# Evolución de las estrategias de ciberseguridad

## Análisis del escenario regional e internacional


**Autores**

Santiago Paz

Martina Bergues

José Callero



BID

# Evolución de las estrategias de ciberseguridad

## Análisis del escenario regional e internacional

**Autores**
Santiago Paz
Martina Bergues
José Callero

Banco Interamericano de Desarrollo

Esta publicación fue desarrollada por el Banco Interamericano de Desarrollo con el apoyo de los siguientes proyectos de cooperación técnica: el Fondo Especial Japonés, financiado por el Gobierno de Japón, y el Fondo Coreano para el Desarrollo Económico, financiado por el Gobierno de Corea.

**Códigos JEL:** H11, O38, O33
**Palabras clave:** ciberseguridad, estrategias, gobernanza, planes de acción, seguridad de la información, ciberseguridad, políticas públicas, economía digital, ciberdefensa, privacidad, seguridad por diseño, resiliencia digital




Banco Interamericano de Desarrollo
1300 New York Avenue, N.W.
Washington D. C. 20577
www.iadb.org

El Sector de Instituciones para el Desarrollo tuvo a su cargo la producción de esta publicación.

**Proveedores externos:** Coordinación de producción editorial: A&S Information Partners, LLC

**Revisión editorial:** Giovana Boselli

**Diagramación:** The Word Express, Inc.

# ÍNDICE

# 1 Resumen ejecutivo

## ¿Por qué realizar un estudio sobre las estrategias nacionales de ciberseguridad?

- El Informe de Riesgos Globales 2023 del Foro Económico Mundial[1] señala que los encuestados consideran que el octavo riesgo más importante es la ciberseguridad. En 2022, la región de América Latina sufrió al menos 360.000 millones de intentos de ataques. Brasil es el segundo país más afectado, después de México, con 103.000 millones de intentos.[2]
- Estas situaciones son cada vez más sofisticadas, y el *ransomware* (extorsión) representa el 17% de las ofensivas detectadas en todo el mundo. Un ejemplo de este tipo de ataques es el que sufrió recientemente la empresa IFX Network[3], el cual afectó a más de 50 empresas públicas y privadas en Colombia y Chile y las dejó fuera de servicio.
- La prevalencia, el aumento y la complejidad de las ofensivas requieren que los países adopten un enfoque estratégico y coordinado proporcional a las amenazas. Las estrategias nacionales de ciberseguridad constituyen una herramienta que permite a los países trazar sus planes con el objetivo de proteger y asegurar el ciberespacio.
- A pesar de que las estrategias nacionales[4] se publican desde hace dos décadas y de que algunos países ya publicaron tres versiones, todavía falta sistematizar el conocimiento necesario a fin de entender la evolución de sus contenidos y la divulgación de las principales lecciones aprendidas es escasa.
- La finalidad de este estudio es crear una metodología que permita comparar documentos heterogéneos e identificar tendencias y patrones que ayuden a los países en su proceso de elaboración de nuevas versiones de sus estrategias nacionales de ciberseguridad.

## ¿Qué metodología se utilizó?

- Se analizaron 43 estrategias nacionales de 19 países, incluidas estrategias de primera, segunda y tercera generación.
- Para cada estrategia, se realizó un análisis de las principales áreas de interés y se tomó como referencia la adaptación de las áreas de interés incluida en la *Guía para la elaboración de una estrategia nacional de ciberseguridad*, publicación elaborada con la coordinación de la Unión Internacional de Telecomunicaciones (UIT).

[1] Global Risk Report 2023.
[2] https://socradar.io/wp-content/uploads/2023/06/Brazil-Threat-Landscape-Report.pdf.
[3] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-que-informacion-se-pudieron-haber-robado-en-el-ciberataque-805730.
[4] La primera estrategia analizada en este estudio data de 2003 y corresponde a la primera estrategia de los Estados Unidos.

- En primer lugar, para documentar la situación actual de las estrategias de ciberseguridad más recientes, el análisis buscó comprender cómo se presenta cada tema en las estrategias vigentes.
- Luego, para identificar patrones y diferencias regionales, se examinaron los mismos aspectos comparando las estrategias de América Latina con las de otros países, lo cual permitió identificar matices regionales y puntos de convergencia global.
- Por último, para comprender cómo esos temas evolucionaron con el tiempo, se adoptó una metodología innovadora. Se categorizaron las estrategias por año de publicación y por generación (primera, segunda o tercera), con lo cual fue posible distinguir matices en las tendencias vinculadas al paso del tiempo y a la madurez de los países.
- Asimismo, el informe incluye estudios de caso con el fin de brindar una visión más amplia y detallada de diversos aspectos de las estrategias analizadas. Los casos brindan perspectivas específicas que enriquecen el análisis comparativo.

## ¿Cuáles son los principales hallazgos?

- A pesar de que los formatos, el alcance, la vigencia y los temas tratados en las diferentes estrategias son muy heterogéneos, es posible identificar diversos patrones y tendencias al efectuar un análisis sistemático.
- Con respecto a las estrategias de las generaciones anteriores, las estrategias de tercera generación son más operativas y menos teóricas.
- Entre los hallazgos regionales, se observa que, en términos de formato y gobernanza de las estrategias, con mayor frecuencia, América Latina tiende a asociar sus estrategias con normativas, mientras que es menos frecuente que defina planes operativos y establezca mecanismos de coordinación con el sector privado.
- Las estrategias más recientes, especialmente en el Norte Global, no solo se centran en la seguridad nacional, sino que también incluyen temas como prosperidad económica y promoción industrial. Esto refleja una tendencia a considerar la ciberseguridad como un ámbito crucial para el desarrollo económico y social de un país.
- Entre las estrategias vigentes hoy en día, prácticamente todas tienen objetivos o iniciativas relacionadas con la preparación y la resiliencia, y la gran mayoría incluye objetivos para fortalecer las capacidades de ciberseguridad.
- En cuanto a los temas, objetivos y líneas de acción incluidas, cabe destacar que las estrategias analizadas del Norte Global muestran, con mayor frecuencia, una preocupación por los ataques a la democracia y los ataques extremistas. También incluyen, en mayor medida, componentes relacionados con la prosperidad económica y la promoción industrial, y establecen más a menudo medidas para proteger los activos digitales de los Gobiernos, entre otras tendencias que se analizarán en el estudio.
- En cuanto al análisis evolutivo, además de la mencionada tendencia a aumentar el número de principios, iniciativas y objetivos relacionados con la prosperidad económica y la promoción industrial de la ciberseguridad, se destacan: (i) el aumento de los principios, iniciativas y objetivos relacionados con la transparencia y la confianza en el ciberespacio; (ii) el aumento de iniciativas destinadas a promover la diversidad en la fuerza de trabajo de la ciberseguridad; (iii) la disminución de objetivos relacionados con la infraestructura crítica (IC) en las estrategias de tercera generación; (iv) el aumento de la

presencia de mecanismos para promover el intercambio de información y ampliar la cooperación, y (v) el aumento de la presencia del concepto de seguridad por diseño *(security by design)*[5], entre otras tendencias que se mencionarán en este estudio.

[5] Según la definición de la Agencia de Ciberseguridad de los Estados Unidos (CISA, por sus siglas en inglés), la seguridad por diseño se refiere a que los productos tecnológicos se desarrollaron de forma tal que protegen contra actores cibernéticos malintencionados que intentan acceder a dispositivos, datos y *software* de infraestructura conectada.

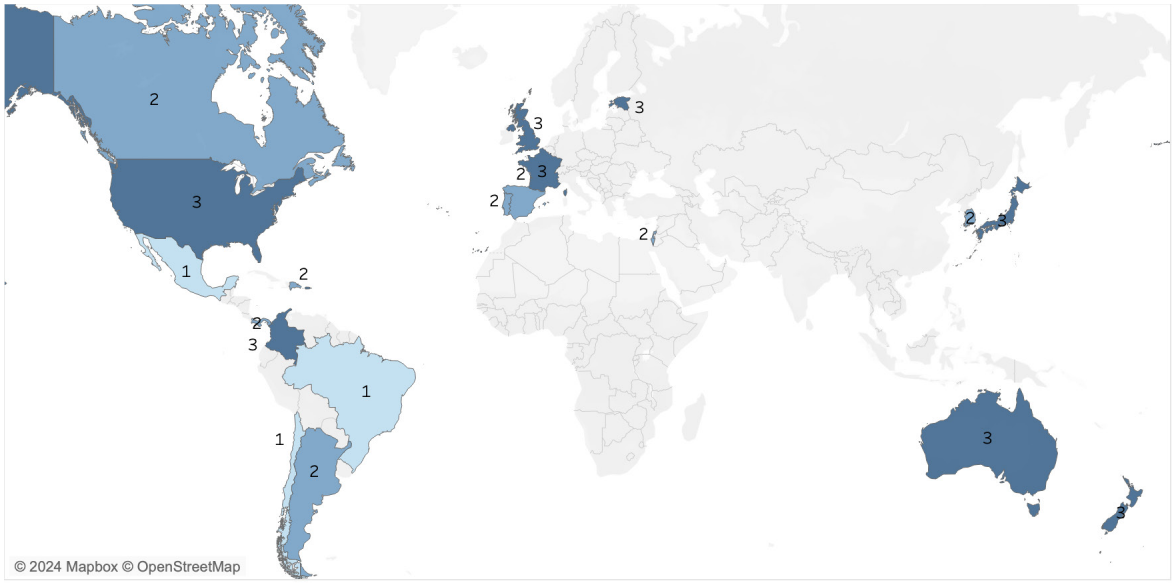
# 2 Metodología

## 2.1. Selección de los países

Con el fin de evaluar la experiencia regional en este tema, se analizaron doce países con un nivel avanzado de madurez fuera de América Latina y siete países de esa región. De las 43 estrategias estudiadas en total, 19 están vigentes. Para identificar a los países que se incluirían en el estudio y garantizar la inclusión de los más avanzados del mundo, se consideró el nivel de madurez del índice global de ciberseguridad (GCI, por sus siglas en inglés) de la UIT[6] y/o su participación en Digital Nations[7]. En cuanto a la elección de los países de América Latina y el Caribe, se consideró el extenso trabajo que el Banco Interamericano de Desarrollo (BID) realizó en la región a fin de incluir países con estrategias que podrían aportar valor al proceso de construcción de la estrategia de ciberseguridad en Brasil. Por lo tanto, se analizaron los siguientes países y la evolución de sus estrategias: Argentina, Australia, Brasil, Canadá, Chile, Colombia, Corea, España, Estados Unidos de América, Estonia, Francia, Israel, Japón, México, Nueva Zelanda, Panamá, Portugal, República Dominicana y Reino Unido.

[6] Global Cybersecurity Index.
[7] DN – Digital Nations.

**MAPA 1 – NÚMERO DE ESTRATEGIAS ANALIZADAS POR PAÍS**



Las estrategias analizadas se clasificaron por tiempo y por generación. El concepto de generación se refiere a si la estrategia considerada fue la primera, segunda o tercera publicada en cada país. La muestra analizada incluye países con una, dos o tres estrategias.[8] El diagrama a continuación presenta el número de estrategias por período y por generación.

**DIAGRAMA 1 – NÚMERO DE ESTRATEGIAS POR PERÍODO Y GENERACIÓN**

| | 1.ª | 2.ª | 3.ª |
|---|---|---|---|
| Antes de 2010 | 3 | 0 | 0 |
| 2011-2015 | 9 | 3 | 0 |
| 2016-2020 | 7 | 9 | 3 |
| Después de 2020 | 0 | 4 | 5 |

## 2.2. Análisis de las estrategias

El análisis de las estrategias se efectuó mediante un estudio documental. Para ello, se recopilaron y examinaron los documentos de las estrategias de ciberseguridad de los países seleccionados.

Se establecieron categorías de análisis predefinidas para realizar una revisión sistemática que permitiera comparar e identificar tendencias y para que todas las estrategias se examinaran con el mismo criterio. Estas categorías se crearon a partir de una adaptación de la *Guía para la elaboración de una estrategia nacional de ciberseguridad*,[9] un documento de referencia internacional elaborado por más de 12 organizaciones asociadas, con la coordinación de la UIT.

[8] Las estrategias se distribuyen por período y por generación de la siguiente forma: primera generación, publicadas antes de 2010: Estados Unidos (2003), Estonia (2008) y Canadá (2010); primera generación, publicadas entre 2011 y 2015: Reino Unido (2011), Nueva Zelanda (2011), Corea (2011), Colombia (2011), Francia (2011), España (2013), Panamá (2013), Portugal (2015), Japón (2015); primera generación, publicadas entre 2016–2022: Australia (2016), Chile (2017), Israel (2017), México (2017), República Dominicana (2018), Argentina (2019), Brasil (2020); segunda generación, publicadas entre 2011–2015: Estonia (2014), Nueva Zelanda (2015), Francia (2015); segunda generación, publicadas entre 2016–2020: Reino Unido (2016), Colombia (2016), Canadá (2018), Estados Unidos (2018), Japón (2018), Corea (2019), España (2019), Portugal (2019), Australia (2020); segunda generación, publicadas después de 2020: Israel (2021), Panamá (2021); República Dominicana (2022), Argentina (2023); tercera generación, publicadas entre 2016–2020: Estonia (2019), Nueva Zelanda (2019), Colombia (2020); tercera generación, publicadas después de 2020: Japón (2021), Francia (2021), Reino Unido (2022), Australia (2023), Estados Unidos (2023). En el caso de Colombia, se consideraron como representantes de las estrategias las políticas públicas plasmadas en los documentos del Consejo Nacional de Política Económica y Social (CONPES).

[9] Guide to Developing a National Cibersecurity Strategy.

Como referencia, las macrocategorías analizadas incluyen componentes transversales: (i) estructura de las estrategias; (ii) amenazas y desafíos; (iii) principios; (iv) objetivos estratégicos (agrupados en 12 categorías), y (v) métricas e indicadores. Además, las macrocategorías incluyen las siguientes áreas de interés: (i) gobernanza; (ii) gestión de riesgos; (iii) resiliencia y preparación; (iv) infraestructura crítica y servicios esenciales; (v) capacidades y concientización; (vi) marco normativo y legislación; (vii) cooperación internacional; (viii) privacidad y datos, y (ix) defensa y capacidad militar. Las dos últimas se añadieron como complemento a las áreas de interés sugeridas en el documento de la UIT. Véanse los detalles en el diagrama a continuación.

## DIAGRAMA 2 – COMPONENTES TRANSVERSALES


Se analizó cada documento con el objetivo de clasificar cada tema de la estrategia y generar datos comparables. Dos investigadores efectuaron una calibración basada en tres estrategias antes de la consolidación de los datos para garantizar que la comprensión de las categorías estuviera alineada y que la metodología fuera sólida. Cabe destacar que el objetivo de la categorización no es comprender exhaustivamente cada una de las estrategias, sino permitir la comparación e identificar las tendencias globales. Es posible que existan pequeñas diferencias en la categorización debido a la metodología; sin embargo, esto no invalida los hallazgos globales del estudio. Se recomienda el estudio de casos y la realización de entrevistas con especialistas para optimizar la categorización y agregar valor al estudio en una próxima edición.

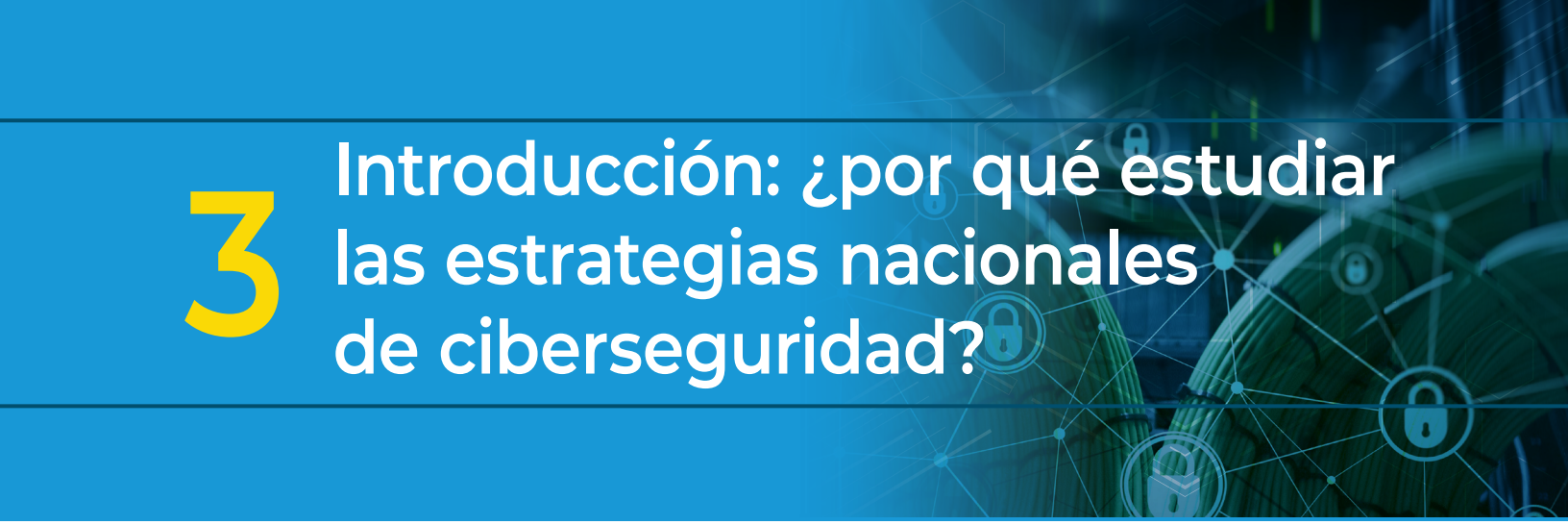
## RECUADRO 1 – LIMITACIONES DEL ESTUDIO: CÓMO LEER LOS GRÁFICOS Y LOS DATOS

El estudio sigue un patrón de análisis para todos los temas seleccionados. Para cada tema, primero se presenta un análisis que incluye solo las estrategias vigentes (según el país, hay estrategias de primera, segunda y tercera generación). En esta etapa, también se efectúa una comparación directa entre las estrategias de América Latina y las de los demás países.

A continuación, y para cada tema, se incluye un gráfico que analiza la evolución de las estrategias desde dos perspectivas: (i) por generación de las estrategias (si es la primera, la segunda o la tercera estrategia de un determinado país) o (ii) por período. La comparación de los dos tipos de evolución ayuda a comprender si existe algún patrón temporal o si la variación de un determinado tema puede estar relacionada con la madurez de los países. Se entiende que una estrategia de tercera generación incluye las lecciones aprendidas de las versiones anteriores.

