

# Resumen ejecutivo

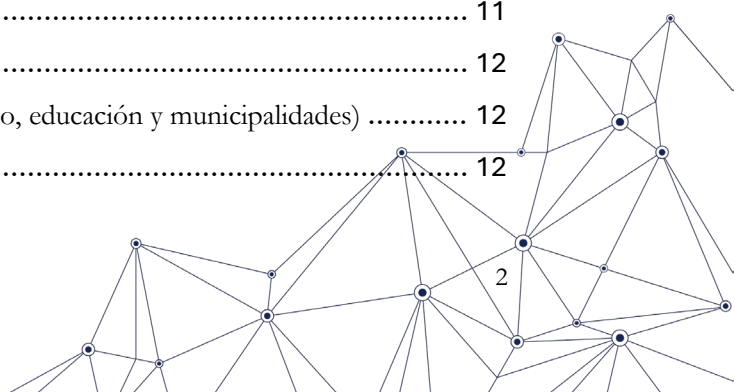
Consulta Pública del Proceso de  
Calificación de Operadores de  
Importancia Vital (OIV)



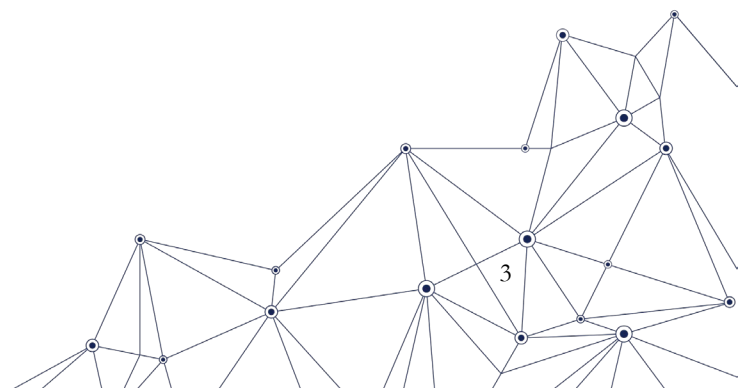
**ANCI**  
AGENCIA NACIONAL  
DE CIBERSEGURIDAD

## Contenidos

<b>Introducción</b> .....	4
<b>Metodología</b> .....	5
<b>Estadísticas generales</b> .....	6
Metodología y participación .....	6
<b>Observaciones recibidas en la Consulta Pública sobre Precalificados</b> .....	8
1. Conformidad con la calificación OIV y fundamentación de la criticidad.....	8
1.1 Proveedores municipales de plataformas críticas.....	8
1.2. Instituciones financieras y bancarias.....	8
1.3. Telecomunicaciones e infraestructura TI .....	8
1.4. Otros servicios críticos y actores relevantes.....	8
2. Oposición o cuestionamiento a la calificación OIV.....	9
2.1. Servicios con baja dependencia informática.....	9
2.2. Empresas pequeñas o de baja relevancia sectorial.....	9
2.3. Rol de terceros y revendedores .....	9
2.4. Proveedores específicos objetados.....	10
3. Preguntas y observaciones sobre criterios, alcance e implementación.....	10
3.1. Proporcionalidad y costos .....	10
3.2. Criterios de inclusión sectorial .....	10
3.3. Coordinación regulatoria interinstitucional.....	10
<b>Observaciones recibidas en la Consulta Pública sobre No-Precalificados</b> .....	11
1. Proveedores de Infraestructura Digital y Plataformas Transversales .....	11
1.1 Infraestructura digital y hosting .....	11
1.2 Conectividad troncal y telecomunicaciones .....	11
1.3 Servicios de ciberseguridad gestionados (SOC/NOC) .....	11
2. Medios de pago, software financiero y seguridad social .....	11
2.1 Medios de pago y transacciones .....	11
2.2 Software financiero y Fintech .....	11
2.3 Seguridad social y previsional .....	12
3. Servicios de soporte crítico al sector público (Gobierno, educación y municipalidades) .....	12
3.1 Sistemas de gestión municipal.....	12



3.2 Educación superior y datos .....	12
3.3 Soporte de software y plataformas.....	12
4. Infraestructura crítica de servicios básicos y logística .....	12
5. Proveedores críticos del sector salud.....	12
5.1 Ficha clínica electrónica y sistemas hospitalarios .....	13
5.2 Centros de salud y hospitales específicos .....	13
6. Comentarios misceláneos y otros proveedores.....	13
6.1 Proveedores de insumos críticos .....	13
6.2 Organizaciones de la sociedad civil y educación inicial .....	13
<b>Conclusiones</b> .....	<b>14</b>



## Introducción

En Chile, la creación de la Agencia Nacional de Ciberseguridad (ANCI) es parte de una agenda pública de institucionalización de la ciberseguridad como prioridad estratégica de Estado. El 01 de enero de 2025, la ANCI entró en funcionamiento como un organismo técnico que tiene por misión regular, supervisar y coordinar la acción del país en materias de ciberseguridad.

