

PROCESO PRESUPUESTARIO 2027

DEFINICIONES ESTRATÉGICAS

Ministerio	MINISTERIO DE SEGURIDAD PÚBLICA	Partida	32
Servicio	AGENCIA NACIONAL DE CIBERSEGURIDAD	Capítulo	06

LEY ORGÁNICA O DECRETO QUE RIGE AL SERVICIO

Ley N° 21.663 Marco de Ciberseguridad. Por su parte el Decreto con Fuerza de Ley N°1-21.663, que fija planta de personal de directivos de la Agencia Nacional de Ciberseguridad y regula otras materias a que se refiere el artículo primero transitorio de la Ley N°21.663, Decreto N°483 del 23 de diciembre de 2024 de la Subsecretaría del Interior aprueba reglamento que determina la estructura interna de la agencia nacional de ciberseguridad.

MISIÓN DEL MINISTERIO

Resguardar, mantener y promover la seguridad y el orden público, la prevención del delito y la protección de las personas en materia de seguridad, hacer frente al crimen organizado y terrorismo, fortalecer a las policías y los colaboradores municipales y privados de seguridad, y la integración de Gendarmería; mediante la articulación del Sistema de Seguridad Pública y la planificación, diseño, formulación, implementación, supervisión y evaluación de políticas, planes y programas en ámbitos de seguridad, prevención y asistencia a víctimas, actuando bajo los principios de protección de derechos humanos, coordinación policial, cooperación interministerial e interoperabilidad.

MISIÓN DEL SERVICIO

Dirigir, coordinar y supervisar la protección, promoción y respeto del derecho a la seguridad de las personas en el entorno digital, mediante la ejecución de acciones orientadas a la prevención y respuesta a incidentes de ciberseguridad, así como al fortalecimiento de las capacidades técnicas, normativas y operativas en materias de ciberseguridad de los actores públicos y privados.

COMPROMISOS PROGRAMÁTICOS DEL MINISTERIO

N°	Compromiso programático del ministerio
1	Recuperar territorios bajo control del crimen organizado, garantizando condiciones de seguridad, protección para la población.
2	Fortalecer el marco normativo y las capacidades del sistema de seguridad municipal para la prevención y control del delito.
3	Fortalecer la interoperabilidad de datos entre las instituciones del sistema de seguridad pública para apoyar la coordinación operativa y la toma de decisiones.
4	Fortalecer las capacidades de coordinación policial mediante sistemas integrados de información de alcance nacional.
5	Fortalecer la seguridad fronteriza mediante la articulación de capacidades de personal, tecnología e infraestructura con enfoque interinstitucional.
6	Integrar institucionalmente el sistema penitenciario al ecosistema de fuerzas de orden y seguridad pública.
7	Desarrollar estrategias de prevención, difusión e información orientadas a reducir los delitos, sus mercados ilícitos asociados y el apoyo a víctimas.
8	Impulsar un marco legal que permita la persecución efectiva de incivildades en coordinación con actores públicos y privados.
9	Fortalecer las capacidades autónomas de las policías para conducir investigaciones de manera eficaz, en el marco del ordenamiento jurídico vigente.
10	Fortalecer el marco normativo del proceso penal para permitir la resolución oportuna de causas, reduciendo la impunidad por no comparecencia del imputado y resguardando las garantías del debido proceso.
11	Diseñar e implementar una estrategia nacional contra el terrorismo que aborde el fenómeno delictual de forma integral.
12	Reducir los delitos contra la propiedad mediante el fortalecimiento de sistemas tecnológicos de detección, seguimiento y atención a víctimas.
13	Modernizar la infraestructura policial para mejorar las condiciones operativas y la atención a la ciudadanía.
14	Fortalecer la regulación y los estándares del sector de seguridad privada como actor del sistema de prevención y control del delito.
15	Fortalecer los controles en rutas para la fiscalización y el orden público.

COMPROMISOS PROGRAMÁTICOS DEL SERVICIO

N°	Compromiso programático del servicio	Compromiso programático ministerial al que se vincula
-	-	-

VINCULACIÓN ESTRATÉGICA

OBJETIVOS ESTRATÉGICOS DEL SERVICIO Y OBJETIVOS ESTRATÉGICOS DEL MINISTERIO

Objetivo Estratégico del Servicio 1

Aumentar las capacidades nacionales para la prevención y gestión de riesgos de ciberseguridad, mediante la implementación de políticas públicas en la materia.

Objetivo Estratégico del Servicio 2

Asegurar la gestión oportuna y eficaz de los incidentes de ciberseguridad mediante la definición e implementación de protocolos y estándares, garantizando que los servicios esenciales cuenten con acceso continuo a una plataforma de reporte y cuenten con mecanismos de respuesta que permitan disminuir la probabilidad de pérdida en la continuidad operacional y en la confidencialidad e integridad de la información.

Objetivo Estratégico del Servicio 3

Diseñar e implementar planes y acciones de formación orientadas a personas y actores que integran el ecosistema de ciberseguridad, que permitan generar concientización sobre el cuidado y la prevención ante las amenazas digitales a las que se ven expuestos.