Es importante tener en cuenta algunas limitaciones.

i. Existe una dificultad inherente en la clasificación comparativa de documentos con diferentes estructuras y niveles de profundidad. Por ejemplo, clasificar en categorías binarias un documento de cinco páginas y otro de 130 representa un desafío, ya que no es posible analizar la profundidad con que cada tema aparece en los documentos, sino simplemente verificar si fue mencionado o no.
ii. El número de estrategias analizadas es reducido (n=19 para el primer conjunto de gráficos y n=43 para el segundo) y no es uniforme entre generaciones, años y regiones. Esto implica que, para algunas categorías, una estrategia tiene más peso que para otras. Otro desafío inherente al fenómeno estudiado es que no existe la misma cantidad de países que hayan publicado estrategias de cada generación en el mismo año. La inclusión de nuevas estrategias en el estudio o de pequeños cambios en la comprensión de las categorías puede generar variaciones en los resultados. Por lo tanto, las estadísticas solo deben utilizarse como un instrumento para identificar tendencias y no como una forma de determinar un resultado específico.
iii. El análisis se efectuó a partir de la lectura de los documentos. Si se tratase de un cuestionario que los países debían completar, la comprensión de cada estrategia podría tener matices difíciles de identificar completamente en un simple análisis documental. Aunque se demostró la solidez de esta metodología, existe un cierto nivel de subjetividad en la interpretación de documentos con formatos y niveles de detalle muy variados.



# 3 Introducción: ¿por qué estudiar las estrategias nacionales de ciberseguridad?

En la era digital, la ciberseguridad se convirtió en un imperativo estratégico para los Gobiernos de todo el mundo. El creciente volumen y sofisticación de las amenazas cibernéticas puso de manifiesto la necesidad de contar con estructuras de protección sólidas y coordinadas. En este contexto, las estrategias nacionales de ciberseguridad emergen como instrumentos fundamentales para garantizar la seguridad y la resiliencia del ciberespacio.

Las estrategias nacionales de ciberseguridad pueden considerarse como marcos estratégicos desarrollados por los países para proteger su infraestructura crítica, redes gubernamentales, empresas privadas y ciudadanos frente a las crecientes amenazas del mundo digital. A pesar de que no existe una definición universal de estrategia de ciberseguridad, y de que la propia UIT en la *Guía para la elaboración de una estrategia nacional de ciberseguridad*[10] señala que "no existe una definición consolidada y consensuada sobre qué constituye una estrategia nacional de ciberseguridad", este estudio propone considerar que una estrategia nacional de ciberseguridad comprende:

- una expresión de la visión, los objetivos de alto nivel, los principios y las prioridades que guían a un país en materia de ciberseguridad;
- una concepción de los actores responsables de mejorar la ciberseguridad del país y sus respectivos papeles y responsabilidades, y
- una descripción de las medidas, los programas y las iniciativas que un país adoptará para proteger su infraestructura cibernética nacional y, en el proceso, aumentar su seguridad y resiliencia.

El objetivo principal de las estrategias es proporcionar una orientación clara y actualizada sobre cómo los Gobiernos, junto con el sector privado y la sociedad civil, pueden hacer frente a las amenazas cibernéticas. Además de establecer objetivos y prioridades, estas estrategias también definen las funciones y responsabilidades de las diferentes partes interesadas, promueven la cooperación internacional y fomentan la innovación en tecnología de seguridad. En otras palabras, funcionan como una brújula para orientar los esfuerzos de un país para aumentar su madurez en ciberseguridad de forma integral.

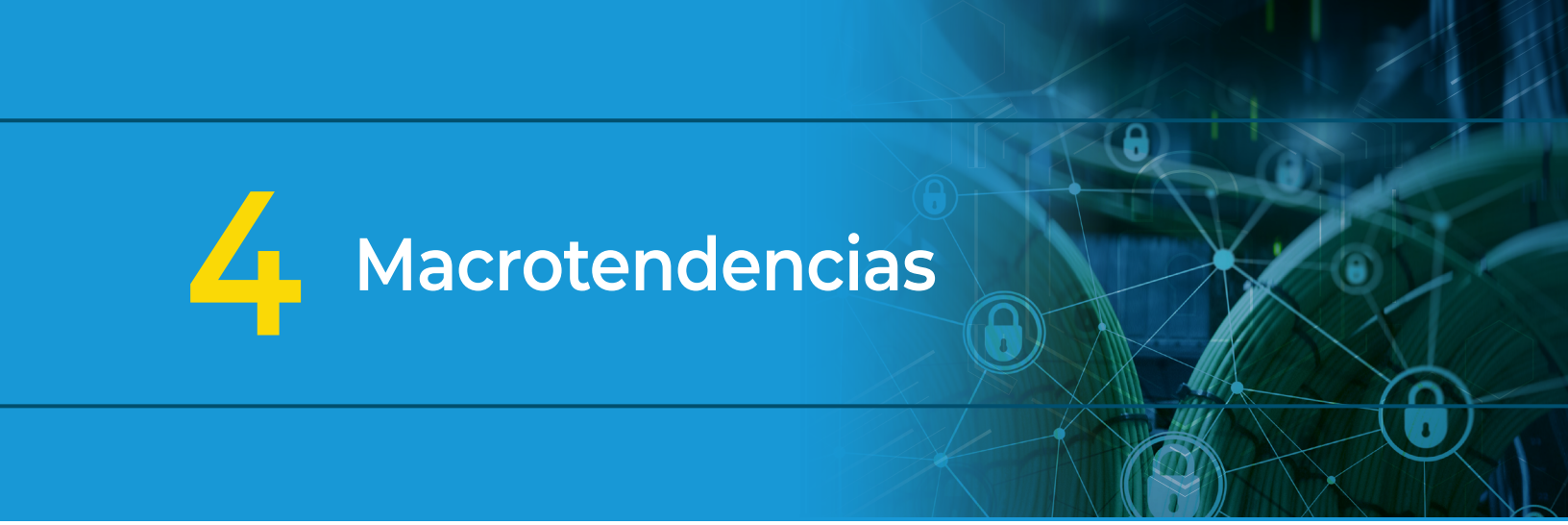
Debido a que el entorno digital evoluciona rápidamente, los países suelen actualizar sus estrategias de ciberseguridad cada cuatro o cinco años. Este ciclo de actualización responde a la necesidad de adaptación a las nuevas tecnologías, al surgimiento de nuevas amenazas y a la evolución del marco jurídico internacional. El ciberespacio es dinámico y aquello que pudo haber sido efectivo hace unos años hoy puede no serlo. Por lo tanto, es crucial que los países

[10] Guía para la elaboración de una estrategia nacional de ciberseguridad, 2021.

revisen y renueven sus estrategias de forma proactiva. Esperar a que una estrategia caduque para crear una nueva versión puede interrumpir los procesos evolutivos y provocar un estancamiento e, incluso, retrocesos en la evolución de la madurez cibernética del país. Es importante tener en cuenta que las acciones orientadas por una estrategia suelen ser la base sobre la cual se construyen los objetivos de su predecesora.

Dado que los países más avanzados en aspectos de ciberseguridad atravesaron un proceso evolutivo en el que las prioridades de las diferentes versiones de sus estrategias cambiaban a medida que se ejecutaban, investigar los pasos que diferentes países dieron en este recorrido puede generar lecciones de gran valor.

Por este motivo, un estudio comparativo de las estrategias nacionales de ciberseguridad permite identificar tendencias globales, evaluar la efectividad de las políticas implementadas en diferentes países, aprender de las mejores prácticas y fortalecer la cooperación internacional en materia de ciberseguridad. A través de este análisis, es posible obtener información valiosa sobre los desafíos comunes que enfrentan los países en el ámbito cibernético, así como sobre las soluciones más innovadoras y efectivas.



# 4 Macrotendencias

- **Las estrategias de la tercera generación son más operativas y menos teóricas en comparación con las de las generaciones anteriores**. Las estrategias de tercera generación definen con mayor claridad a los responsables de las acciones incluidas (63% frente al 26% de las de primera generación), están más vinculadas con el presupuesto[11] para la implementación de la estrategia (88% frente al 21% de las de primera generación), definen con mayor frecuencia un plan operativo[12] (75% frente al 37% de las de primera generación) y, en la medida de lo posible, incluyen más indicadores o métricas de éxito (25% frente al 0% de las de primera generación).
- **Las estrategias vigentes suelen incluir recomendaciones e iniciativas para mejorar los mecanismos de coordinación intragubernamentales y con el sector privado.** Aunque las medidas propuestas no siempre se pueden identificar de manera específica, se observa una preocupación constante por la existencia y el fortalecimiento de mecanismos de coordinación, ya sea dentro del sector público o del sector privado y académico.
- **Según lo observado, existe una tendencia de que las estrategias más recientes no se limiten a tratar únicamente la seguridad nacional, sino que también incluyan temas de prosperidad económica y promoción industrial**. Especialmente en los países del Norte Global, las estrategias de tercera generación tienden a incluir, con mayor frecuencia, principios (75%), objetivos (71%) o iniciativas destinadas a incentivar a la industria para generar oportunidades económicas (63%) por entender que el área de la ciberseguridad es un campo fértil para el desarrollo económico y social.
- **La protección de los derechos humanos y los derechos fundamentales es una constante en la mayoría de las estrategias, y suele ser el principio más frecuente.** De las estrategias vigentes analizadas que declaran sus principios, el 83% contiene algún principio relacionado con estos derechos.
- **Las iniciativas y los objetivos vinculados a la preparación y resiliencia, capacidades y sensibilización y cooperación internacional están presentes en prácticamente todas las estrategias.** En algunos casos, los temas se presentan como objetivos de alto nivel; en otros, como iniciativas o líneas de acción. Sin embargo, siempre hay una preocupación o una acción específica dirigida a estas cuestiones.

[11] Se consideraron tanto las estrategias que ya tienen un presupuesto definido en el documento publicado como aquellas que mencionan que la estrategia tendrá un presupuesto definido en la próxima etapa.

[12] Se consideraron tanto las estrategias que ya cuentan con un plan operativo en el documento publicado como aquellas que mencionan que se elaborará un plan de acción o un plan de implementación en la próxima etapa.

- **Las estrategias tienden a incluir una creciente preocupación por los ataques a la democracia.** Entre las amenazas que generan preocupación en las estrategias, se observa un aumento de la inclusión de amenazas cibernéticas que promueven ataques a la democracia. Esta tendencia se concentra en los países del Norte Global.
- **Se observa un aumento en los temas de transparencia y confianza en el ciberespacio en las estrategias de tercera generación.** Ya sea como principio o como área de interés, los temas de transparencia y confianza aparecen de manera más constante en las estrategias más recientes. Esto ilustra la posible tendencia de que el ciberespacio y su seguridad se traten, con mayor preocupación, como parte de este tema.
- **Las estrategias analizadas resaltan la necesidad de generar recursos humanos capaces de enfrentar los desafíos que impone la ciberseguridad.** Todas las versiones de las estrategias incluyen aspectos relacionados con la investigación y el desarrollo, la concientización y los estudios formales. Al mismo tiempo, hay una tendencia creciente de incorporar iniciativas relacionadas con medidas para aumentar la capacidad de los funcionarios públicos y promover la generación de profesionales en el sector privado.
- **La colaboración entre entidades o países para detectar incidentes y responder ante estos adquiere cada vez mayor importancia.** Esto se refleja en una mayor mención de iniciativas vinculadas al intercambio de información sobre incidentes y la cooperación entre los sectores público y privado.

# 5 Tendencias en perspectiva comparada

## 5.1. Estructura de las estrategias

### PUNTOS CLAVE DE LA SECCIÓN

- **Variedad en la estructura.** Las estrategias analizadas tienen estructuras muy diversas (documentos de 5 a 130 páginas, con estilos más teóricos u operativos, con plazos de vigencia definidos o indeterminados y con diferentes alcances y enfoques).
- **Componentes comunes.** A pesar de la variedad, las estrategias tienen componentes en común como parte de la estructura del documento.
  - El 94,7% incluye objetivos estratégicos.
  - El 63,2% incluye una sección de principios.
  - El 63,2% define una visión clara para el país.
- **Indicadores.** La mayoría de las estrategias no incluye indicadores o métricas de éxito asociadas (solo el 10,5% lo hace). Véase la sección *Indicadores y métricas* para más detalles.

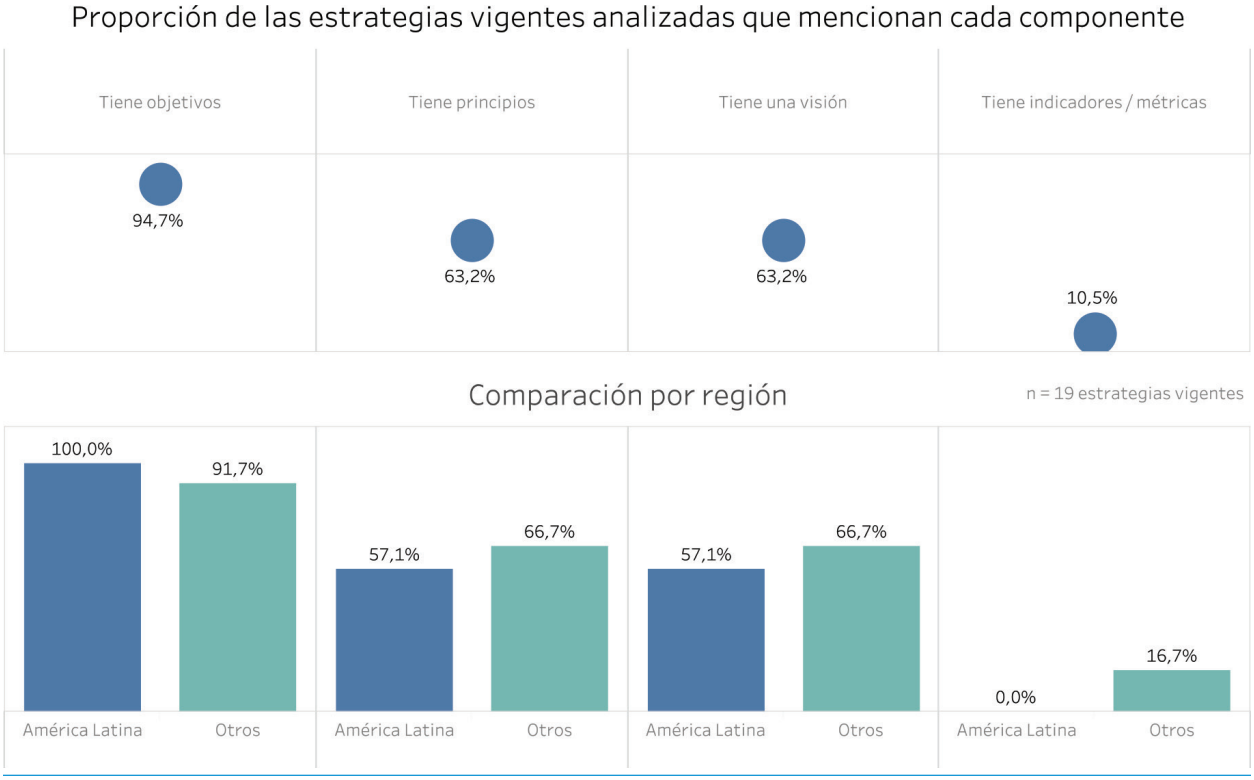
Como estos documentos varían en formato, extensión y propósito, comparar la estructura y la evolución de las estrategias a lo largo del tiempo es todo un desafío. Para ilustrar la amplitud de esta diversidad, basta con mencionar que la estrategia más breve analizada tiene solo cinco páginas,[13] mientras que la más extensa tiene 130 páginas.[14] La vigencia de las estrategias también varía. Algunas cubren un período de cuatro años, mientras que otras se extienden por diez años, y muchas no definen un marco temporal específico y permanecen vigentes hasta la elaboración de un nuevo documento.

Además, las estrategias también presentan estilos diversos. Algunas adoptan un enfoque más teórico y académico, mientras que otras optan por un enfoque más práctico y orientado a la acción y describen actividades específicas (este aspecto se explorará en más detalle en la sección que trata sobre gobernanza).

A pesar de esta heterogeneidad, es posible identificar componentes en común entre las diferentes estrategias (y que suelen ser usuales en los documentos de estrategias de otros ámbitos, no solo en ciberseguridad). Como consecuencia, y para posibilitar la comparación de las estructuras de la muestra analizada, se analizaron los documentos considerando cuatro categorías: presencia de objetivos estratégicos, inclusión de principios, enunciado explícito de una visión y uso de indicadores. En general, quedó claro que la definición de objetivos es casi universal, y solo una de las 19 estrategias vigentes analizadas no tiene objetivos claramente delineados. Además de los objetivos, alrededor de dos tercios de las estrategias

[13] Corresponde a la estrategia de Corea de 2011.
[14] Corresponde a la estrategia del Reino Unido de 2022.

## GRÁFICO 1 – ESTRUCTURA: COMPONENTES COMUNES ENTRE LAS ESTRATEGIAS




examinadas incorporan principios (véase la sección *Principios* para más detalles) y una visión definida con precisión. Con respecto a la presencia de indicadores, esta categoría es bastante menor, ya que solo dos de las estrategias vigentes incluyen algún tipo de indicador o métrica de éxito (véase la sección *Métricas e indicadores* para más detalles).

En el análisis por región, se observa que las estrategias analizadas del Norte Global se caracterizan por tener una presencia ligeramente mayor de secciones sobre principios y por poseer una visión definida con mayor frecuencia. Además, esta región incluye a los pocos países que cuentan con algún tipo de indicador o métrica para medir el éxito de la estrategia.