El presente documento sintetiza los resultados de la consulta pública realizada por la ANCI en función del procedimiento para la calificación de los Operadores de Importancia Vital (OIV). Este proceso responde directamente a las atribuciones conferidas a la ANCI por la Ley N°21.663, marco de ciberseguridad, que define la necesidad de identificar y regular a aquellas entidades públicas o privadas cuya interrupción o vulneración puede tener efectos significativos sobre la seguridad nacional, la continuidad de los servicios esenciales o el bienestar de la población. El procedimiento de calificación, además, está regulado en el Decreto Supremo N°285, de 6 de septiembre de 2024, del Ministerio del Interior y Seguridad Pública, que aprueba el Reglamento del Procedimiento de Calificación de los Operadores de Importancia Vital de la Ley N°21.663 (Reglamento).

De conformidad con la Resolución Exenta N°24 del 2025 de la ANCI la primera fase del procedimiento abordó los sectores de generación, transmisión y distribución eléctrica; telecomunicaciones; infraestructura digital, servicios digitales y servicios de tecnología de la información gestionados por terceros; servicios bancarios, financieros y medios de pago; prestación institucional de servicios de salud; empresas públicas; y, organismos de la Administración del Estado. Se revisó un universo estimado en torno a sesenta mil instituciones y se definió preliminarmente a 1.712 entidades como posibles OIV,

La consulta pública, que se extendió por 30 días, abrió un espacio de participación ciudadana, con la finalidad de recoger, ordenar y examinar las observaciones formuladas por personas naturales y jurídicas respecto de la nómina preliminar de OIV publicada por la ANCI en su primer procedimiento de calificación. Se trata de un hito relevante para la consolidación de la gobernanza en ciberseguridad, pues abre un espacio formal donde distintos actores pueden expresar sus comentarios, reparos y propuestas frente a la definición de qué entidades son críticas para la seguridad digital del país.

Este resumen ejecutivo, además de dar cumplimiento al artículo 15° del Reglamento, permite a la ANCI pronunciarse sobre las observaciones planteadas por la ciudadanía relacionadas directamente con el proceso de calificación en curso.<sup>1</sup>

---

<sup>1</sup> Aprobado mediante Decreto N°[285](#) de 2024 del Ministerio del Interior y Seguridad Pública.



## Metodología

La consulta pública se realizó entre el 16 de septiembre y el 16 de octubre de 2025, a través de los siguientes tres formularios disponibles en el Portal ANCI: i) formulario 1 de caracterización; ii) formulario 2 para referirse a las instituciones preliminarmente calificadas; y, iii) formulario 3 para referirse a instituciones no calificadas.

Para acceder al Portal los participantes ingresaron utilizando su Clave Única y un segundo factor de autenticación. En la instancia participaron personas naturales y jurídicas, en este caso, a través de sus respectivos representantes legales.

Para el presente resumen se normalizó, clasificó y analizó la información recibida por la ANCI. Esta información fue sometida a procedimientos de estandarización de variables, depuración de registros duplicados y codificación temática orientada a identificar patrones argumentativos, recurrencias y tipos de solicitudes.

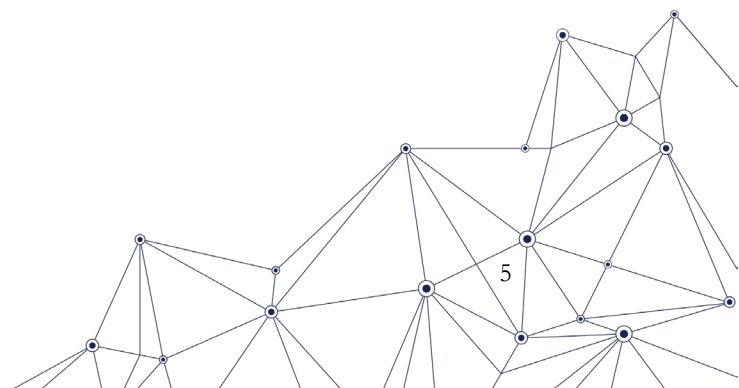
El criterio general fue preservar la integridad de los comentarios, pero ofreciendo una visión agrupada que permitiera la comparación entre casos similares.

Conforme a lo anterior, se realizó una sistematización general, que reúne las observaciones de carácter transversal vinculadas a la aplicación de la ley N°21.663; al diseño del procedimiento de calificación; a los criterios de inclusión o exclusión de operadores de importancia vital; y a las interpretaciones sobre el alcance de los servicios esenciales. Esto se realizó a los Formularios 2 y 3.

El enfoque de análisis combinó herramientas cuantitativas y cualitativas. En el plano cuantitativo se elaboraron indicadores de participación: número total de observaciones, distribución por género, región, y otros datos de caracterización disponibles, así como la frecuencia de los argumentos más repetidos.

