse [6]. El bloqueo irreversible de inmutabilidad se aplicará tras validar retenciones, restauración y autorización municipal. Los respaldos no deberán quedar bajo el control exclusivo de las credenciales que administran producción.

Se definirá redundancia del almacenamiento de respaldo y viabilidad de recuperación ante indisponibilidad regional. La replicación entre regiones y Azure Site Recovery, si se requieren, se cotizarán por separado; replicar datos no reemplaza conservar versiones protegidas. Se realizará restauración de muestra antes de la puesta en marcha y pruebas trimestrales posteriores en un entorno aislado.

14 Objetivos de recuperación propuestos

Servicio	RPO propuesto	RTO propuesto
Portal y subsitios	Hasta 24 horas para contenido; transacciones a definir.	Hasta 8 horas.
Sistemas internos	Hasta 4 horas para datos transaccionales.	Hasta 8 horas.

RPO es la pérdida máxima de datos tolerable medida en tiempo; RTO es el tiempo objetivo para recuperar el servicio. Son metas preliminares para evaluación municipal y prueba contractual. Un respaldo diario no satisface un RPO de cuatro horas: los sistemas internos requerirán copias o registros transaccionales con frecuencia suficiente y soporte del motor. Ninguna meta se considerará cumplida sin una restauración integral medida y documentada.

15 Respuesta a incidentes y evidencia

El procedimiento deberá establecer detección, clasificación, contención, preservación de evidencia, erradicación, recuperación y revisión posterior. Se definirán responsables, canal de escalamiento y comunicación institucional. Las acciones automáticas de aislamiento deberán considerar el impacto en la operación y la preservación de evidencia. Los registros y artefactos relevantes se custodiarán con

trazabilidad, integridad y acceso restringido; su retención se acordará con las unidades responsables.

Monitoreo y operación del servicio

16 Registro y alertas

Se centralizarán registros de actividad de Azure, accesos administrativos, WAF, sistemas operativos, aplicaciones, autenticación y respaldos, según compatibilidad y licencias. Azure Monitor y Log Analytics podrán utilizarse para esta función. Microsoft Sentinel se cotizará cuando se requiera correlación SIEM y automatización de respuesta; contratar una herramienta no equivale a contar con un equipo que atienda sus alertas.

Se propone mantener 90 días de consulta operativa y 12 meses de conservación de registros de seguridad seleccionados, sujetos a finalidad, privacidad y aprobación municipal. La oferta separará ingestión, consulta, archivo, recuperación y transferencia. Se deberán evitar secretos o datos personales innecesarios en los registros y probar las alertas con eventos controlados.

El monitoreo comprenderá disponibilidad HTTPS por dominio crítico, respuesta de la aplicación, CPU, RAM, disco, certificados próximos a vencer, intentos de acceso anómalos, estado de EDR y fallas de respaldo. Se exigirá una prueba externa de disponibilidad y un reporte mensual de incidentes, cambios, capacidad, vulnerabilidades, restauraciones y consumo.

17 Soporte y atención

Prioridad	Ejemplo	Objetivo inicial de atención
Crítica	Caída de servicio crítico o compromiso activo confirmado.	Recepción 24 × 7 y respuesta humana en 30 minutos.
Alta	Degradación importante o pérdida de redundancia.	Respuesta en 2 horas.
Normal	Consulta, ajuste o incidente de bajo impacto.	Respuesta en 1 día hábil.

Estos tiempos son requisitos propuestos para la contratación y deben acordarse expresamente. Respuesta significa inicio de atención y no resolución garantizada. Se deberá definir cobertura por prioridad, escalamiento, reportes de avance, tiempos de mitigación y exclusiones. El soporte de Microsoft, el soporte del proveedor de infraestructura y el de los fabricantes de aplicaciones se identificarán como servicios diferenciados.

18 Responsabilidades

La Municipalidad aprobará accesos, criticidad, tratamiento de datos, cambios y aceptación, y designará responsables funcionales. El proveedor implementará y operará los componentes contratados, conservará documentación actualizada y demostrará controles. Los proveedores de aplicaciones validarán compatibilidad y corregirán su

software conforme al contrato. Se exigirá una matriz de responsabilidades que evite vacíos en parches, certificados, DNS, licencias, bases de datos, restauraciones y notificación de incidentes.