Objetivo Estratégico del Servicio 4

Desarrollar y ejecutar el procedimiento definido en la Ley N° 21.663 para la calificación de operadores de importancia vital, asegurando la identificación oportuna de las instituciones públicas y privadas cuya afectación tenga un impacto significativo en la seguridad y el orden público, o en la provisión continua y regular de servicios esenciales.

Objetivo Estratégico del Servicio 5

Garantizar el cumplimiento de los fines y disposiciones de la Ley N° 21.663, sus reglamentos, protocolos, estándares técnicos, e instrucciones generales y particulares emitidos por la Agencia a través del diseño de estrategias y mecanismos de fiscalización y sanción.

Objetivo Estratégico del Servicio 6

Gestionar y operar la Red de Conectividad Segura del Estado para contar con una infraestructura de red con un alto nivel de disponibilidad y resiliencia, que permita el intercambio confidencial e íntegro de información para los organismos de la Administración del Estado.

Contribuyen

Contribuyen

Objetivo Estratégico Ministerial

Reducir la exposición a riesgos y amenazas de ciberseguridad que puedan afectar la continuidad de los servicios esenciales y operadores de importancia vital, articulando las capacidades nacionales.

Objetivo Estratégico Ministerial

Reducir la exposición a riesgos y amenazas de ciberseguridad que puedan afectar la continuidad de los servicios esenciales y operadores de importancia vital, articulando las capacidades nacionales.

Nube de palabras: términos destacados de los OES y OEM vinculados mostrados arriba.

esenciales cuentan
continuidad operacional
confidencialidad integridad
actores integran
políticas públicas
definición implementación
importancia vital
diseñar implementar planes
acceso continuo plataforma
respuesta permitan disminuir
ciberseguridad puedan afectar
gestión oportuna
permiten generar concientización
capacidades nacionales
intercambio confidencial integro
formación orientadas personas

Nota: El presente reporte considera aquellos objetivos estratégicos del servicio (OES) que cuentan con una vinculación estratégica con su respectivo objetivo estratégico ministerial (OEM), evaluada y validada satisfactoriamente desde el punto de vista metodológico por DIPRES. Por lo tanto, los OES que no se encuentran incluidos en el reporte corresponden a aquellos que no cumplen con esta condición, aun cuando se encuentran registrados en la plataforma del Formulario A1 de DIPRES.

Por lo anterior, en el presente reporte, el número de objetivos de desempeño presentados en esta tabla no necesariamente coincidirá con el número de objetivos de desempeño con los cuales se vinculan los programas públicos en el apartado siguiente, dado que la evaluación de los objetivos de desempeño y la evaluación de la vinculación de los programas públicos con dichos objetivos se realizaron de manera independiente.

BIENES Y SERVICIOS FINALES

VINCULACIÓN CON OBJETIVOS ESTRATÉGICOS DEL SERVICIO

N°	Bien o servicio final	Objetivo Estratégico del Servicio al cual se relaciona
1	Implementación y seguimiento de la Política Nacional de Ciberseguridad y su Plan de Acción.	Objetivo 1
2	Recepción y gestión de reportes de incidentes de ciberseguridad.	Objetivo 2
3	Gestión y administración del Registro Nacional de Incidentes de Ciberseguridad.	Objetivo 2
4	Elaboración de material didáctico en materias de prevención de ciberseguridad.	Objetivo 3
5	Calificación de instituciones públicas y privadas como operadores de importancia vital.	Objetivo 4
6	Fiscalización del cumplimiento de obligaciones de ciberseguridad.	Objetivo 5
7	Monitoreo y emisión de alertas y avisos técnicos para la RCSE.	Objetivo 6

Nota: Los bienes y servicios se presentan en su totalidad, de acuerdo con lo informado por los servicios, sin que exista una selección previa por parte de DIPRES.

OFERTA PROGRAMÁTICA DEL SERVICIO

VINCULACIÓN CON OBJETIVOS ESTRATÉGICOS DEL SERVICIO

N°	Programa público	Objetivo Estratégico del Servicio al cual se relaciona
-	-	-

Nota: El presente reporte considera únicamente los programas de la Oferta de Programas Públicos (OP) que cuentan con al menos una vinculación estratégica con un objetivo estratégico del servicio, evaluada y validada satisfactoriamente por DIPRES desde el punto de vista metodológico. En consecuencia, no se incluyen en el reporte aquellos programas que no cuentan con vinculaciones que cumplan con esta condición, ni aquellas vinculaciones que no hayan sido validadas satisfactoriamente desde el punto de vista metodológico.

Nota: El presente formulario contiene oferta programática 2026.

Nota general: En el marco de la revisión de los indicadores de desempeño del Formulario H, se podrán corregir y posteriormente incorporar al Formulario A1 aquellos elementos que mantengan observaciones de DIPRES derivadas de la revisión de dicho formulario.