En el plano cualitativo se aplicó una codificación semántica de carácter inductivo, que permitió agrupar los argumentos en familias temáticas tales como: dependencia tecnológica, naturaleza del servicio prestado (esencial o no), efectos de un incidente de impacto significativo, rol en la cadena de valor de un sector determinado, entre otras.

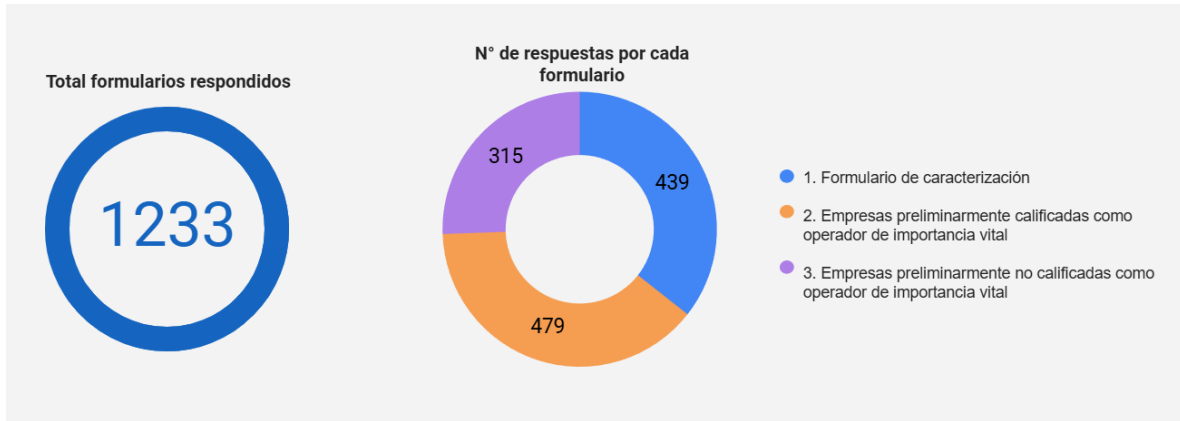
El resultado es un conjunto de productos que permiten dar una mirada ordenada, transparente y documentada del proceso de consulta, facilitando la detección de tendencias, preocupaciones recurrentes y puntos de tensión.



## Estadísticas generales

### Metodología y participación

Se dispusieron 3 formularios independientes, para que cada persona respondiera lo que considerara pertinente.

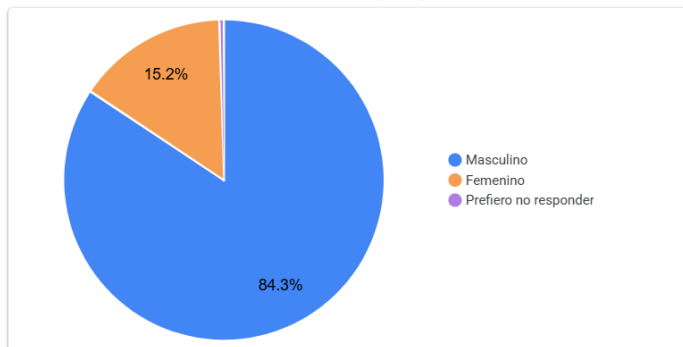


Caracterización voluntaria de los representantes de entidades o personas que respondieron, considerando género, región y ocupación.

### Total de respuestas caracterización

434

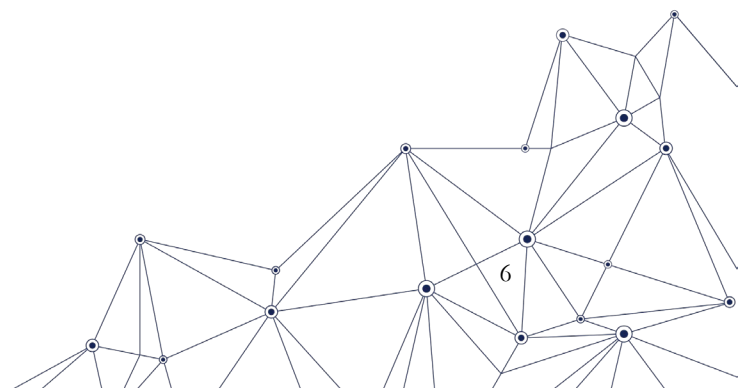
### Caracterización por género



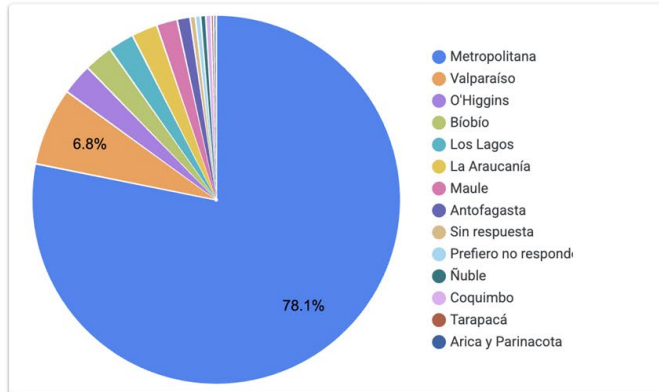
Pregunta no obligatoria

### Caracterización por género

Género	Respondidas por Género	% respondidas por género
Femenino	66	15.21%
Masculino	366	84.33%
Prefero no responder	2	0.46%