### RECUADRO 2 – MÁS DETALLES SOBRE LA ESTRUCTURA DE LAS VISIONES DE LAS ESTRATEGIAS

La visión debe ser una declaración clara de aquello que el Gobierno pretende lograr a través de la estrategia. Debe transmitir una aspiración e incluir una visión de futuro. Debe generar una expectativa compartida de los resultados y mencionar cómo estos contribuyen a objetivos más amplios. Es importante que presente una imagen convincente de la transformación esperada y que promueva el entendimiento compartido con todas las partes interesadas. Una visión clara puede motivar el trabajo en común de diferentes actores al permitir que todos comprendan los objetivos de la estrategia y cómo estos forman

*(continúa en la página siguiente)*

## RECUADRO 2 – MÁS DETALLES SOBRE LA ESTRUCTURA DE LAS VISIONES DE LAS ESTRATEGIAS *(continuación)*

parte de un proyecto más amplio. Por lo tanto, la visión debe ser ambiciosa, audaz e inspiradora, pero alcanzable dentro de un período realista. Cuanto más clara sea la visión, más convincente será la estrategia. A continuación, se presentan algunos ejemplos de cómo los países estructuraron sus visiones.

| País | Año | Visión |
|---|---|---|
| Estonia | 2014 | "Estonia tiene la capacidad de garantizar la seguridad nacional y promover el funcionamiento de una sociedad abierta, inclusiva y segura". |
| Reino Unido | 2011 | "Nuestra visión es que, en 2015, el Reino Unido obtenga un enorme valor económico y social de un ciberespacio vibrante, resiliente y seguro, en el cual nuestras acciones —guiadas por nuestros valores fundamentales de libertad, justicia, transparencia y Estado de derecho— aumenten la prosperidad y la seguridad nacional y fortalezcan a la sociedad". |
| Reino Unido | 2016 | "Nuestra visión para 2021 es que el Reino Unido sea seguro y resistente a las amenazas cibernéticas, próspero y confiable en el mundo digital". |
| Reino Unido | 2022 | "Nuestra visión es que, en 2030, el Reino Unido continúe siendo una potencia cibernética líder, responsable y democrática, capaz de proteger y promover nuestros intereses en el ciberespacio y a través de él, en consonancia con los objetivos nacionales". |
| Portugal | 2019 | "Que Portugal sea un país seguro y próspero mediante acciones innovadoras, inclusivas y resilientes, que preserve los valores fundamentales de un Estado de derecho democrático y garantice el buen funcionamiento de las instituciones frente a la evolución digital de la sociedad". |
| Nueva Zelanda | 2015 | "Nuestra visión es que Nueva Zelanda sea segura, resiliente y próspera en línea". |
| Nueva Zelanda | 2019 | "Esta estrategia tiene la visión de que Nueva Zelanda sea segura y confiable en el mundo digital para que el país pueda prosperar en línea". |
| Corea | 2019 | "Crear un ciberespacio libre y seguro para fortalecer la seguridad nacional, promover la prosperidad económica y contribuir a la paz internacional". |
| República Dominicana | 2022 | "Para 2030, la República Dominicana tendrá un ciberespacio más seguro, con las medidas necesarias para el desarrollo confiable de actividades productivas y recreativas para toda la población, dentro de un marco de respeto a los derechos fundamentales". |
| Israel | 2017 | "El Gobierno de Israel definió una visión para que el país se convierta en una nación líder en el aprovechamiento del ciberespacio como un mecanismo de crecimiento económico, bienestar social y seguridad nacional". |

Los ejemplos anteriores abordan las visiones de manera diferente. La mayoría de los países, como el Reino Unido, Portugal y Nueva Zelanda, destacan la importancia de la seguridad nacional y la resiliencia en el ciberespacio, además de la búsqueda de un entorno digital seguro y resistente a las amenazas. Algunos países, incluidos el Reino Unido, Estonia e Israel, reconocen al ciberespacio como un motor para la prosperidad económica. Comparten la visión de utilizar el ciberespacio para impulsar el crecimiento económico y el bienestar social.

Siempre en términos comparativos, algunos países hacen hincapié en valores fundamentales como la libertad, la justicia, la transparencia y el Estado de derecho como principios rectores de su accionar en el ciberespacio. Entre tanto, otros países aprovechan la visión para enfatizar su aspiración de ser una nación líder en el aprovechamiento del ciberespacio. Esto demuestra su ambición no solo por garantizar la seguridad y prosperidad internas, sino también por ejercer una influencia mundial en el ámbito cibernético.

## 5.2. Mecanismos de gobernanza presentes en las estrategias

### PUNTOS CLAVE DE LA SECCIÓN

- **Autoridad en cuestiones de ciberseguridad.** El 78,9% de las estrategias vigentes reconocen a una institución como responsable de las cuestiones de ciberseguridad (ya sea de forma general o como guardiana de la estrategia).
- **Responsables claros.** Si bien definen una autoridad, aproximadamente dos tercios de las estrategias vigentes analizadas no señalan claramente a los responsables de las acciones presentes en la estrategia.
- **Presupuesto.** El 47,4% de las estrategias tienen un presupuesto asociado, ya sea en la propia estrategia o previsto para un momento posterior.
- **Plan operativo.** El 63,2% de las estrategias tienen o prevén la creación de un plan operativo para su implementación.
- **Énfasis en la coordinación.** Más del 80% de las estrategias prevén algún mecanismo de coordinación, ya sea intragubernamental o con el sector privado. Las estrategias del Norte Global enfatizan más en la coordinación con el sector privado que las estrategias de América Latina.

En esta sección, se analizan las categorías relacionadas con la gobernanza e institucionalidad de las estrategias, con el objetivo de comprender qué mecanismos existen para implementar cada estrategia y cuál es la estructura de la organización para lograrlo.

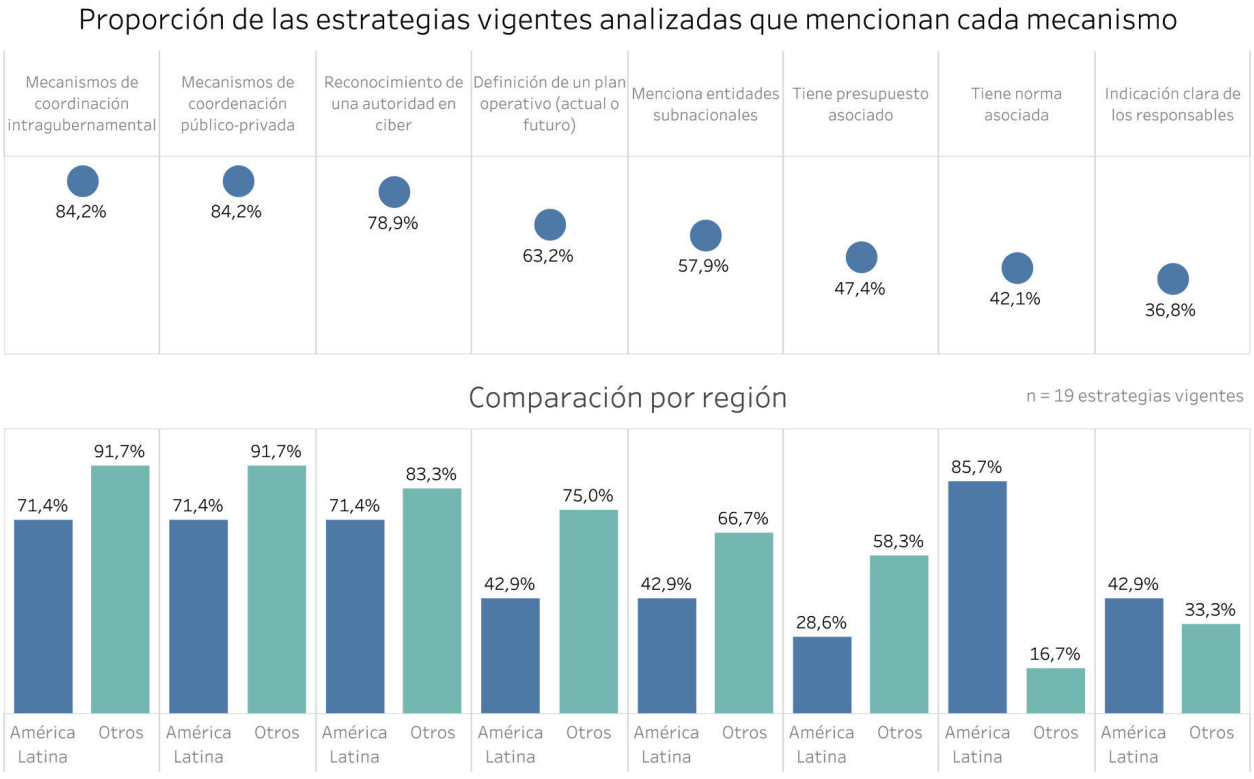
Algunos aspectos interesantes son el énfasis que la mayoría de las estrategias otorgan a la coordinación, ya sea dentro del propio Gobierno (el 84,2%[15] de las estrategias vigentes mencionan algún tipo de coordinación entre las agencias gubernamentales) o a través de una coordinación entre el sector público y el sector privado (el 84,2%[16] de las estrategias vigentes mencionan algún tipo de coordinación entre ambos sectores). Además de los mecanismos de coordinación, también se destaca que cerca del 78,9% reconoce a algún organismo como autoridad en cuestiones de ciberseguridad, ya sea de forma general o específica para liderar la implementación de la estrategia.

En términos comparativos, el análisis de las 19 estrategias vigentes en la actualidad y que formaron parte de la muestra seleccionada indica que no es muy común que las estrategias informen el monto del presupuesto asignado. Sin embargo, casi la mitad de las estrategias mencionan explícitamente el presupuesto destinado o aclaran que se determinará el presupuesto en el futuro, lo cual implica una preocupación con respecto al financiamiento y a la ejecución exitosa de las iniciativas del documento. Aunque no significa que la mitad de las estrategias carezcan necesariamente de presupuesto (ya que este análisis se limitó a la lectura de las estrategias sin profundizar en los presupuestos públicos de los países seleccionados), esta tendencia sugiere que podría ser el caso para aproximadamente la mitad de ellas.

Dado que ninguna estrategia se autofinancia, es fundamental que se definan los recursos que se utilizarán para garantizar la ejecución de las iniciativas mencionadas en el documento y cómo se desarrollará el proceso. Por ejemplo, se pueden considerar únicamente iniciativas que estén incluidas en el presupuesto de cada institución gubernamental o bien, asignar

[15] Aquí se consideraron las menciones a mecanismos específicos de coordinación (por ejemplo, consejos, comités, etc.), así como las menciones más genéricas (por ejemplo, acciones en el futuro para aumentar la coordinación o el reconocimiento explícito de la necesidad de coordinación).
[16] Ídem.

## GRÁFICO 2 – ÁREA DE INTERÉS: GOBERNANZA E INSTITUCIONALIDAD




un presupuesto especial a las iniciativas mencionadas en la estrategia. Cualquiera sea el modelo que elija un país, es fundamental garantizar que las iniciativas contempladas en la estrategia cuenten con los recursos necesarios para una adecuada implementación.

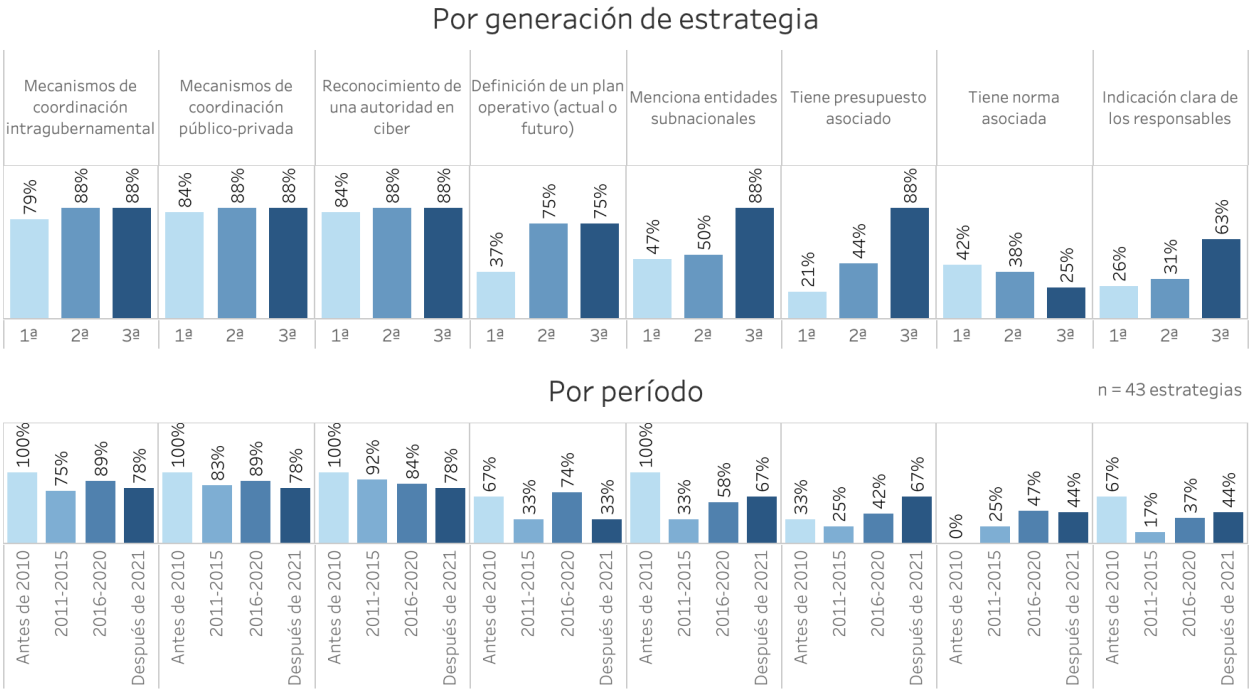
El análisis por región indica que los países de América Latina presentan una mayor tendencia a vincular sus estrategias a alguna normativa (decreto, ordenanza, resolución o demás). Esto indica que la preocupación por la coordinación intragubernamental o con el sector privado está presente en menor escala que en los países del Norte Global. También es posible observar que las estrategias de América Latina asignan un presupuesto menor que las estrategias del Norte Global; esto implica una potencial oportunidad para el fortalecimiento de las estrategias de la región.

Se observan algunos patrones interesantes al analizar la evolución de las estrategias (gráfico 3). En primer lugar, se advierte que las estrategias de tercera generación tienden a definir un plan operativo (ya sea como parte de la propia estrategia o porque está previsto para la fase de implementación); esto indica que las estrategias más recientes tienden a ser menos teóricas y más orientadas a acciones concretas. En relación con este punto, también se advierte un enorme avance en la tercera generación de estrategias con respecto a la definición clara de los responsables de cada acción. De hecho, el 63% de las estrategias de tercera generación define con mayor claridad quién es responsable de las acciones referidas en el plan, mientras que solo el 31% de las estrategias de segunda generación refiere este dato.

En el análisis evolutivo, se observa que, en las estrategias de tercera generación, existe una mayor tendencia a contar con un presupuesto asociado (el porcentaje de estrategias con

## GRÁFICO 3 – EVOLUCIÓN DEL ÁREA DE INTERÉS: GOBERNANZA E INSTITUCIONALIDAD

Evolución de la presencia de los mecanismos en las estrategias analizadas




presupuesto aumentó de 21% en las estrategias de primera generación a 88% en las de tercera generación). Este aspecto también refuerza la percepción indicada en la sección *Macrotendencias* de que las estrategias son cada vez más operativas y ejecutivas y menos teóricas.

En cuanto a los mecanismos asociados para la aplicación de la ley, las estrategias no suelen incluir obligaciones o sanciones por incumplimiento. En general, el lenguaje de las estrategias adquiere un carácter más orientador, y se definen líneas de acción, prioridades, objetivos y recomendaciones. Al mismo tiempo, muchas estrategias indican que se crearán mecanismos para su implementación, por ejemplo, se definirán personas de referencia en cada departamento, se establecerá la obligatoriedad de realizar supervisiones anuales, se formarán comités para el seguimiento de la implementación, entre otros.

### RECUADRO 3 – MAYORES DETALLES DEL ÁREA DE INTERÉS

#### La gobernanza en la estrategia de Estonia (2019)

La tercera estrategia de Estonia, actualmente en vigencia, presenta un interesante modelo de gobernanza que incorpora mecanismos de coordinación entre secretarías y de colaboración con el sector privado y la sociedad civil.

Es importante destacar que el proceso de elaboración de la estrategia fue participativo y contó con la participación de organismos gubernamentales, del ámbito académico, de laboratorios de ideas

*(continúa en la página siguiente)*

**RECUADRO 3 – MAYORES DETALLES DEL ÁREA DE INTERÉS** *(continuación)*

y del sector privado. Este tipo de procesos es de ayuda en la fase de implementación, una vez que los diferentes actores ya se apropiaron de los contenidos y objetivos del documento.

El Ministerio de Asuntos Económicos y Comunicaciones coordina la planificación de la política de ciberseguridad y la implementación de la estrategia. Este ministerio también es responsable de las cuestiones de gobierno digital y la transformación digital del sector público. A nivel estratégico, la coordinación se realiza a través del Consejo de Ciberseguridad del Comité de Seguridad del Gobierno de la República, que garantiza la implementación de los objetivos de la estrategia a través de documentos de planificación, programas y planes de trabajo elaborados en conjunto con las instituciones gubernamentales responsables. Por lo tanto, las instituciones gubernamentales que forman parte del Consejo son las principales responsables de implementar la estrategia.

Para ejecutar de forma coordinada los objetivos acordados en la estrategia, se designa una persona de referencia en cada ministerio u organismo. Esta actúa como enlace para las cuestiones relacionadas con la garantía de la ciberseguridad nacional en su respectiva área. Asimismo, garantiza que se pongan en práctica las prioridades pautadas en la estrategia y respaldadas en los documentos de planificación del respectivo departamento. El Ministerio de Asuntos Económicos y Comunicaciones se encarga de coordinar la cooperación y el intercambio de información entre los responsables.

Una vez al año, el Comité de Seguridad del Gobierno de la República aprueba el informe consolidado sobre las actividades de cada organismo en el ámbito de la ciberseguridad con el fin de compartir con la sociedad y el Gobierno una visión panorámica de las actividades que se realizaron en el marco de la estrategia.

Además de la gobernanza en el ámbito gubernamental, la estrategia también traza un plan para la cooperación con los centros de competencia, las universidades, las instituciones de investigación y los socios del sector privado que tienen conocimientos y capacidades en este campo. Entre estos se destacan el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE, por sus siglas en inglés) de la Organización del Tratado del Atlántico Norte (OTAN) y la e-Governance Academy (EGA, por sus siglas en inglés), un centro de consulta y reflexión sobre la información para la sociedad. La estrategia también menciona a otros socios para el intercambio de conocimientos y experiencia.

## 5.3. Métricas e indicadores

**PUNTOS CLAVE DE LA SECCIÓN**

- **Presencia incipiente de indicadores.** Entre las estrategias vigentes en la actualidad, solo dos cuentan con algún tipo de indicador cuantitativo y/o métricas de éxito. Al ampliar el análisis para considerar la evolución de la presencia de indicadores entre las 43 estrategias analizadas, además de las vigentes ya mencionadas, solo otras dos cuentan con algún tipo de métrica de éxito.