Migración segura y aceptación técnica

19 Plan de ejecución

Fase 1 — Evaluación: levantar inventario, dependencia y estado de seguridad; determinar las aplicaciones recuperables y validar respaldos con la investigación del incidente. Preservar evidencia antes de intervenir equipos afectados. No trasladar imágenes completas comprometidas sin una evaluación y autorización técnica documentada.

Fase 2 — Construcción: desplegar la red y las identidades desde configuraciones controladas, crear VM desde imágenes confiables, aplicar actualizaciones y activar monitoreo, EDR y respaldos. Rotar credenciales, claves de servicio y certificados potencialmente expuestos. Validar también la confianza de directorios, equipos administradores e integraciones de origen.

Fase 3 — Recuperación y pruebas: restaurar únicamente datos y componentes verificados, examinar malware y vulnerabilidades, validar consistencia de bases de datos y ejecutar pruebas funcionales con usuarios responsables. La ausencia de alertas no constituye por sí sola una certificación de limpieza.

Fase 4 — Cambio productivo: efectuar copia final consistente, sincronizar datos, ejecutar la ventana autorizada y modificar DNS. El plan deberá definir reducción previa de TTL, tratamiento de sesiones y escrituras, responsables y criterios de reversa. La reversa no deberá reintroducir un entorno comprometido ni perder transacciones sin reconciliación.

Fase 5 — Estabilización: mantener seguimiento reforzado, corregir hallazgos, verificar facturación y entregar documentación y capacitación. Cada fase tendrá hitos, plazos y responsables en la oferta; la duración final dependerá del inventario y de la recuperación del incidente.

20 Criterios mínimos de aceptación

La recepción requerirá evidencia de que: a) todos los dominios y sistemas inventariados superan sus pruebas funcionales; b) no existen IP públicas ni puertos administrativos expuestos en las VM; c) la segmentación bloquea accesos no autorizados; d) MFA, permisos y cuentas de emergencia funcionan; e) WAF y EDR detectan eventos de prueba; f) los registros y alertas llegan al equipo responsable; g) se restaura una aplicación con sus datos y se miden RPO y RTO; h) se retira un nodo web y se verifica la continuidad prevista; i) se prueba la conectividad privada de los funcionarios; y j) se entrega control municipal de los recursos.

No deberán quedar vulnerabilidades críticas sin resolver ni riesgos altos sin aceptación expresa del responsable municipal. El informe de pruebas incluirá fecha, ejecutor, resultados, evidencias y acciones pendientes. El acta de recepción distinguirá disponibilidad del proveedor de nube, disponibilidad real de las aplicaciones y objetivos de recuperación, evitando atribuir un SLA de extremo a extremo sin medición ni compromiso contractual.

Presupuesto y condiciones administrativas

21 Desglose económico exigido

La oferta deberá presentar costo inicial de evaluación, implementación, migración y capacitación; costo mensual recurrente; y total para el período de contratación. Se separarán cómputo de las tres VM, licencias de sistema operativo y motores, discos y operaciones, WAF y gateway, IP y DNS, VPN, administración segura, control de egreso, protección de servidores, identidad, respaldo, registros, transferencias y soporte. Las alternativas de continuidad regional y herramientas SIEM se individualizarán.

El cálculo deberá indicar región, SKU, horas mensuales utilizadas —por ejemplo, 730 como supuesto de estimación—, moneda, tipo de cambio, impuestos aplicables, tráfico saliente, volumen de logs y datos protegidos. Se adjuntará una estimación reproducible y sus supuestos. El total anual corresponderá al costo inicial más doce meses recurrentes, más los consumos variables estimados. No se fija un monto en este documento porque no existe una cotización ni medición de carga.

Se configurarán presupuestos y avisos de consumo, por ejemplo al 50 %, 80 % y 100 % del presupuesto aprobado. Estas alertas no constituyen un límite duro de gasto. Se acordarán umbrales de autorización para ampliar recursos y medidas de contención que no provoquen la detención automática de servicios esenciales.

22 Condiciones contractuales y salida

La Municipalidad deberá conservar titularidad y control de datos, dominios, configuración y suscripción o, cuando el modelo comercial exija otra modalidad, derechos contractuales equivalentes de administración, exportación y continuidad. Se exigirán confidencialidad, control de subcontratistas, acceso restringido, registro de acciones y notificación oportuna al municipio ante incidentes, con un plazo contractual definido.