### Caracterización por Región

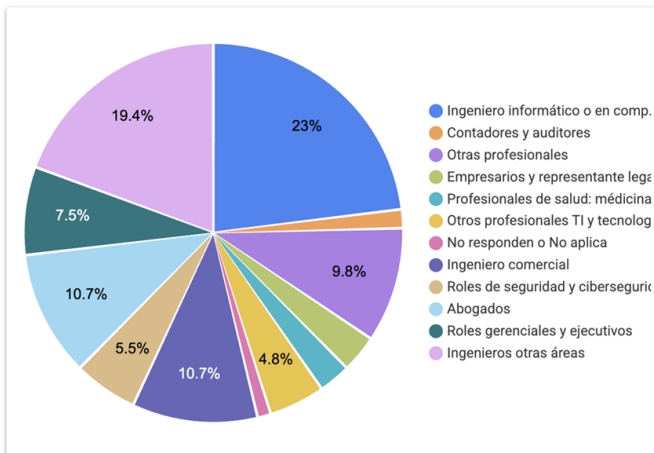


Pregunta no obligatoria

### Caracterización por Región

Región	Respondidas por región	% respondidas por región
Metropolitana	343	78,13 %
Valparaíso	30	6,83 %
O'Higgins	12	2,73 %
BíoBío	11	2,51 %
Los Lagos	10	2,28 %
La Araucanía	10	2,28 %
Maule	8	1,82 %
Antofagasta	5	1,14 %
Sin respuesta	2	0,46 %
Prefiero no responder	2	0,46 %
Ñuble	2	0,46 %
Coquimbo	2	0,46 %
Tarapacá	1	0,23 %
Arica y Parinacota	1	0,23 %

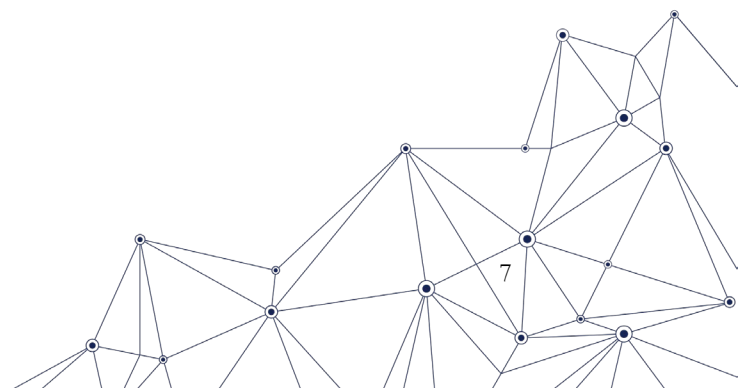
### Profesión u oficio



Pregunta abierta, por lo que la categorización reúne las respuestas similares en una clasificación a posteriori

### Profesión u oficio

Profesión u oficio	Menciones	Menciones
Ingeniero informático o en computación	101	23,01 %
Ingenieros otras áreas	85	19,36 %
Abogados	47	10,71 %
Ingeniero comercial	47	10,71 %
Otras profesionales	43	9,8 %
Roles gerenciales y ejecutivos	33	7,52 %
Roles de seguridad y ciberseguridad	24	5,47 %
Otros profesionales TI y tecnología	21	4,78 %
Empresarios y representante legal	14	3,19 %
Profesionales de salud: medicina, enfermería	12	2,73 %
Contadores y auditores	7	1,59 %
No responden o No aplica	5	1,14 %



## Observaciones recibidas en la Consulta Pública sobre Precalificados

Los comentarios recibidos se pueden agrupar en tres grandes categorías, que son las siguientes:

### 1. Conformidad con la calificación OIV y fundamentación de la criticidad

En un primer grupo aparecen observaciones que respaldan la inclusión de determinadas instituciones que prestan servicios esenciales como OIV. La idea central es que, si dichos servicios se ven interrumpidos, no solo se resiente la continuidad del Estado, sino también la seguridad de la población y, en varios casos, la estabilidad económica y el funcionamiento cotidiano de servicios esenciales.