Además de los principales elementos que garantizan una gobernanza efectiva, la literatura enfatiza la importancia de los mecanismos de supervisión de las estrategias. Establecer estos mecanismos, junto con indicadores clave de rendimiento u otras medidas de evaluación, es importante para la implementación exitosa de las estrategias. Sin embargo, a pesar de la importancia de que las estrategias cuenten con indicadores y formas de supervisión, el análisis realizado permitió constatar que la presencia de indicadores o métricas de éxito en las estrategias es muy incipiente. De las 19 estrategias vigentes, solo dos presentan indicadores (Estonia, 2019 y Francia, 2021). Al ampliar el análisis para incluir las estrategias antiguas, también se observan dos estrategias de segunda

generación que tienen métricas cualitativas de éxito (Reino Unido, 2016 y Australia, 2020).

Cabe destacar que algunas estrategias mencionan que los indicadores y mecanismos de supervisión se definirán en una etapa posterior, lo cual prevé, por ejemplo, la elaboración de un plan de acción para implementar la estrategia. Estos documentos adicionales no entraron en el ámbito del análisis.

En esta sección, se analizarán con más detalle los indicadores presentes en la estrategia de tercera generación de Estonia (2019), la estrategia de tercera generación de Francia (2021) y la estrategia de segunda estrategia del Reino Unido (2016). Dado que Estonia es un referente en el tema y pionera en la publicación de las estrategias, se entiende que, aunque todavía no se refleje en los datos, el hecho de que esta estrategia mencione explícitamente los indicadores puede marcar una tendencia a que otros países también los publiquen en sus futuros documentos.

A continuación, se presenta un resumen de los tipos de indicadores incluidos en la estrategia mencionada. Existen dos tipos de indicadores: los indicadores de impacto, que están vinculados transversalmente a la estrategia, y los indicadores de desempeño, que están vinculados a cada objetivo.

Entre los indicadores de impacto supervisados en la estrategia se destacan:

- el porcentaje de residentes que evitan la comunicación electrónica con el sector público o con proveedores de servicios para evitar riesgos de seguridad, y
- el porcentaje de usuarios con una identidad digital segura.

En cuanto a los indicadores de rendimiento, algunos pueden servir de inspiración para el desarrollo de nuevas estrategias:

- número total de servicios abiertos en la red del Estado;
- volumen de exportaciones de las empresas del sector;
- número de nuevas empresas emergentes (*startups*) en el sector de la ciberseguridad;
- cantidad de tesis doctorales concluidas y defendidas en el área de ciberseguridad;
- porcentaje de usuarios que experimentaron pérdidas por estar expuestos a alguna vulnerabilidad en línea;
- porcentaje de empresas que utilizan una política oficial de seguridad de las Tecnologías de la Información y las Comunicaciones (TIC);
- nivel de concientización y competencias en ciberseguridad entre los empleados del sector público;
- déficit de fuerza de trabajo en el sector.

El caso de la estrategia de 2021 de Francia es interesante, ya que se trata de una estrategia muy centrada en el aspecto económico de la ciberseguridad. Esto refleja, una vez más, la tendencia de que las estrategias más nuevas del Norte Global incluyen, con mayor frecuencia, los temas de prosperidad económica. Aunque no sean indicadores de supervisión de la estrategia específicamente, se destacan porque incluyen metas que orientan la estrategia. Entre estas sobresalen: triplicar las ventas en el sector de la ciberseguridad, duplicar el número de empleos en el sector y aumentar un 20% el número de patentes registradas, entre otras.

También es interesante el enfoque cualitativo de las métricas de éxito adoptado en la estrategia del Reino Unido, ya que materializa lo que se entiende como el éxito de la implementación de la estrategia. En este caso, la estrategia define los resultados estratégicos esperados y las mediciones que indican si se alcanzan los resultados. Sin embargo, se entiende que este formato dificulta la supervisión más objetiva del logro de los resultados esperados. A continuación, se incluyen algunos ejemplos de cómo se utiliza este enfoque.

- Resultado esperado: el Reino Unido tiene la capacidad de gestionar y responder eficazmente a incidentes cibernéticos a fin de reducir el daño causado al país y combatir a los adversarios cibernéticos.
- Indicadores de éxito:
  - mayor número de denuncias de incidentes a las autoridades, lo cual permite desarrollar una mejor comprensión del tamaño y la escala de la amenaza;
  - gestión más efectiva, eficiente e integral de los incidentes cibernéticos después de la creación del Centro Nacional de Ciberseguridad (National Cyber Security Centre [NCSC]) como mecanismo centralizado de notificación y respuesta a incidentes;
  - reducción en la ocurrencia de ataques reiterados en víctimas y sectores.

## 5.4. Desafíos y amenazas

### PUNTOS CLAVE DE LA SECCIÓN

- **Componente de amenazas y desafíos.** Las estrategias suelen incluir —en su contexto— alguna sección o capítulo dedicado a los tipos de amenazas y desafíos relacionados con la ciberseguridad.
- **Tipos comunes de amenazas.** Entre los tipos de amenazas más comunes mencionados en los documentos se destacan: (i) ciberdelitos (84,2%); (ii) ciberguerra o ataques de otros países (57,9%); (iii) terrorismo (57,9%), y (iv) espionaje (42,1%).
- **Evolución de los tipos de amenazas.** Se percibe una disminución en el enfoque en los ataques terroristas y un aumento de nuevas amenazas, como los ataques a la democracia.
- **Ataques a la democracia.** La tendencia a incluir los ataques a la democracia como una amenaza en el ciberespacio crece entre las estrategias de tercera generación de los países del Norte Global.

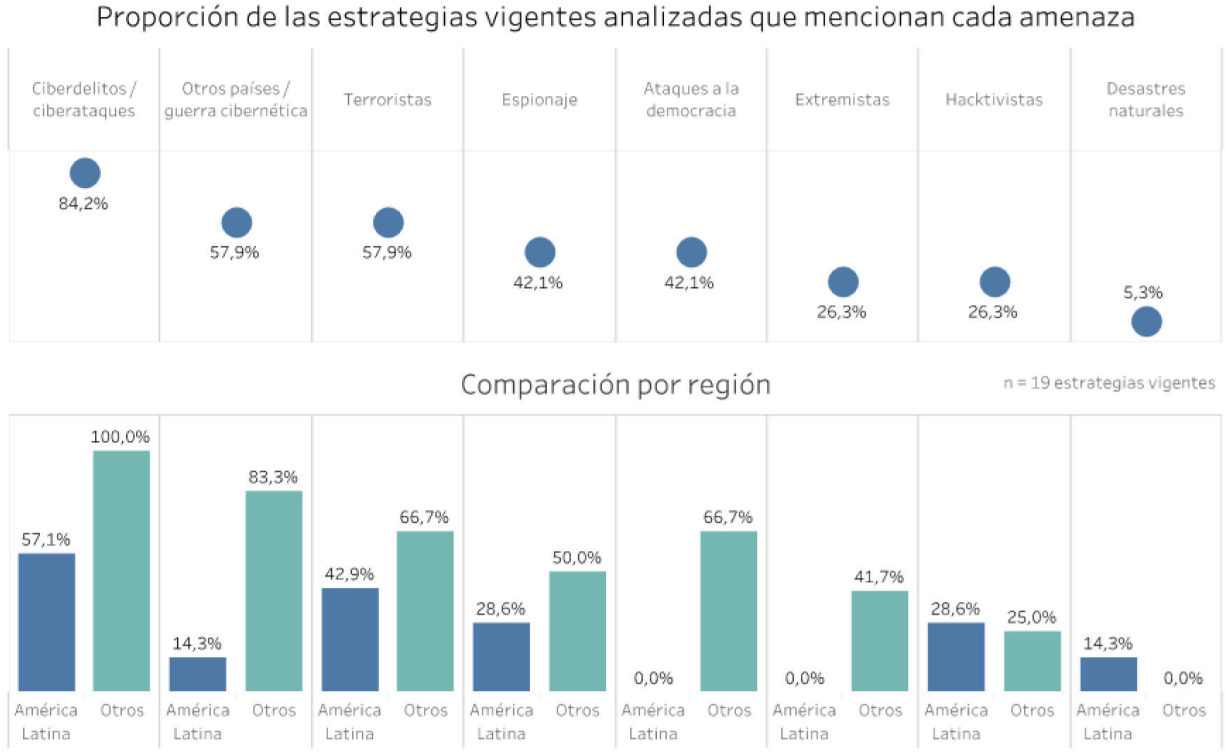
Es muy común que las estrategias de ciberseguridad incluyan alguna sección o capítulo dedicado a exponer cuáles son los tipos de amenazas y desafíos que enfrenta el país en esa área. En cierto modo, la estrategia surge precisamente como respuesta a esos tipos de amenazas. En algunas ocasiones, los distintos tipos de amenazas adquieren un sentido muy real; por ejemplo, la primera estrategia de Estonia (2008) surgió como respuesta al ataque masivo que el país había sufrido en 2007. En otros casos, se trata de identificar las principales categorías de riesgos asociados, con el fin de garantizar que las iniciativas incluidas en la estrategia puedan hacer frente a dichas amenazas.

Como se ilustra en el gráfico 4, entre los tipos de amenazas más frecuentes, se destaca que el 84,2% de las estrategias analizadas citan ciberdelitos y, alrededor del 60%, mencionan ataques de otros países (o ciberguerra) como amenazas recurrentes. Luego, cuestiones de terrorismo y espionaje ocupan el tercer y cuarto puesto entre las amenazas identificadas con mayor frecuencia.

En la comparación regional, se pueden inferir algunos patrones interesantes. La primera reflexión es que, en comparación con las estrategias de América Latina y el Caribe, las estrategias del Norte Global de la muestra incluyen, con mayor frecuencia, un resumen de las amenazas. El segundo punto es que, incluso entre las estrategias que mencionan a las categorías de amenazas, algunos tipos parecen ser más frecuentes en las estrategias fuera de la región de América Latina, lo cual podría explicarse por factores geopolíticos, por ejemplo. En este sentido, se destaca cómo la amenaza creada por otros países, el terrorismo y los ataques a la democracia tienen mayor presencia en estrategias fuera del continente americano.

El gráfico 5 muestra la evolución de la mención de los tipos de amenazas a lo largo del tiempo y por generación. Esta serie comparativa permite identificar patrones interesantes vinculados a hechos históricos y geopolíticos. Por ejemplo, se destaca la disminución gradual de las estrategias

## GRÁFICO 4 – TIPOS DE AMENAZAS IDENTIFICADOS



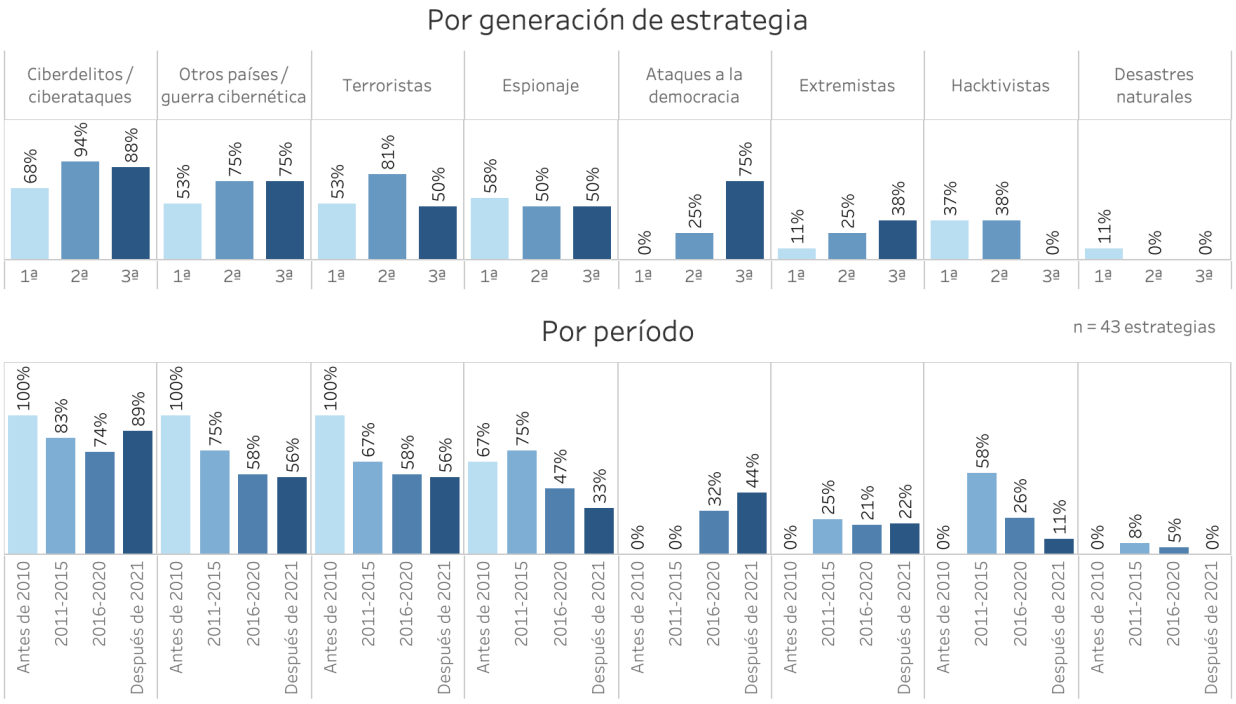

que citan explícitamente a los terroristas como la principal amenaza que enfrenta un país en materia de ciberseguridad (el auge de este tipo de amenaza fue antes de 2015). Otro dato interesante es el marcado crecimiento de las amenazas centradas en los ataques a la democracia en la tercera generación de estrategias. Esto indica una posible tendencia para los próximos años. Casos como la injerencia rusa en las elecciones estadounidenses y otros episodios de este tipo pueden ser la raíz de este aumento reciente.

En cuanto a los desafíos del área de ciberseguridad, no fue posible efectuar una categorización estándar para llevar a cabo un análisis comparado. Esto se debió a que, muchas veces, los desafíos mencionados estaban vinculados a contextos específicos o se abordaban de forma fragmentada en las estrategias, sin una sección dedicada que permitiera extraer datos de manera uniforme en todas las estrategias de la muestra seleccionada.

A pesar de esta diversidad, es importante destacar que algunos desafíos son recurrentes en varias de las estrategias analizadas. Entre los desafíos que comparten prácticamente todos los países, se encuentran el crecimiento exponencial de la tecnología y el aumento de la conectividad, con la consecuente expansión del ciberespacio. Además del tamaño del ciberespacio, muchas estrategias mencionan como principal desafío la creciente dependencia de la sociedad en el ciberespacio. En este sentido, las estrategias más modernas enfatizan cómo los ciberataques, cada vez más, representan ataques a la forma de vida y a los valores sociales. De igual forma, muchas de las estrategias mencionan las amenazas y los desafíos relacionados con la protección de la infraestructura crítica y los servicios esenciales. También es común citar desafíos y riesgos asociados a la mayor digitalización de los servicios públicos.

## GRÁFICO 5 – EVOLUCIÓN DE LOS TIPOS DE AMENAZAS IDENTIFICADOS

Evolución de la presencia de los tipos de amenaza en las estrategias analizadas




Asimismo, algunas estrategias abordan desafíos más específicos con mayor detalle. Una cuestión a destacar es la falta de oferta de profesionales de ciberseguridad calificados en los países, lo cual indica un déficit de este tipo de profesional. Esto resalta la urgencia de que las estrategias incluyan también iniciativas para mejorar la situación. Las medidas priorizadas se explorarán en la sección que trata sobre las capacidades.

Por último, y también dentro del amplio alcance de los desafíos mencionados, vale la pena recordar que algunas estrategias —en general, las del Norte Global— señalan los cambios geopolíticos como un gran desafío para las cuestiones de ciberseguridad. El desafío de la naturaleza transnacional del ciberespacio también está muy presente, lo cual indica que es imposible que las estrategias no consideren las iniciativas para fortalecer el ciberespacio más allá de sus fronteras nacionales. El tema de la cooperación internacional se detallará en la sección correspondiente.

### RECUADRO 4 – ESTUDIO DE CASO

#### LAS ESTRATEGIAS DE CIBERSEGURIDAD EN ESPAÑA Y SU ESQUEMA DE SEGURIDAD NACIONAL

A pesar de no haber sido uno de los primeros países en contar con una estrategia de ciberseguridad, España desarrolló su primera estrategia antes que la mayoría de los países estudiados (2013) y lanzó su segunda versión en 2019. Si bien ambas estrategias tienen muchos puntos destacados, dos conceptos son objeto de un debate interesante: (i) la generación de una estructura común para la gestión de

*(continúa en la página siguiente)*

**RECUADRO 4 – ESTUDIO DE CASO** *(continuación)*

la ciberseguridad en todo el Estado y (ii) la definición, desde el inicio, de una estructura organizacional que promueva los objetivos de las estrategias.

El Esquema de Seguridad Nacional es un marco común de principios básicos, requisitos y medidas de seguridad para la protección adecuada de la información procesada y los servicios prestados por la Administración pública y sus proveedores. Su definición comenzó antes del lanzamiento de la primera estrategia de seguridad nacional, pero fue en esa estrategia donde se estableció como una línea de acción específica. El marco también mantuvo su papel clave en la segunda versión de la estrategia. Su constante evolución, la definición de normativas y el desarrollo de un ecosistema público-privado proporcionaron a España una herramienta que permite el establecimiento de requisitos mínimos de seguridad medibles y auditables, los cuales —a su vez— permiten mejorar la ciberseguridad en todo el país.

En su primera estrategia, España dedica un capítulo completo a la definición de una estructura organizativa para la ciberseguridad, destinada a promover los objetivos definidos. En busca de una visión integral de la ciberseguridad y, en consonancia con los principios del Sistema de Seguridad Nacional, la estrategia define la creación de dos comités en el ámbito del Consejo de Seguridad Nacional: uno especializado en ciberseguridad y otro, en consciencia situacional. El primero promoverá la coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad, mientras que el segundo será responsable de administrar situaciones de crisis en este ámbito. En la segunda versión de la estrategia, se amplía esta estructura y se sustituye el comité de ciberseguridad por una nueva estructura liderada por el Consejo Nacional de Ciberseguridad. Este consejo está compuesto por tres entidades: el Foro Nacional de Ciberseguridad, la Comisión Permanente de Ciberseguridad, y una tercera formada por las autoridades públicas competentes en el ámbito de la seguridad de las redes, los sistemas de información y los equipos de respuesta ante emergencias informáticas (CSIRT, por sus siglas en inglés) de referencia nacional.

Tanto el Esquema de Seguridad Nacional como la definición temprana de una estructura organizativa son ejemplos de acciones que tuvieron una relación directa con el aumento de la madurez de la ciberseguridad en España. No solo porque se implementaron en el momento oportuno, sino también por su constante evolución a lo largo del tiempo.