El proveedor entregará al término de la contratación inventario, documentación, configuraciones, respaldos exportables y asistencia para la transferencia. Se definirán formatos, plazos, costos de egreso y validación de recuperación antes de eliminar recursos. Las credenciales delegadas deberán revocarse y la eliminación de datos se acreditará conforme a retenciones y obligaciones aplicables.

23 Marco normativo y validación jurídica

La Ley N° 21.663 contempla a las municipalidades dentro de la Administración del Estado para sus efectos [7]. La unidad jurídica deberá determinar las obligaciones de gestión y reporte aplicables, las instrucciones vigentes de la autoridad y los canales correspondientes. Este anexo no presume una calificación específica como operador de importancia vital ni reemplaza el análisis jurídico del incidente.

Se deberá revisar el tratamiento de datos personales conforme al régimen vigente y considerar la transición de la Ley N° 21.719, cuya regla de entrada en vigor se encuentra en sus disposiciones transitorias [8]. La ubicación, transferencias, accesos y conservación de información se aprobarán según esa evaluación. La justificación de

Azure es técnica; cualquier exigencia de marca, modalidad de adquisición o causal excepcional requerirá fundamento jurídico y administrativo propio.

Riesgos residuales y referencias

24 Riesgos que deben quedar documentados

Riesgo	Tratamiento y límite
Reintroducir el compromiso original	Reconstrucción confiable, investigación y rotación de secretos. Migrar no elimina la causa.
Falla del servidor interno	Restauración probada; cotizar redundancia si el RTO resulta insuficiente.
Falla de base de datos o archivos	Diseñar protección y disponibilidad propias; dos nodos web no cubren estas dependencias.
Interrupción de Internet municipal	Evaluar enlaces y equipos redundantes; probar el acceso de contingencia.
Credenciales privilegiadas comprometidas	MFA, roles mínimos, separación de respaldos y supervisión de acciones.
Costos superiores a lo previsto	Medición, desglose, alertas y revisión mensual de consumo.
Software antiguo o sin soporte	Plan de actualización con fabricante; no aceptar exposición sin mitigación documentada.

25 Referencias oficiales

Documentación consultada el 16 de octubre de 2026. Los números entre corchetes vinculan el fundamento técnico o normativo con las fuentes siguientes. Los dimensionamientos, metas y condiciones contractuales son propuestas de este documento y no especificaciones ni compromisos de Microsoft.

[1] Microsoft Learn — Responsabilidad compartida en la nube
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility/

[2] Microsoft Learn — Azure Application Gateway
https://learn.microsoft.com/en-us/azure/application-gateway/overview

[3] Microsoft Learn — WAF en Application Gateway
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

[4] Microsoft Learn — Private Link en Azure Front Door Premium
https://learn.microsoft.com/en-us/azure/frontdoor/private-link

[5] Microsoft Learn — Defender for Servers
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-overview

[6] Microsoft Learn — Buenas prácticas de protección con Azure Backup
https://learn.microsoft.com/azure/backup/azure-backup-data-protection-best-practices

[7] Biblioteca del Congreso Nacional — Ley N° 21.663
https://www.bcn.cl/leychile/Navegar?idNorma=1202434

[8] Biblioteca del Congreso Nacional — Ley N° 21.719
https://www.bcn.cl/leychile/navegar?i=1209272

Ficha del proveedor

HÁBIL

RAZÓN SOCIAL
RSCOMPUTACION SPA
RUT 76.601.667-7

Nombre de fantasía	Rscomputacion
Estado de habilidad	HÁBIL (Cumple con los requisitos de inscripción en el Registro de Proveedores)
Estado de acreditación	Proveedor acreditado hasta 18-08-2027
Domicilio legal	DR M BARROS BORGONO 71 OF 1105 11P, PROVIDENCIA, REGION METROPOLITANA
Empresa de Menor Tamaño (EMT)	**Si** clasifica como Empresa de Menor Tamaño según información del Servicio de Impuestos Internos.

Revisa mas información sobre Empresa de Menor Tamaño (EMT)

Información general | Habilidad | Idoneidad | Documentos | Comportamiento

Administración de la empresa

Fuente: Declaración Jurada del Registro de Proveedores registrada por el proveedor en Mercado Público

Administrador	JOSÉ MIGUEL NAVARRETE NÚÑEZ
Administrador	JORGE ANDRE GUAJARDO MEDINA

Usuarios de la empresa