#### 1.1 Proveedores municipales de plataformas críticas

Se valora especialmente la presencia de empresas que arriendan y administran plataformas informáticas para los municipios. Se indica que un corte o compromiso de estos sistemas tendría efectos inmediatos en la provisión de servicios municipales esenciales, porque allí se concentra información tributaria, financiera, de personal y de atención ciudadana, muchas veces muy sensible. La indisponibilidad de estas plataformas no solo entorpece la gestión pública local; también erosiona la confianza de la ciudadanía en su municipalidad.

#### 1.2. Instituciones financieras y bancarias

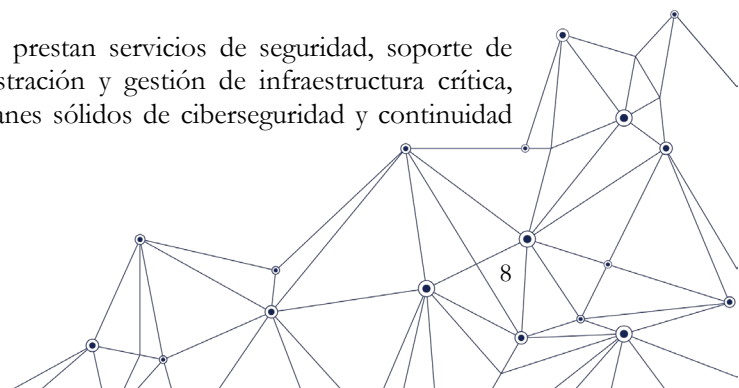
Existe un respaldo claro a la calificación de bancos y cooperativas como OIV. Las observaciones subrayan su rol crítico, en tanto aumentar el estándar regulatorio permite proteger los ahorros, otorgar crédito, posibilitar servicios digitales, sostener el flujo de transacciones seguras y, en definitiva, permitir que el comercio y la inversión sigan funcionando con un mínimo de confianza. Se destaca que los servicios financieros –presenciales y en línea– están hoy tan extendidos que cualquier interrupción prolongada se traduce en un impacto directo sobre la vida diaria de las personas y sobre la estabilidad económica y social.

#### 1.3. Telecomunicaciones e infraestructura TI

También se respalda la inclusión de proveedores de servicios de telecomunicaciones y de tecnologías de la información, entendidos como la columna vertebral sobre la que descansan múltiples servicios esenciales.

#### 1.4. Otros servicios críticos y actores relevantes

Además, se apoya la inclusión de empresas que prestan servicios de seguridad, soporte de seguridad para la Banca y la Minería, y administración y gestión de infraestructura crítica, especialmente cuando demuestran contar con planes sólidos de ciberseguridad y continuidad operativa.



Se considera fundamental calificar como OIV a los proveedores de firma electrónica avanzada, dado que son piezas clave en el ecosistema de funcionamiento digital del país. Junto con ello, se releva el rol de la academia como actor crítico en la generación de conocimiento especializado y en la entrega de una mirada técnica independiente, que permite cuestionar y mejorar los enfoques vigentes.

Por último, se subraya la importancia de los sistemas de identificación para la emisión de cédulas y pasaportes, al ser herramientas básicas para el ejercicio de derechos, la movilidad y la seguridad de las personas. Su interrupción se percibe como especialmente delicada.

## 2. Oposición o cuestionamiento a la calificación OIV

Un segundo conjunto de observaciones revierte la pertinencia de incluir a ciertas entidades en la categoría de OIV o directamente solicita su exclusión. Los argumentos se concentran en la supuesta falta de impacto significativo, la baja dependencia de sistemas informáticos o la existencia de redundancias que amortiguarían los efectos de una eventual interrupción.

### 2.1. Servicios con baja dependencia informática

Se sostiene, por ejemplo, que algunos servicios de salud, como la hemodiálisis, no dependen de manera crítica de redes ni de sistemas informáticos para su prestación. Según estas opiniones, una falla en los sistemas podría ser molesta, pero no impediría que el servicio siguiera prestándose ni comprometería el cumplimiento de las funciones del Estado en esta materia. Desde esa mirada, no se cumplirían los dos requisitos copulativos de la ley: dependencia de sistemas e impacto significativo.

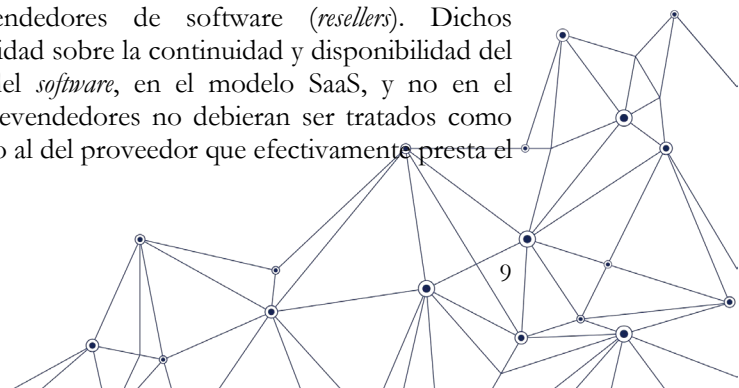
### 2.2. Empresas pequeñas o de baja relevancia sectorial

Otro bloque de comentarios se refiere a empresas de menor tamaño o “bajo impacto” dentro de ciertos sectores, como el eléctrico. Se plantea que el funcionamiento –o incluso la eventual desaparición– de estas compañías no altera de forma apreciable la disponibilidad general del servicio a nivel nacional.