*Fuente:* Estrategias de ciberseguridad de España.

## 5.5. Principios

### PUNTOS CLAVE DE LA SECCIÓN

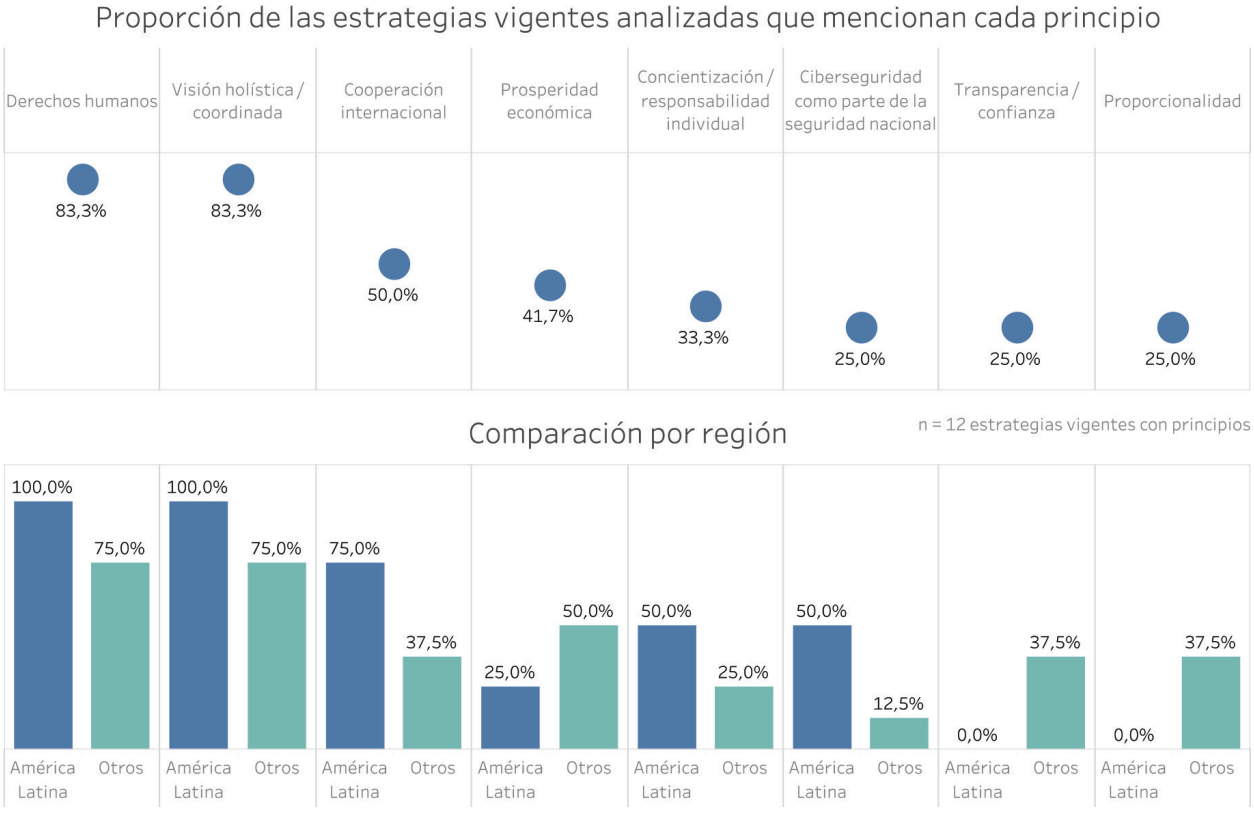
- **Principios.** Alrededor de dos tercios de las estrategias analizadas tienen una sección donde comparten sus principios.
- **Derechos humanos.** El principio más común, citado en el 83,3% de las estrategias vigentes, se refiere a cuestiones relacionadas con los derechos humanos o la protección de los derechos fundamentales.
- **Prosperidad económica.** Se observa una tendencia a mencionar cada vez más los principios relacionados con la prosperidad económica, principalmente fuera de América Latina. Esto indica una posible tendencia a que las estrategias enfaticen temas de economía y promoción industrial, además de los temas más clásicos de seguridad nacional.
- **Transparencia y confianza.** También se destaca el aumento significativo de los principios relacionados con la transparencia en las estrategias de tercera generación.

No existe un consenso entre todos los actores sobre qué engloba el concepto de ciberseguridad. Como consecuencia, las estrategias suelen incluir principios fundamentales para orientar a los formuladores de políticas y garantizar que todas las partes interesadas tengan un entendimiento común de aquello que se espera. Los principios son un conjunto de lineamientos que informan y apoyan la forma en que debe abordarse transversalmente la ciberseguridad. En términos generales, proporcionan una referencia sólida, pero flexible que permite orientar las decisiones sobre estos temas.

Como se demuestra en la sección sobre la estructura de las estrategias, alrededor de dos tercios incluyen una sección dedicada a los principios. En cuanto al formato, las estrategias utilizan diferentes niveles de detalles en sus principios, desde palabras aisladas hasta frases completas que incorporan lineamientos estratégicos. Los gráficos 6 y 7 destacan los temas de los principios más comunes que se encuentran en las estrategias analizadas, así como su evolución a lo largo del tiempo.

Es fundamental resaltar que no se pueden sacar conclusiones apresuradas basándose en estos patrones. El hecho de que un principio específico gane o pierda protagonismo con el tiempo no implica, necesariamente, que el tema asociado se haya vuelto más o menos importante en la estrategia del país. Por ejemplo, se puede observar una disminución de las referencias a principios de cooperación internacional en las estrategias más recientes o en las estrategias de tercera generación. Sin embargo, es importante observar que la cooperación internacional sigue siendo un tema recurrente en todas las estrategias. Este hecho puede indicar que, en las primeras

**GRÁFICO 6 – TIPOS DE PRINCIPIOS**



estrategias, el tema se planteaba de manera transversal como principio, pero que ahora existe una tendencia a que el tema se trate como un objetivo estratégico con iniciativas asociadas.

La hipótesis planteada aquí es que los temas aparecen como principios cuando los países aún no tienen claro cómo será su operación en la práctica (y cómo traducirlos en objetivos o acciones concretas), pero sí quieren demostrar que los consideran importantes y transversales. Cuando hay mayor claridad sobre cómo se efectuará la implementación, los temas presentes en los principios se convierten en objetivos con mayores posibilidades de concretarse.

Entre los principios que predominan en las estrategias, se destaca de manera significativa el tema de los derechos humanos y los derechos fundamentales. A pesar de que las diferentes estrategias pueden abordarlo de diversas maneras, se observa que el 83,3% de las estrategias vigentes incorporan algún principio relacionado con esta cuestión. Cabe observar que todas las estrategias en América Latina incluyen dicho principio. A continuación, se presentan algunos ejemplos ilustrativos.

- La protección y la promoción de los derechos y libertades fundamentales son importantes tanto en el ciberespacio como en el entorno físico (Estonia, 2019).
- Se protegerán y promoverán rigurosamente los valores fundamentales del Reino Unido. Estos valores incluyen la democracia, el Estado de derecho, la libertad, las instituciones y los gobiernos abiertos y responsables, los derechos humanos y la libertad de expresión (Reino Unido, 2016).
- Equilibrio entre los derechos individuales y la ciberseguridad: lograr un equilibrio entre la protección del ciberespacio y la salvaguardia de los derechos fundamentales de las personas, por ejemplo, la privacidad (Corea, 2019).
- Respeto por los derechos y las libertades individuales: la protección de los individuos en el ámbito de la ciberseguridad debe considerar el respeto a los derechos y las libertades individuales consagrados en la Constitución Nacional y en los tratados internacionales de los que es signataria la República Argentina (Argentina, 2019).

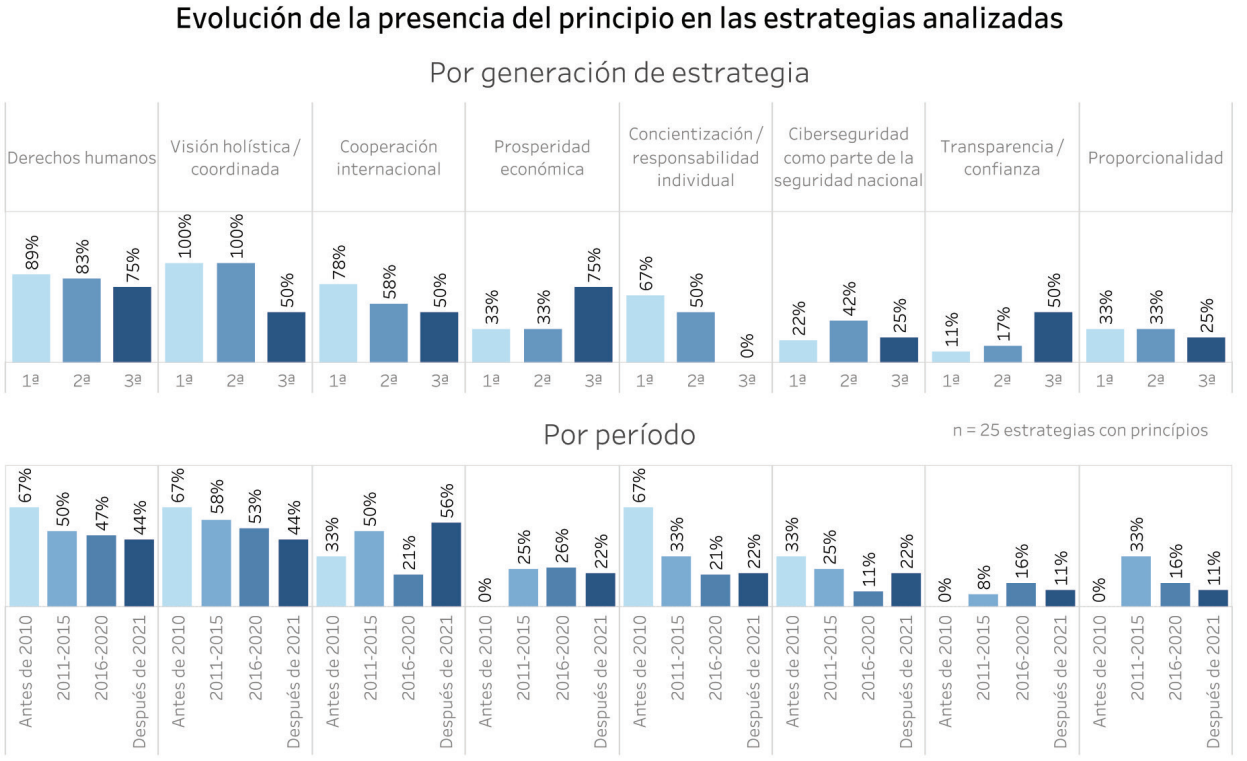
Otro punto para destacar es que el 83,3% de las estrategias vigentes incorporan algún tipo de principio que enfatiza la necesidad de coordinación o que considera la ciberseguridad como un tema holístico e interconectado. En determinados casos, dicha coordinación se menciona en relación con diferentes actores, tanto del sector privado como del público. En otros casos, se destaca la importancia de no segmentar la ciberseguridad en una categoría aislada, separada de los demás temas de seguridad o transformación digital. A continuación, se incluyen algunos ejemplos.

- El trabajo será en conjunto. Es posible proteger con éxito al Reino Unido en el ciberespacio solo si se trabaja con las administraciones descentralizadas, todas las partes del sector público, las empresas, las instituciones y los ciudadanos individuales (Reino Unido, 2016).
- Asegurar que la responsabilidad sea compartida entre varias partes interesadas para promover la máxima colaboración y cooperación, teniendo en cuenta la función y el grado de responsabilidad de cada parte para gestionar los riesgos de seguridad digital y proteger el entorno digital (Colombia, 2016).

Al observar los patrones de evolución de los principios (gráfico 7), algunos puntos llaman la atención y pueden dar indicios sobre las tendencias recientes en la evolución de las estrategias.

Un punto que vale la pena destacar es el principio de prosperidad económica. Se observa que existe un patrón claro en las distintas

## GRÁFICO 7 – EVOLUCIÓN DE LOS TIPOS DE PRINCIPIOS IDENTIFICADOS




generaciones de estrategias. Mientras que en las primeras era menos común hablar de prosperidad económica, el 75% de las estrategias de la tercera generación incluyen un principio relacionado con el tema. Este dato puede indicar la tendencia de que las estrategias más recientes no se centren exclusivamente en la seguridad nacional o la protección, sino que amplíen el alcance y el ámbito para incorporar temas relacionados con la promoción industrial y otros.

Asimismo, es interesante observar que América Latina aún no enfatiza este aspecto en sus estrategias. Solo una de cada cuatro estrategias de la muestra de la región destaca claramente la prosperidad económica como el principio rector del documento. Esto indica un área potencial de crecimiento y desarrollo para futuras políticas y estrategias en la región. Los siguientes ejemplos ilustran cómo este principio se manifiesta en algunas estrategias.

- La ciberseguridad se considera un elemento facilitador y amplificador del rápido desarrollo digital de Estonia, que es la base del crecimiento socioeconómico del país. La seguridad debe apoyar la innovación, y esta, a su vez, debe apoyar la seguridad (Estonia, 2019).
- La capacidad de los ciudadanos y de las empresas para operar en el ciberespacio de manera segura y protegida será una prioridad. El objetivo es que puedan maximizar los beneficios económicos y sociales de la tecnología digital y ejercer sus derechos legales y democráticos (Reino Unido, 2022).
- Incentivo a la ciberseguridad para los negocios, el crecimiento económico y la prosperidad (Canadá, 2018).

Otro patrón interesante que se destaca es la disminución, a lo largo del tiempo y de las

generaciones de estrategias, del principio relacionado con la concientización general de la población o el énfasis en la responsabilidad individual en cuestiones de ciberseguridad. Al igual que con el tema de la cooperación internacional, esta disminución no indica que el tema haya dejado de ser una cuestión central de las estrategias. Según los datos de la sección sobre capacidades, casi todas las estrategias vigentes de la muestra tienen al menos una medida relacionada con programas de concientización. Esto indica que el tema pasó de ser un principio transversal a considerarse un área de interés con acciones específicas.

Por último, cabe destacar el crecimiento del principio de transparencia en las estrategias de tercera generación. Este principio indica que es cada vez más necesario que las políticas de ciberseguridad incorporen la transparencia y se centren en aumentar la confianza en el ciberespacio. Ese aumento en la importancia que se le atribuye a la transparencia sugiere un cambio en los enfoques anteriores, lo cual indica una tendencia general hacia políticas de ciberseguridad más abiertas.

## 5.6. Objetivos estratégicos

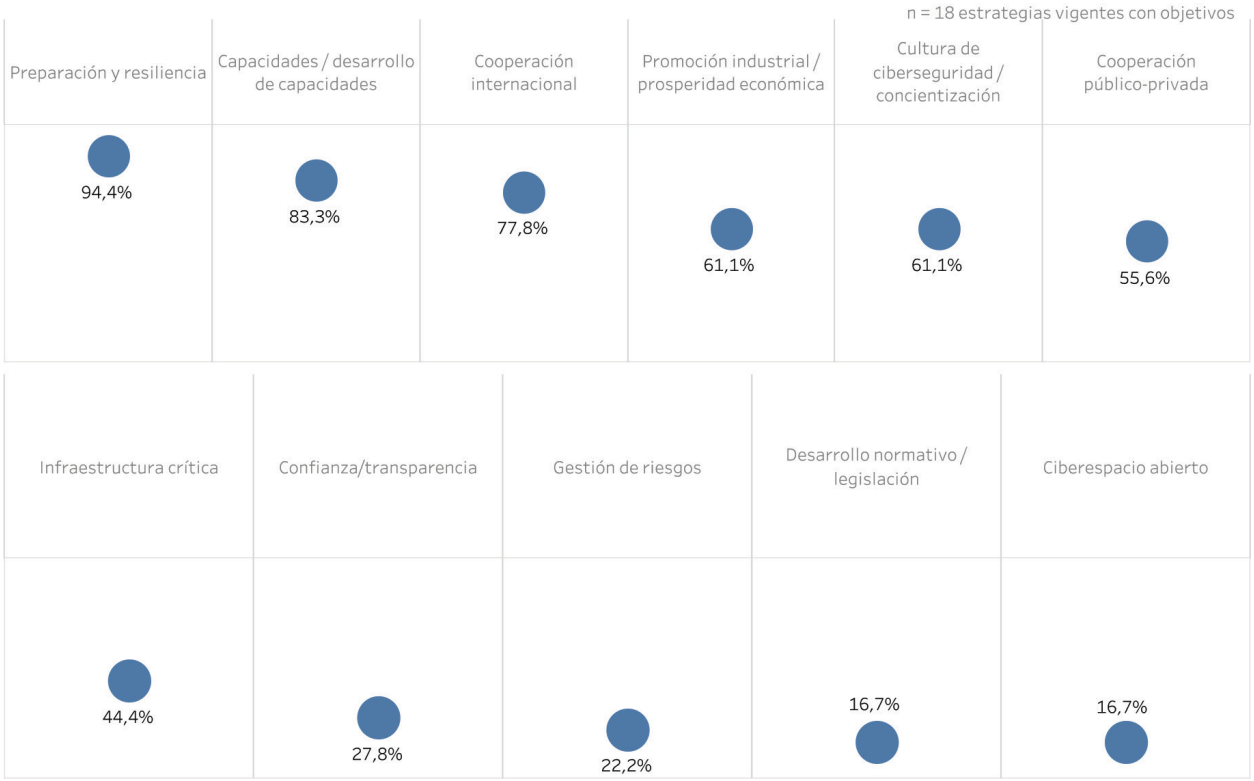
### PUNTOS CLAVE DE LA SECCIÓN

- **Objetivos.** El 94,7% de las estrategias analizadas definen objetivos estratégicos.
- **Preparación y resiliencia.** El 94,4% de las estrategias analizadas poseen, al menos, un objetivo relacionado con los temas de preparación y resiliencia.
- **Capacidades.** El 83,3% de las estrategias analizadas poseen, al menos, un objetivo para fortalecer las capacidades de ciberseguridad del país.
- **Prosperidad económica.** Al igual que con los principios, se observa un aumento en la presencia de objetivos vinculados a la promoción industrial de la ciberseguridad, especialmente en los países del Norte Global (71% en las estrategias de tercera generación, en comparación con 39% en las de primera generación).
- **Cooperación público-privada.** Mayor presencia de objetivos estratégicos vinculados a la cooperación público-privada (71% frente al 44% de la primera generación) en las estrategias de tercera generación.
- **Transparencia.** Las estrategias de tercera generación tienen más objetivos vinculados a la transparencia (43% frente al 17% de la primera generación).