En el mercado de los seguros de vida, se mencionan empresas pequeñas ya supervisadas por la Comisión para el Mercado Financiero (CMF), lo que, según se argumenta, generaría una doble carga regulatoria sin un beneficio proporcional. Se añade que estas compañías no prestan servicios directos de soporte al Estado y que su interrupción no afectaría la seguridad ni el orden público. En otros casos, se llega a afirmar que, si determinadas empresas de distribución de soluciones de comunicación y seguridad dejaran de operar –en especial cuando su operación central está en el extranjero–, el funcionamiento del país “no se vería mayormente alterado”.

### 2.3. Rol de terceros y revendedores

Se cuestiona también la inclusión de revendedores de software (*resellers*). Dichos cuestionamientos se centran en que la responsabilidad sobre la continuidad y disponibilidad del servicio (*uptime*) recae en el proveedor titular del *software*, en el modelo SaaS, y no en el intermediario comercial. Bajo esta lógica, estos revendedores no debieran ser tratados como OIV, ya que su rol en la cadena de valor es distinto al del proveedor que efectivamente presta el servicio.



## 2.4. Proveedores específicos objetados

Algunas observaciones se refieren a la delimitación respecto de cuáles instituciones deben considerarse verdaderamente críticas, especialmente en la línea de su rol en la cadena de suministro o a la posibilidad de algunos servicios de mitigar su interrupción con medidas analógicas.

## 3. Preguntas y observaciones sobre criterios, alcance e implementación

Un tercer grupo de comentarios no se alinea ni con el respaldo ni con las objeciones de casos concretos, sino que se concentra en pedir aclaraciones, ajustes y mejoras al marco normativo, a los criterios de calificación y a la forma en que se implementaría el régimen OIV en la práctica.

### 3.1. Proporcionalidad y costos

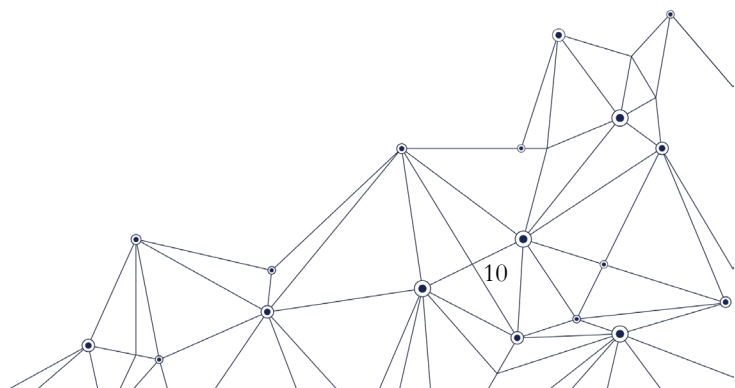
Diversos participantes comentan que las obligaciones de la Ley N°21.663 deben ser proporcionales al nivel de criticidad real de cada entidad. Se propone aplicar criterios de gradualidad y de equivalencia normativa que hagan viable el cumplimiento, especialmente para quienes cuentan con menos recursos.

### 3.2. Criterios de inclusión sectorial

Algunas observaciones requieren establecer diferencias respecto a infraestructura, procesos o funciones consideradas esenciales, particularmente en sectores como el energético.

### 3.3. Coordinación regulatoria interinstitucional

Se subraya la importancia de una coordinación efectiva entre la ANCI y los otros reguladores de las instituciones, sugiriendo dictar normas conjuntas que declaren la equivalencia entre las obligaciones de ciberseguridad ya establecidas por aquellas que ya cuentan con normas en la materia y las que derivan de la ley N°21.663, para evitar duplicidades, vacíos y posibles inconsistencias regulatorias. Se busca, en suma, que las entidades sometidas a múltiples regulaciones encuentren un marco coherente y no una superposición fragmentada de exigencias.



## Observaciones recibidas en la Consulta Pública sobre No-Precalificados

Los comentarios recibidos en este instrumento se pueden agrupar en seis grandes grupos de entidades, que son los siguientes:

### 1. Proveedores de Infraestructura Digital y Plataformas Transversales

Bajo esta categoría se agrupan las empresas que están “detrás de escena”, sosteniendo la infraestructura tecnológica que usan muchos OIV y Proveedores de Servicios Esenciales (PSE). Las observaciones resaltan su carácter sistémico: si fallan, arrastran consigo a varios otros actores que dependen de ellas para operar con normalidad.