Los objetivos constituyen el centro neurálgico de las estrategias y, tal como se observó, únicamente en una de las 43 estrategias analizadas no se los define de manera explícita. Así como se analizó la evolución de los principios a lo largo del tiempo, en esta sección, se analizan los contenidos que más se destacan en los objetivos y cómo evolucionaron a través del tiempo y en las diferentes generaciones de estrategias. Para efectuar un análisis exhaustivo, se identificaron siete temas que abarcan la mayoría de los objetivos presentes en las estrategias. En el gráfico 8, se muestra la frecuencia con la que aparecen. Cabe destacar que este análisis incluye solo el nivel más alto de los objetivos, es decir que, si una estrategia, por ejemplo, tenía objetivos estratégicos y subobjetivos, este gráfico identifica solo el nivel de objetivos estratégicos. Con respecto a esta limitación, también es importante ejercer cautela al sacar conclusiones. El hecho de que un país no haya incluido un determinado tema en su nivel más alto de objetivos no implica que no tenga acciones específicas al respecto. Los subobjetivos se tratarán en las áreas de interés exploradas en las próximas secciones.

El 94,4% de las estrategias vigentes analizadas cuenta, al menos, con un objetivo que incluye cuestiones de preparación y resiliencia.

## GRÁFICO 8 – TIPOS DE OBJETIVOS




En segundo lugar, los objetivos de fortalecimiento de las capacidades del país en ciberseguridad y algún objetivo relacionado con la cooperación internacional aparecen en el 83,3% y 77,8% de las estrategias analizadas, respectivamente. El gráfico 8 muestra los demás temas comunes.

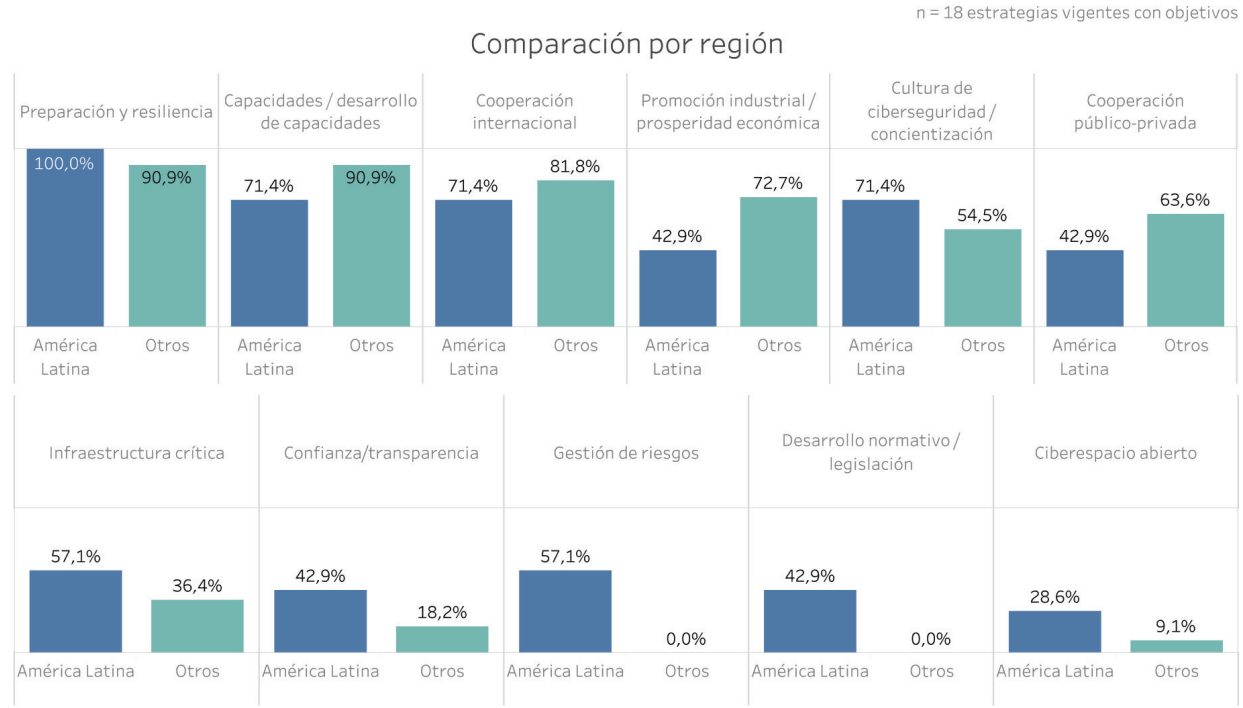
En cuanto al análisis por región (gráfico 9), se observa que, en muchas categorías, no parece haber diferencias tan significativas entre las regiones estudiadas. Sin embargo, algunos temas refuerzan las tendencias observadas en las secciones anteriores y merecen una mención especial.

En primer lugar, así como el principio de prosperidad económica estuvo algo ausente en los principios de las estrategias de América Latina, se observa que los objetivos estratégicos vinculados a la promoción industrial de la ciberseguridad también estuvieron ausentes en la región. Mientras que el tema se menciona en el 42,9% de las estrategias analizadas en América Latina, el 72,7% de las estrategias del Norte Global tiene algún tipo de objetivo estratégico vinculado a la industria nacional o a la prosperidad económica.

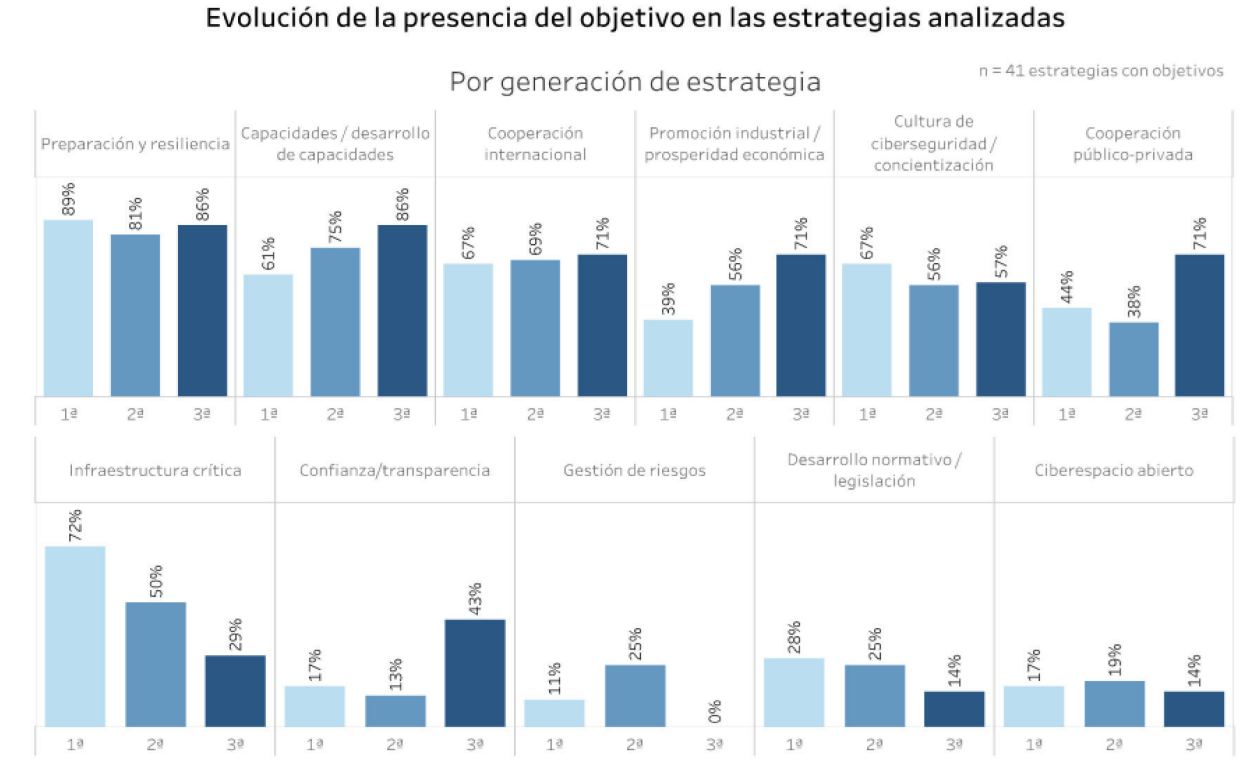
Otro punto a destacar al comparar las estrategias de América Latina con las de los países fuera de la región es que se observa que las primeras tienden más a incluir objetivos asociados a la redacción o mejora de leyes relacionadas con la ciberseguridad. Las estrategias vigentes de América Latina también presentan, con mayor frecuencia, objetivos estratégicos relacionados con la gestión de riesgos.

La evolución de los objetivos desde la perspectiva de la generación de estrategias (gráfico 10) también revela puntos interesantes sobre posibles tendencias. Como ya se mencionó, y con respecto a las generaciones de las estrategias, se observa que las cuestiones vinculadas a

## GRÁFICO 9 – TIPOS DE OBJETIVO, POR REGIÓN




## GRÁFICO 10 – EVOLUCIÓN DE LOS TIPOS DE OBJETIVOS



la prosperidad económica tienen mayor presencia en las estrategias de aquellos países que ya se encuentran en la tercera generación. Además, a medida que los países evolucionan en sus estrategias, se percibe el crecimiento del tema de la cooperación público-privada. También se observa una menor presencia de objetivos de primer nivel centrados explícitamente en la protección de la infraestructura crítica. Se entiende que esta disminución puede explicarse por el hecho de que el tema de la protección de la infraestructura crítica ahora se trata de una manera más transversal y se incluye en conceptos más amplios, como la resiliencia o, incluso, la cooperación con el sector privado (este tema se explorará en el área de interés sobre la infraestructura crítica).

Por último, el mayor enfoque en la transparencia, destacado en la sección *Principios*, también se repite en el aumento de la mención de este tema en los objetivos estratégicos. Esto refuerza la tendencia ya identificada de que las estrategias de ciberseguridad consideran cada vez más seriamente las cuestiones relacionadas con la transparencia y el aumento de la confianza.

Al no encontrarse patrones destacados en el análisis anual de este tema, se optó por no incluir el gráfico comparativo de los períodos. Las tendencias más interesantes se identifican al evaluar la evolución por generación.

Con respecto a los números de los macrobjetivos, no se identificó ninguna tendencia de aumento o disminución a lo largo de los años. La gran mayoría de las estrategias se centran en cuatro o cinco pilares, objetivos estratégicos o grandes áreas de acción. En los recuadros a continuación, se incluyen ejemplos cualitativos de cómo se presentan los objetivos estratégicos en tres estrategias seleccionadas.

### RECUADRO 5 – EJEMPLO DE OBJETIVOS – ESTONIA, 2019

#### OBJETIVO 1. SOCIEDAD DIGITAL SOSTENIBLE

Estonia es una sociedad digital sostenible que cuenta con una fuerte resiliencia tecnológica y preparación para emergencias.

#### OBJETIVO 2. SECTOR DE LA CIBERSEGURIDAD, INVESTIGACIÓN Y DESARROLLO

El sector de la ciberseguridad de Estonia es fuerte, innovador, competitivo en el ámbito mundial y con fuerte énfasis en la investigación; además, abarca todas las competencias básicas del país.

#### OBJETIVO 3. CONTRIBUCIÓN INTERNACIONAL DESTACADA

Estonia es un socio confiable e idóneo en el ámbito internacional.

#### OBJETIVO 4. SOCIEDAD CON ALFABETIZACIÓN CIBERNÉTICA

Estonia es una sociedad cibernética que dispone de talento suficiente y con visión de futuro.

### RECUADRO 6 – EJEMPLO DE OBJETIVOS – ESTADOS UNIDOS, 2023

I. Defender la infraestructura crítica
II. Interrumpir y desmantelar a los agentes de amenazas
III. Influir en las fuerzas del mercado para impulsar la seguridad y la resiliencia
IV. Invertir en un futuro resiliente
V. Forjar alianzas internacionales para alcanzar objetivos compartidos

**RECUADRO 7 – EJEMPLO DE OBJETIVOS – COREA, 2019**

Garantizar la estabilidad de las operaciones del Estado: fortalecer la seguridad y la resiliencia de la infraestructura principal del país para permitir el funcionamiento continuo a pesar de las amenazas cibernéticas.

Responder a los ciberataques: fortalecer las capacidades de seguridad para impedir las ciberamenazas, detectarlas y bloquearlas rápidamente, y responder a cualquier incidente con prontitud.

Construir una base sólida de ciberseguridad: cultivar un ecosistema justo y autónomo en el que la tecnología de ciberseguridad, los recursos humanos y las industrias sean competitivos.

## 5.7. Áreas de interés y acciones vinculadas

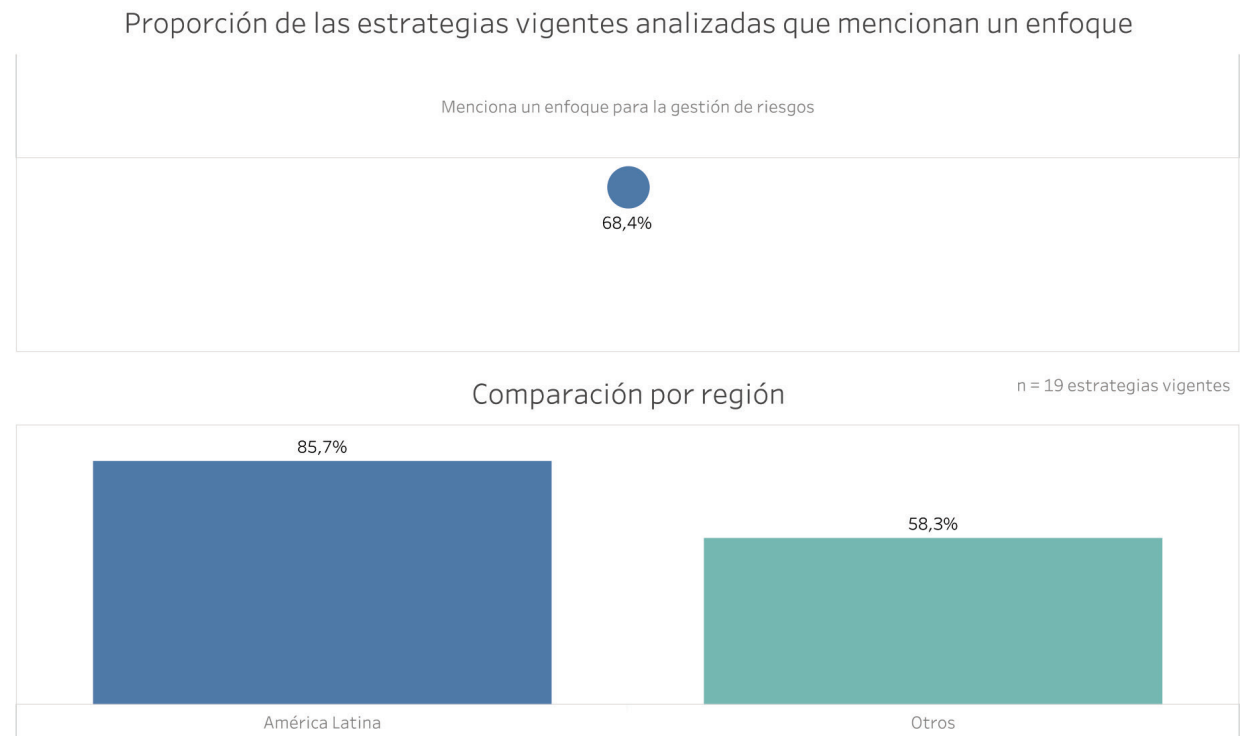
Esta sección del estudio analiza las áreas de acción de las estrategias a través de los temas incluidos en forma de iniciativas, subobjetivos, líneas de acción, pilares de acción u otras categorías similares presentes en las estrategias. Las áreas de interés comprenden las siete categorías prioritarias definidas en la publicación de la UIT que se mencionó anteriormente, junto con otras dos categorías adicionales. Dentro de cada área, se seleccionaron diferentes temas y acciones por evaluar.

### 5.7.1. *Área de interés: gestión de riesgos*

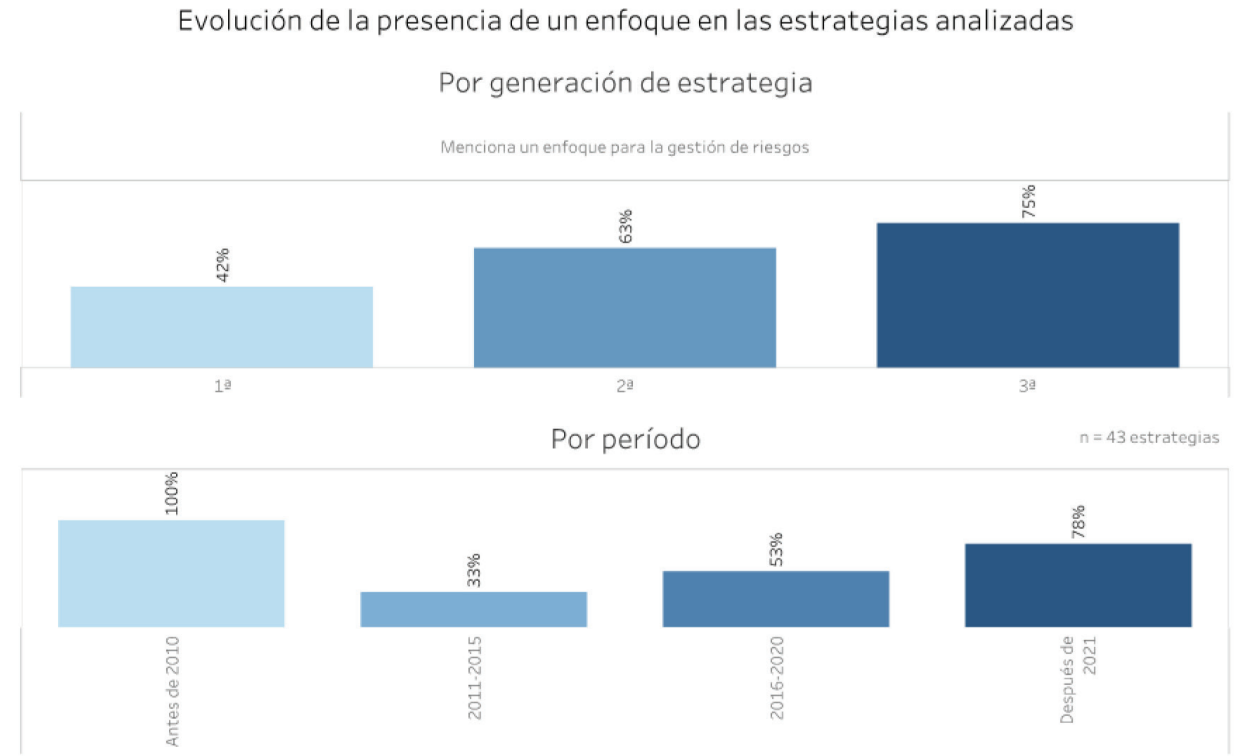
**PUNTOS CLAVE DE LA SECCIÓN**

- **Enfoque para la gestión de riesgos.** Se observa una tendencia creciente a incluir un enfoque para la gestión de riesgos como parte de las acciones de la estrategia, aunque el detalle no incluya la definición de una metodología específica.

**GRÁFICO 11 – ÁREA DE INTERÉS: GESTIÓN DE RIESGOS**



## GRÁFICO 12 – EVOLUCIÓN DEL ÁREA DE INTERÉS: GESTIÓN DE RIESGOS




### RECUADRO 8 – MAYORES DETALLES DEL ÁREA DE INTERÉS

#### La gestión de riesgos en España

España es un ejemplo donde existen una definición de la gestión de riesgos, una metodología de gestión y un conjunto de políticas y normativas que avalan este procedimiento. Sin embargo, la estrategia solo detalla la iniciativa por desarrollar, siendo en esta (y no en la estrategia en sí) donde se especifican todos los aspectos necesarios para la implementación.

En términos generales, la definición del enfoque, la metodología y las políticas de gestión de riesgos son prácticas excelentes que se deben considerar en una estrategia. No obstante, no es necesario incluir todas estas prácticas en el documento principal. Se trata de un tema amplio que requiere un gran conjunto de definiciones y afecta a múltiples actores. Además, también requiere una estructura normativa que le otorgue solidez y aplicabilidad, ya que la estrategia sirve como una herramienta para impulsar su promoción, pero no necesariamente para definir los detalles técnicos.

Identificar, medir y evaluar los riesgos permite que el Gobierno pueda gestionarlos de manera efectiva. En el ámbito nacional, también es necesario definir una metodología común y transversal que permita evaluar y comparar cada uno de los organismos estatales. Sin embargo, y de acuerdo con este análisis, esa definición suele incluirse en documentos complementarios y no en la propia estrategia.

De las estrategias estudiadas, el 68,4% de las que están vigentes definen un enfoque para la gestión de riesgos. Este número aumenta al

85,7% si se consideran solo las estrategias de América Latina. Al analizar cómo este tema se trata en las estrategias según la generación o el período, se observa claramente un aumento que confirma que se trata de un aspecto cada vez más en consideración. La estrategia de Colombia es un ejemplo, ya que incluye la gestión de riesgos desde la segunda edición y el tema mantiene su importancia en la tercera.

Es importante destacar que las estrategias que mencionan la necesidad de contar con un enfoque para la gestión de riesgos rara vez incluyen detalles técnicos u operativos. En cambio, delegan esta función a documentos complementarios. Por ejemplo, estrategias como la de España no detallan una metodología en el documento estratégico, pero sí implementan un método en el ámbito nacional. Esto sugiere una tendencia de las estrategias a no entrar en detalles técnicos minuciosos.

### 5.7.2. *Área de interés: resiliencia y preparación*

**PUNTOS CLAVE DE LA SECCIÓN**

- **Capacidad de respuesta a incidentes.** Todas las estrategias abordan este tema, incluso en estrategias de diferentes generaciones de un mismo país y consideran diversas cuestiones.
- **Intercambio de información.** El intercambio de información es una capacidad esencial en el ámbito de la ciberseguridad. Es un requisito fundamental para generar conocimiento, mejorar las capacidades de ciberseguridad y fortalecer los lazos entre los diferentes actores que participan en la protección de un país. Este tema está presente en el 84,2% de las estrategias vigentes y registra una trayectoria de crecimiento a lo largo de las generaciones de estrategias.

Como se verá en todos los temas de esta área de interés, la protección y la resiliencia tienen gran relevancia en todas las estrategias, especialmente en las actuales. Existen varias iniciativas que buscan mejorar la protección y la resiliencia de forma transversal. Un ejemplo es la Ley de Ciberresiliencia de la Unión Europea (UE),[17] que establece requisitos de ciberseguridad para los productos con elementos digitales. Otro ejemplo es la Ley de Resiliencia Operativa Digital de la UE,[18] cuyo objetivo es regular y unificar la legislación para la gestión de riesgos digitales en el sector financiero.

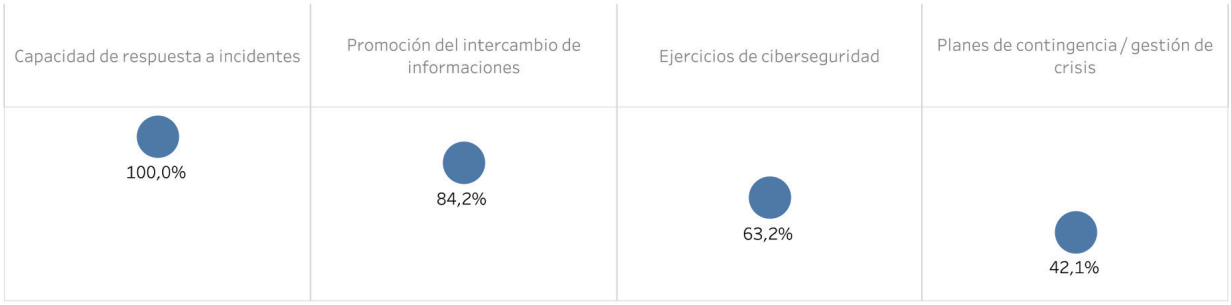
La capacidad de respuesta a incidentes es un tema de interés para todos los países, y es posible observar su mención de manera explícita en todas las estrategias vigentes. A diferencia de otros temas, la capacidad de respuesta está presente en un alto porcentaje en todas las generaciones de estrategias. Esto se debe a que, a medida que los países mejoran sus capacidades en ciertos aspectos, el dinamismo de las amenazas crea nuevos desafíos que deben abordarse con nuevos objetivos. Al considerar como ejemplo a la República Dominicana, se observa que, en su primera estrategia, las principales líneas de acción para mejorar la capacidad de respuesta a incidentes se centraron en la promoción de mejores prácticas, la creación de un centro nacional de respuesta a incidentes y el desarrollo de equipos de respuesta ante incidentes de seguridad (CSIRT) sectoriales. En la segunda generación de su estrategia, se mantiene el mismo objetivo; sin embargo, las líneas de acción están más relacionadas con el desarrollo de planes de respuesta, el fortalecimiento de las estructuras organizativas ya existentes y la coordinación e intercambio de información.

[17] Ley de Ciberresiliencia. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[18] Ley de Resiliencia Operativa Digital. https://www.digital-operational-resilience-act.com/.

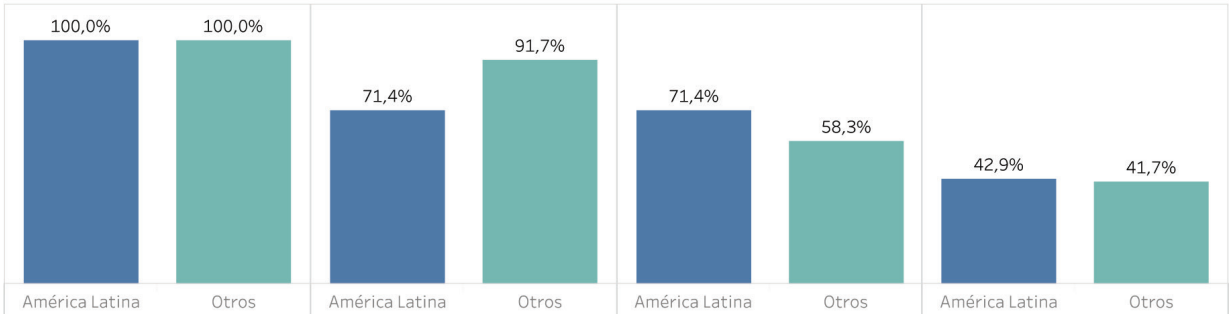
## GRÁFICO 13 – ÁREA DE INTERÉS: PREPARACIÓN Y RESILIENCIA

Proporción de las estrategias vigentes analizadas que mencionan cada mecanismo




Comparación por región

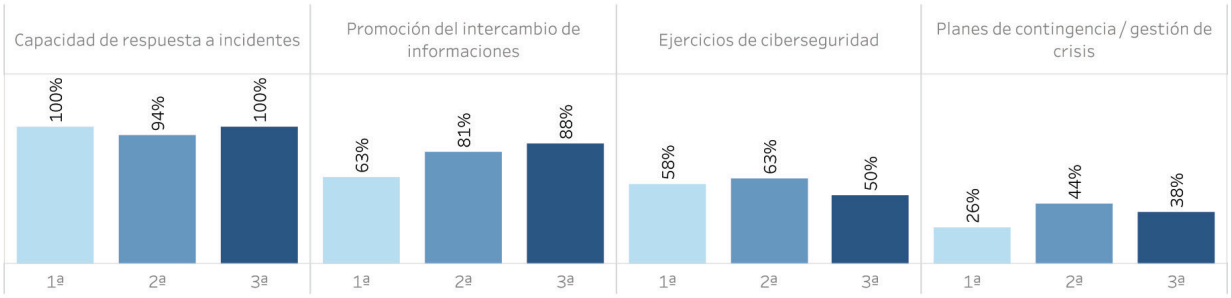
n = 19 estrategias vigentes




## GRÁFICO 14 – EVOLUCIÓN DEL ÁREA DE INTERÉS: PREPARACIÓN Y RESILIENCIA

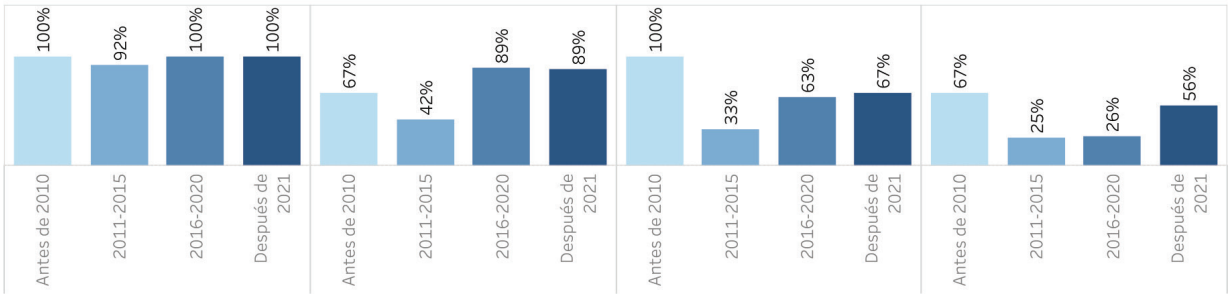
Evolución de la presencia del mecanismo en las estrategias analizadas

Por generación de estrategia




Por período

n = 43 estrategias



Como es de conocimiento público, las amenazas y los grupos delictivos organizados que operan en el espacio cibernético no tienen fronteras. El conocimiento es un insumo clave en la preparación para las amenazas actuales y emergentes. Saber cuáles son las amenazas activas, cuáles son las tendencias y qué datos técnicos pueden enriquecer y fortalecer la capacidad de detectar incidentes y responder a ellos son aspectos que deben estar presentes en las estrategias de ciberseguridad. Ese conocimiento se debe generar y compartir tanto en el ámbito nacional como en el internacional con el fin de establecer vínculos bidireccionales capaces de nutrir todas las partes. Los datos observados como parte de este estudio con respecto a esta cuestión muestran que el 84,2% de las estrategias actuales promueven el intercambio de información, una tendencia que registró un aumento constante a lo largo de las generaciones de estrategias. Los Estados Unidos, en su estrategia más reciente, establecen como objetivo estratégico "Aumentar la velocidad y la escala del intercambio de información y la notificación a las víctimas". Este objetivo cuenta con el apoyo del Centro de Integración de Inteligencia contra Amenazas Cibernéticas[19], entre otras entidades.

Según lo declarado en la sección *Área de interés: capacidades y concientización*, la capacitación en seguridad cibernética es un elemento presente en prácticamente todas las estrategias. No es de extrañar que, según el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC2, por sus siglas en inglés), en su informe *Cybersecurity Workforce Study*[20], se estime que existan 3.400.000 de empleos en seguridad cibernética vacantes. Una manera de desarrollar habilidades en ciberseguridad es a través de ejercicios destinados a exponer a los involucrados a escenarios de crisis. El objetivo principal es adquirir experiencia y tener la preparación para gestionar las crisis de la mejor manera posible. Existen varios tipos de ejercicios, orientados a diferentes públicos, como se muestra en los ejemplos a continuación.

- Ejercicios orientados a equipos técnicos: se simulan la infraestructura de una organización (de la forma más realista posible) y los escenarios (de forma controlada) en que los equipos técnicos se enfrentan a diferentes tipos de incidentes. En esta simulación, los equipos deben detectar, contener y mitigar las amenazas tal como lo harían en un escenario del mundo real.
- Ejercicios orientados a los tomadores de decisión: con frecuencia se utilizan simulaciones de incidentes que involucran a los tomadores de decisión de una organización, en el ámbito nacional o internacional *(Table Top Exercises)*. Se trata de escenarios hablados que simulan incidentes, en los cuales todos los involucrados deben tomar decisiones que afecten la situación y el resultado final del incidente.

De las estrategias actuales, el 63,3% considera este tipo de ejercicio en mayor o menor medida.

En la sección *Área de interés: protección y resiliencia*, el tema menos presente en las estrategias es la elaboración de un plan de contingencia para la gestión de las crisis. Al observar las estrategias actuales, solo el 42,1% menciona de manera directa el tema; sin embargo, es posible observar que este porcentaje aumenta en

[19] Centro de Integración de Inteligencia sobre Amenazas Cibernéticas. https://www.dni.gov/index.php/ctiic.

[20] ISC2 Cybersecurity Workkforce Study. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196.

las estrategias publicadas más recientemente. Según la UIT, "la estrategia debería exigir el desarrollo de un plan nacional de contingencia para emergencias y crisis de ciberseguridad. El plan debe formar parte del plan nacional de contingencia general o seguir sus lineamientos".

## RECUADRO 9 – ESTUDIO DE CASO

### LAS ESTRATEGIAS DE CIBERSEGURIDAD EN COLOMBIA

Colombia es el primer país de la región que contó con una estrategia de ciberseguridad (la primera se publicó en 2011) y el único país de América Latina que publicó tres versiones. Todas sus estrategias abordan temas de ciberseguridad y están fuertemente relacionadas con la ciberdefensa, una característica poco común en las estrategias analizadas en este estudio. Un aspecto muy interesante es la inclusión de las lecciones aprendidas, tanto en la segunda como en la tercera edición, y cómo estas influyen en los objetivos.

En su primera edición de la estrategia, Colombia consideraba que los principales desafíos eran los puntos débiles en la capacidad del Estado para lidiar con las amenazas en ese momento, la falta de coordinación de las iniciativas y operaciones de seguridad y defensa cibernéticas, así como las deficiencias en los aspectos legales y regulatorios. Gran parte de estos puntos débiles aún persisten. Para resolver estos problemas, los principales objetivos estaban relacionados con: (i) la implementación de organismos para prevenir, coordinar y controlar posibles amenazas contra el Estado, con especial énfasis en la creación de una estructura organizacional para coordinar las acciones como respuesta a incidentes; (ii) la oferta de capacitación especializada en seguridad y defensa cibernética, y (iii) el fortalecimiento de aspectos de la legislación y la adhesión a instrumentos internacionales.

Para su segunda edición, publicada en 2016, Colombia analizó las acciones impulsadas por la primera estrategia y la situación de ciberseguridad en ese momento. Concluyó que había aspectos pendientes que no habían sido considerados en la primera versión. Uno de estos aspectos era la gestión de riesgos, que asume un papel destacado en los nuevos objetivos. Como consecuencia, la segunda estrategia se centró en cuatro principios: salvaguardar los derechos humanos y los valores fundamentales de la ciudadanía, adoptar un enfoque inclusivo y colaborativo, garantizar la responsabilidad compartida entre todas las partes y adoptar una metodología para la gestión de riesgos.

En la tercera y última edición, publicada en 2020, así como en la segunda edición, Colombia analiza los aspectos que no habían sido considerados en las estrategias anteriores. A partir de este análisis, la confianza y la seguridad digital surgen como conceptos nuevos y fundamentales. Estos sirven como herramientas para fortalecer la inclusión social y aumentar la competitividad de Colombia en el ámbito digital. En consecuencia, el primer objetivo es fortalecer las capacidades de seguridad digital de la ciudadanía, el sector público y el sector privado. El segundo objetivo es actualizar la estructura de gobernanza para la seguridad digital.

Colombia es un excelente ejemplo de cómo las lecciones aprendidas de una estrategia son fundamentales para desarrollar la siguiente. Este proceso evolutivo considera tanto los aspectos pendientes como aquellos que cobran mayor importancia.

### 5.7.3. *Área de interés: infraestructura crítica y servicios esenciales*

**PUNTOS CLAVE DE LA SECCIÓN**

- **Medidas para proteger las infraestructuras críticas.** Este es un tema que está presente en la mayoría de las estrategias (en el 89,5% de las estrategias vigentes).
- **Sector privado.** La participación de este sector en la gestión de las infraestructuras críticas suele ser elevada; por lo tanto, es importante abordar la cooperación con el sector privado en la estrategia. Se puede observar que, a lo largo de los años, las estrategias mencionan este aspecto cada vez más.
- **Activos del gobierno digital.** Se observa el aumento de este tema en las estrategias cada año, posiblemente debido a la preocupación por proteger los activos del gobierno digital para continuar la digitalización de los servicios.
- **Identificación de infraestructuras críticas.** La identificación de infraestructuras críticas es fundamental para establecer un plan de protección. El análisis muestra que, cada vez más, los países tienden a identificar estas infraestructuras en las primeras etapas de sus estrategias.
- **Servicios esenciales.** Se observa un aumento de las menciones del concepto de servicios esenciales (ya sea en sustitución o en complemento del concepto de infraestructuras críticas), especialmente en las estrategias más recientes del Norte Global.