#### 1.1 Infraestructura digital y hosting

Incluye *data centers*, servicios de alojamiento, procesamiento y plataformas donde se ejecutan aplicaciones críticas. Son vistos como el “suelo” sobre el cual se montan los servicios que luego entregan al ciudadano.

#### 1.2 Conectividad troncal y telecomunicaciones

Considera a los operadores troncales, redes de alta capacidad y servicios mayoristas de conectividad que permiten que distintos sectores se comuniquen entre sí. Su interrupción puede dejar fuera de línea a múltiples servicios esenciales al mismo tiempo.

#### 1.3 Servicios de ciberseguridad gestionados (SOC/NOC)

Comprende proveedores que ofrecen monitoreo, operación y gestión de incidentes de seguridad y de red. Las observaciones los identifican como piezas clave para detectar y contener ataques que podrían escalar rápidamente si no se controlan a tiempo.

### 2. Medios de pago, software financiero y seguridad social

En este grupo se ubican entidades cuya paralización se percibe como altamente sensible para la vida diaria: pagos, cobros, transferencias, pensiones y beneficios. Las respuestas insisten en que cualquier interrupción prolongada tiene efectos inmediatos en la economía doméstica y en la confianza en el sistema financiero.

#### 2.1 Medios de pago y transacciones

Operadores de tarjetas, adquirentes, redes de cajeros y sistemas de compensación de pagos. Se les reconoce un rol fundamental en el funcionamiento del comercio y en la circulación básica del dinero.

#### 2.2 Software financiero y Fintech

Plataformas tecnológicas que soportan operaciones financieras críticas o servicios innovadores de pago e inversión. Aunque algunas son relativamente nuevas, las observaciones advierten que su masificación las vuelve crecientemente sensibles desde el punto de vista sistémico.

### 2.3 Seguridad social y previsional

Entidades que gestionan fondos, plataformas de pago de beneficios y pensiones. La criticidad se asocia al riesgo de que millones de personas dejen de recibir sus ingresos o prestaciones en tiempo y forma.

## 3. Servicios de soporte crítico al sector público (Gobierno, educación y municipalidades)

Aquí se agrupan actores que permiten que el Estado funcione en el día a día: lo que incluye a municipios, servicios públicos y universidades, entre otros. La mirada se centra en quienes proveen, operan o mantienen sistemas donde se aloja información sensible o donde se gestionan procesos clave de la administración.

### 3.1 Sistemas de gestión municipal

Plataformas integrales que apoyan recaudación, finanzas, recursos humanos y atención ciudadana en municipios. Su interrupción se traduciría en trámites detenidos, retrasos en pagos y, en general, en una gestión local muy limitada.

### 3.2 Educación superior y datos

Universidades y sistemas que administran datos académicos, personales y de investigación. Se enfatiza el volumen y la sensibilidad de la información que manejan, así como su rol en la formación de capital humano avanzado.

### 3.3 Soporte de software y plataformas

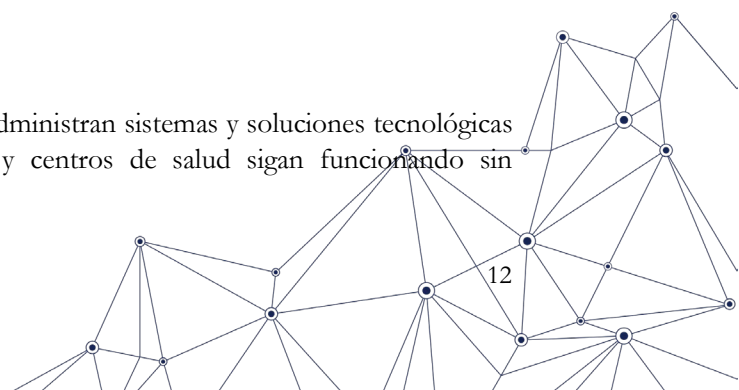
Proveedores que dan soporte a aplicaciones utilizadas por más de un organismo público. Cuando estos fallan, el impacto se multiplica porque afecta a varias instituciones a la vez, no solo a una en particular.

## 4. Infraestructura crítica de servicios básicos y logística

Esta categoría reúne servicios esenciales que forman parte de la segunda etapa del primer procedimiento de calificación que comenzará a fines de noviembre de 2025, tales como suministro de agua potable, transporte y combustibles. Las observaciones remarcan que una afectación sería en estos ámbitos puede tener consecuencias que escalan muy rápido a nivel social y económico.

## 5. Proveedores críticos del sector salud

En este grupo se consideran empresas que desarrollan o administran sistemas y soluciones tecnológicas que se han vuelto indispensables para que hospitales y centros de salud sigan funcionando sin



interrupciones mayores. La idea de fondo es que, si se cae el proveedor, se afectan al mismo tiempo muchos recintos asistenciales.

### 5.1 Ficha clínica electrónica y sistemas hospitalarios

Plataformas que sostienen la gestión clínica, administrativa y de apoyo a la toma de decisiones médicas. Una falla severa en estos sistemas puede complicar desde la atención diaria hasta la continuidad de tratamientos complejos.

### 5.2 Centros de salud y hospitales específicos

Entidades cuya infraestructura digital o servicios tecnológicos son especialmente críticos para que determinados hospitales o redes de salud puedan atender a sus pacientes.

## 6. Comentarios misceláneos y otros proveedores

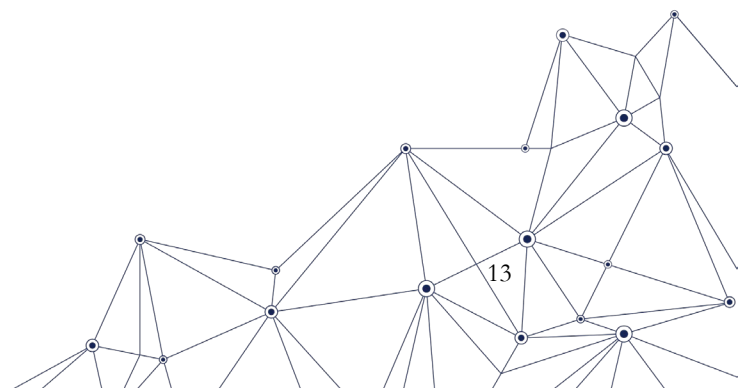
Finalmente, se agrupan aquí observaciones más heterogéneas, que no encajan del todo en las categorías anteriores, pero que apuntan a riesgos específicos o a preocupaciones sobre trato regulatorio equitativo entre actores.

### 6.1 Proveedores de insumos críticos

Empresas que suministran bienes materiales necesarios para la operación de servicios esenciales (por ejemplo, ciertos insumos técnicos o especializados). La preocupación se centra en la vulnerabilidad de la cadena de suministro.

### 6.2 Organizaciones de la sociedad civil y educación inicial

Actores no lucrativos o educativos, especialmente vinculados a la primera infancia y grupos vulnerables. Su inclusión se fundamenta en el valor social de su trabajo y en la necesidad de resguardar su continuidad frente a incidentes de ciberseguridad.



## Conclusiones

El proceso de consulta pública desarrollado por la Agencia Nacional de Ciberseguridad constituyó un ejercicio fundamental para fortalecer la legitimidad, la transparencia y la calidad técnica del primer procedimiento de calificación de Operadores de Importancia Vital (OIV). La metodología utilizada, basada en instrumentos diferenciados, autenticación robusta y un análisis combinado de datos cuantitativos y cualitativos, permitió captar de manera fiel y ordenada la diversidad de perspectivas existentes entre personas naturales, instituciones públicas y privadas, y organizaciones de la sociedad civil.

Los resultados evidencian un ecosistema heterogéneo, en el que conviven valoraciones positivas sobre la calificación de múltiples entidades, cuestionamientos fundados sobre casos específicos y, especialmente, un amplio conjunto de inquietudes transversales relativas a criterios, definiciones, alcances e impactos de la ley N°21.663. La sistematización realizada muestra que la ciudadanía y los actores regulados comprenden plenamente la relevancia del régimen OIV, pero también demandan que su implementación sea técnica, proporcional y coherente entre sectores, entre otros.

Asimismo, se observa un reconocimiento generalizado del rol estratégico de la infraestructura digital, los servicios de conectividad, la banca y los sistemas de salud, así como de la necesidad de considerar adecuadamente la criticidad de proveedores que sostienen transversalmente al Estado y a los servicios esenciales. En paralelo, emergen preocupaciones sobre la carga regulatoria, los riesgos de asimetrías competitivas y la necesidad de mayor claridad interpretativa, todos elementos clave para garantizar un proceso equilibrado y sostenible en el tiempo.

El ejercicio participativo permitió identificar patrones, tendencias y puntos de tensión que serán decisivos para perfeccionar el diseño definitivo del procedimiento de calificación. Las observaciones recogidas constituyen insumos valiosos para fortalecer los criterios de evaluación, mejorar la coherencia regulatoria, orientar ajustes sectoriales y asegurar que las obligaciones asociadas al régimen OIV se apliquen de manera justa, efectiva y consistente con la criticidad real de cada entidad.

En suma, la consulta pública no solo aportó evidencia técnica para la toma de decisiones, sino que reafirmó la importancia de la colaboración entre Estado, sector privado y ciudadanía en la construcción de una política de ciberseguridad robusta, moderna y centrada en la resiliencia del país. La ANCI continuará avanzando en este proceso con el compromiso de integrar las recomendaciones recibidas, perfeccionar sus mecanismos de coordinación y fortalecer la protección de los servicios esenciales y de la infraestructura digital que sostiene la vida cotidiana de millones de personas.