La protección de las infraestructuras críticas es una preocupación que comparten todos los países. De hecho, el 100% de las estrategias analizadas, en su primera edición, tienen como objetivo establecer medidas para la protección de las infraestructuras críticas. Esto no es sorprendente, ya que estos ataques se observan desde hace muchos años; por ejemplo, en 2010, un *malware* afectó a una fábrica iraní,[21] y más recientemente, en 2021, la infraestructura de soporte de gasoductos en los Estados Unidos se vio comprometida por un *ransomware*.[22]

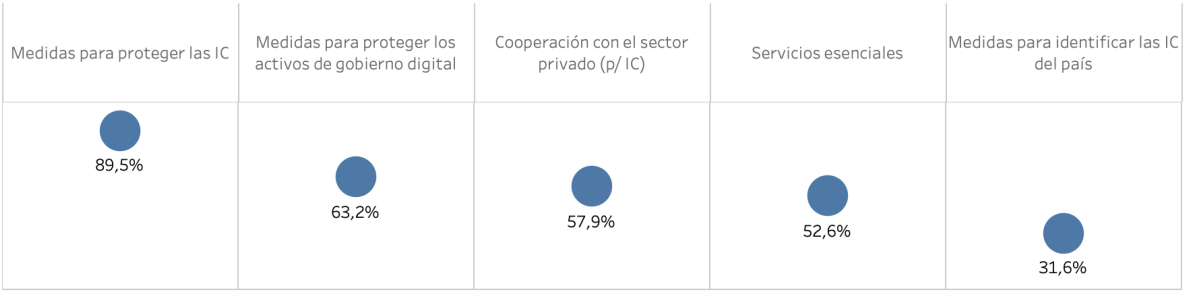
Según la Directiva Europea 2008/114/CE del 8 de diciembre de 2008,[23] la infraestructura crítica se define como "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones". En cuanto a los servicios esenciales, la UIT los define como "servicios que son esenciales para las actividades socioeconómicas indispensables".

Entre los temas de esta área de interés, el establecimiento de medidas para proteger la infraestructura crítica está presente en el 89,5% de las estrategias vigentes. Asimismo, se puede observar que, a medida que los países publican nuevas ediciones de sus estrategias, este tema tiene una presencia cada vez menor, que comienza con el 100% en la primera generación de estrategias, y llega al 75% en la tercera. Esto puede deberse a que, aunque sigue siendo un aspecto importante, los países lograron aumentar suficientemente la protección de sus infraestructuras críticas y prefirieron centrarse en otros aspectos. También se observa el cambio de nomenclatura a "servicios esenciales". En la primera generación de estrategias, únicamente el 32% de las estrategias mencionaba el término en comparación con el 50% en la tercera generación.

[21] Caso Stuxnet. https://www.bbc.com/news/world-middle-east-11414483.
[22] CISA. El ataque al oleoducto colonial. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.
[23] DIRECTIVA 2008/114/CE. https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

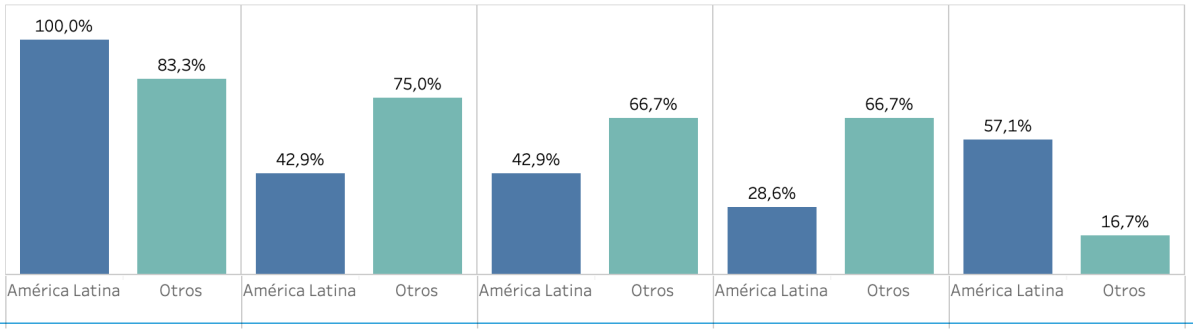
## GRÁFICO 15 – ÁREA DE INTERÉS: INFRAESTRUCTURA CRÍTICA (IC) Y SERVICIOS ESENCIALES

Proporción de las estrategias vigentes analizadas que mencionan cada mecanismo




Comparación por región

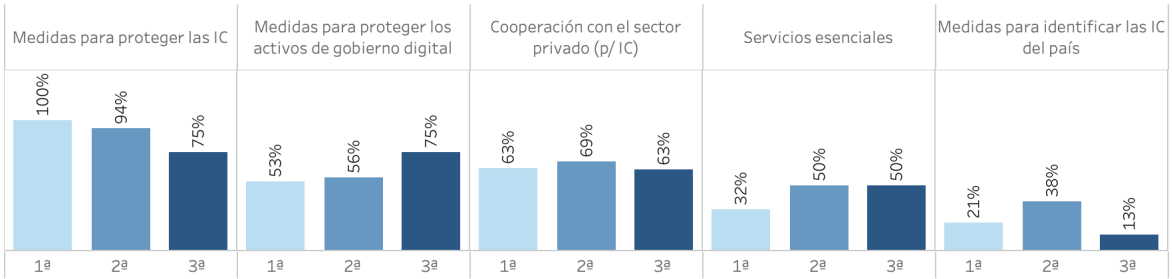
n = 19 estrategias vigentes




## GRÁFICO 16 – EVOLUCIÓN DEL ÁREA DE INTERÉS: INFRAESTRUCTURA CRÍTICA (IC) Y SERVICIOS ESENCIALES

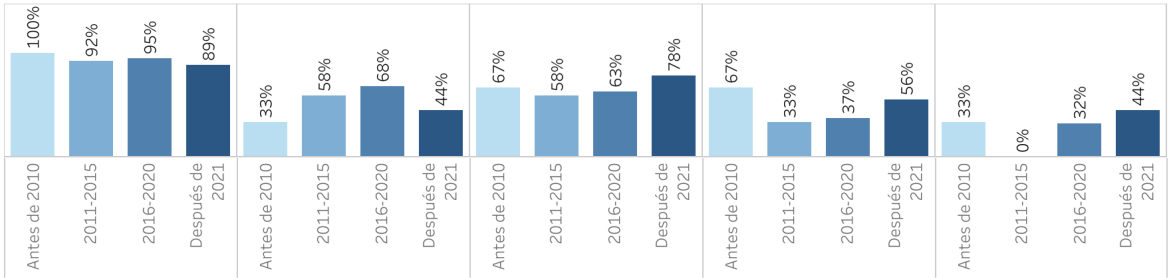
Evolución de la presencia del mecanismo en las estrategias analizadas

Por generación de estrategia




Por período

n = 43 estrategias



La cooperación con el sector privado está presente en varias áreas de interés de la mayoría de las estrategias modernas, y lo mismo sucede en lo que respecta a las infraestructuras críticas. Si se considera que, en la mayoría de los países, la administración de las infraestructuras críticas está a cargo de empresas privadas, es natural que el tema de la cooperación con el sector privado para las infraestructuras críticas esté presente constantemente. Por ejemplo, en su tercera estrategia, Japón declara como actividad "avanzar en la protección de infraestructuras críticas con base en asociaciones público-privadas", en la que detalla: "Para la prestación segura y continua de los servicios de las infraestructuras críticas, las cuales constituyen la base de la vida de las personas y las actividades socioeconómicas, los sectores público y privado compartirán una política común entre el Gobierno nacional, que asume la responsabilidad por la protección de estas infraestructuras, y los operadores de las infraestructuras críticas, encargados de la protección de estas de forma independiente".

Con respecto a las medidas para proteger los activos gubernamentales digitales, existe una presencia moderada en las estrategias de América Latina, con un 42,9%, y una presencia mayor en las de los otros países, con un 75%. Se observa una tendencia creciente del tema, a medida que surgen nuevas generaciones de las estrategias, con un pico entre los años 2016 a 2020, que posiblemente coincide con la rápida evolución de la digitalización de los servicios públicos. Esto puede indicar que la preocupación de los Gobiernos por la protección de sus activos digitales crece a medida que los Estados avanzan en la digitalización de estos y existe una mayor exposición e importancia de los servicios.

El último tema, medidas para identificar las infraestructuras críticas del país, está claramente más presente en América Latina, con un 57,1%, en comparación con otros países, con solo un 16,7%. Este punto es fundamental cuando se comienza a tratar el tema de la protección de las infraestructuras críticas. Es evidente que, después de identificar las infraestructuras, este deje de ser un objetivo prioritario. Tal vez por ese motivo, solo el 13% de las estrategias lo abordan en su tercera edición.

### 5.7.4. *Área de interés: capacidades y concientización*

**PUNTOS CLAVE DE LA SECCIÓN**

- **Capacidades y concientización.** La necesidad de fortalecer las capacidades en ciberseguridad en el país es una constante en prácticamente todas las estrategias.
- **Medidas más frecuentes.** Entre los tres temas sobre capacidades más mencionados en las estrategias, se destacan: (i) innovación e investigación y desarrollo (94,7%); (ii) programas de concientización (94,7%), y (iii) medidas para la capacitación de profesionales (89,5%).
- **Diversidad.** Se observa una tendencia creciente a incluir medidas para aumentar la diversidad de la fuerza de trabajo en el campo de la ciberseguridad (género, entre otras desigualdades) en las estrategias.

La necesidad de fortalecer las capacidades de ciberseguridad es una constante en prácticamente todas las estrategias, y es un elemento presente en la sección principal de los documentos. Lo que varía entre las estrategias analizadas es la manera en que se trata el tema y el énfasis atribuido a sus diferentes aspectos.

Entre los cinco temas más mencionados en las estrategias relacionadas con este asunto, se destacan: (i) innovación e investigación y desarrollo, (ii) programas de concientización, (iii) medidas en la educación superior, (iv) medidas para la formación de profesionales y (v) medidas para aumentar las capacidades en ciberseguridad de los funcionarios públicos.

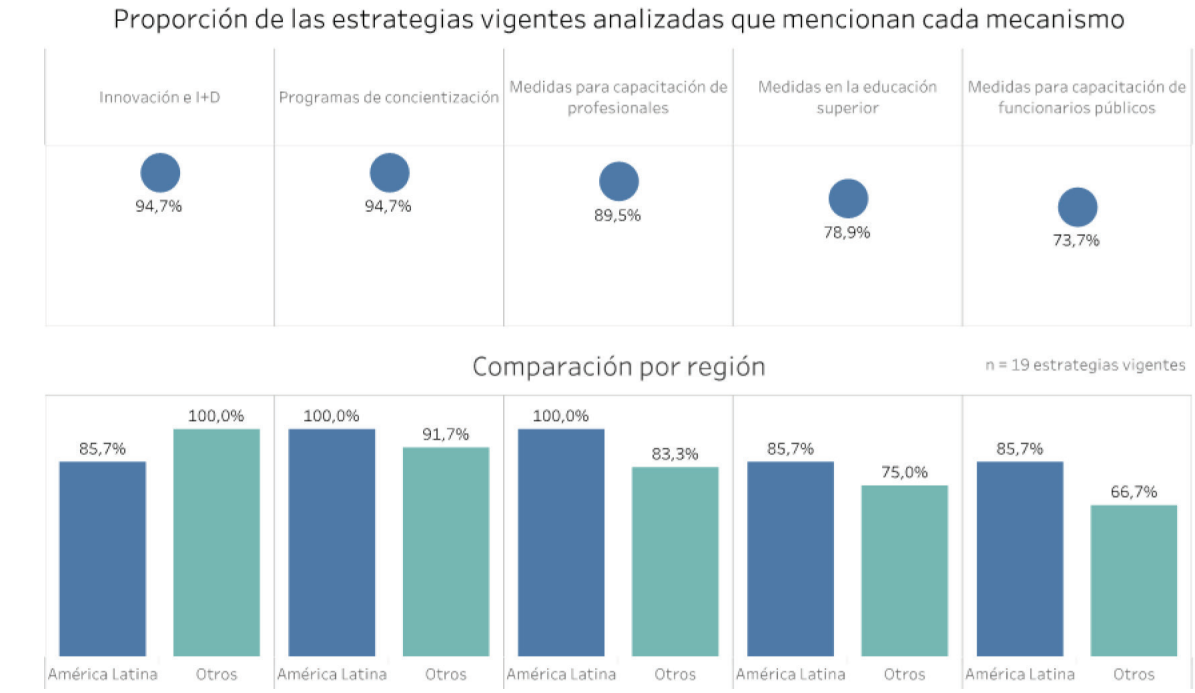
Cabe destacar que estas medidas tienen objetivos distintos. Algunas se enfocan en la escasez de profesionales y fuerza de trabajo especializada en ciberseguridad y buscan estimular la disponibilidad de especialistas calificados en la materia. Otras se dirigen al usuario final, con el objetivo de aumentar la concientización sobre cuestiones de ciberseguridad en la población en general. En la práctica, la mayoría de las estrategias adoptan un enfoque híbrido, que reconoce la importancia tanto de contar con especialistas sumamente calificados como de educar al público en general para que comprenda mejor los desafíos y las prácticas seguras en el entorno digital. Este equilibrio refleja una visión holística para fortalecer las capacidades en ciberseguridad dentro de un contexto nacional.

El gráfico 17 ilustra que el 94,7% de las estrategias analizadas posee iniciativas o subobjetivos relacionados con el fomento de la innovación, la investigación y el desarrollo en materia de ciberseguridad. Estos son algunos ejemplos de cómo se mencionan estas iniciativas.

- Preparar un plan nacional de investigación y desarrollo en materia de ciberseguridad que defina las áreas prioritarias para el Estado (Estonia, 2019).
- Promover y mejorar las capacidades tecnológicas necesarias para contar con soluciones confiables que permitan proteger adecuadamente los sistemas contra diferentes amenazas, e incentiven las actividades de investigación, desarrollo e innovación (I+D+i) en los ámbitos público y privado (Argentina, 2019).
- Promover la producción científica, el desarrollo y la innovación en los diversos ámbitos de la seguridad en el ciberespacio, con el objetivo de mantener y afirmar la independencia nacional en este ámbito (Portugal, 2019).

En relación con las medidas de concientización, también presentes en el 94,7% de las estrategias vigentes, se presentan algunos ejemplos que ilustran cómo se menciona el tema.

**GRÁFICO 17 – ÁREA DE INTERÉS: CAPACIDADES Y CONCIENTIZACIÓN**



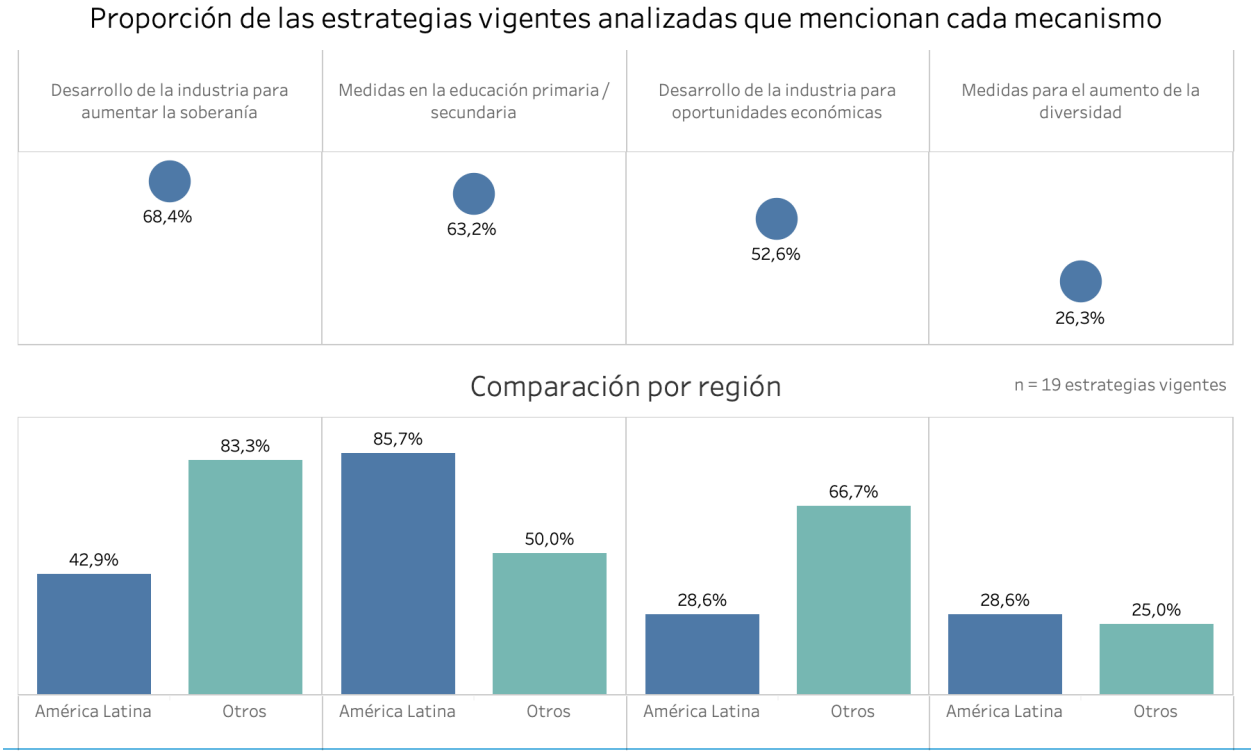
- Crear un programa nacional de concientización sobre seguridad en el espacio cibernético, que abarque a la sociedad en su conjunto (Argentina, 2019).
- Llevar a cabo actividades de concientización dirigidas al público en general (Estonia, 2019).
- Establecer una política para el desarrollo de competencias digitales en la población, con énfasis en la seguridad cibernética, que incluya programas de educación, entrenamiento técnico, sensibilización y concientización para lograr un espacio cibernético más seguro (República Dominicana, 2022).

El gráfico 18 presenta otros cinco temas recurrentes en las acciones relacionadas con las capacidades, especialmente en las medidas vinculadas al desarrollo de la industria y aquellas destinadas a aumentar la diversidad de la fuerza de trabajo.

En relación con el análisis evolutivo en el tiempo (gráficos 19 y 20), una de las tendencias observadas es el incremento de las medidas destinadas a la educación primaria y secundaria a partir de 2016. Esto refleja el esfuerzo por aumentar la concientización de las nuevas generaciones sobre prácticas seguras en el entorno virtual. Al mismo tiempo, desde 2016, también se observa un aumento de las iniciativas de formación profesional en respuesta al desafío de la escasez de profesionales calificados en el mercado de la ciberseguridad. Además, a lo largo de los años, el porcentaje de estrategias que incluyen iniciativas de innovación e investigación y desarrollo se aproxima al 88–89%.

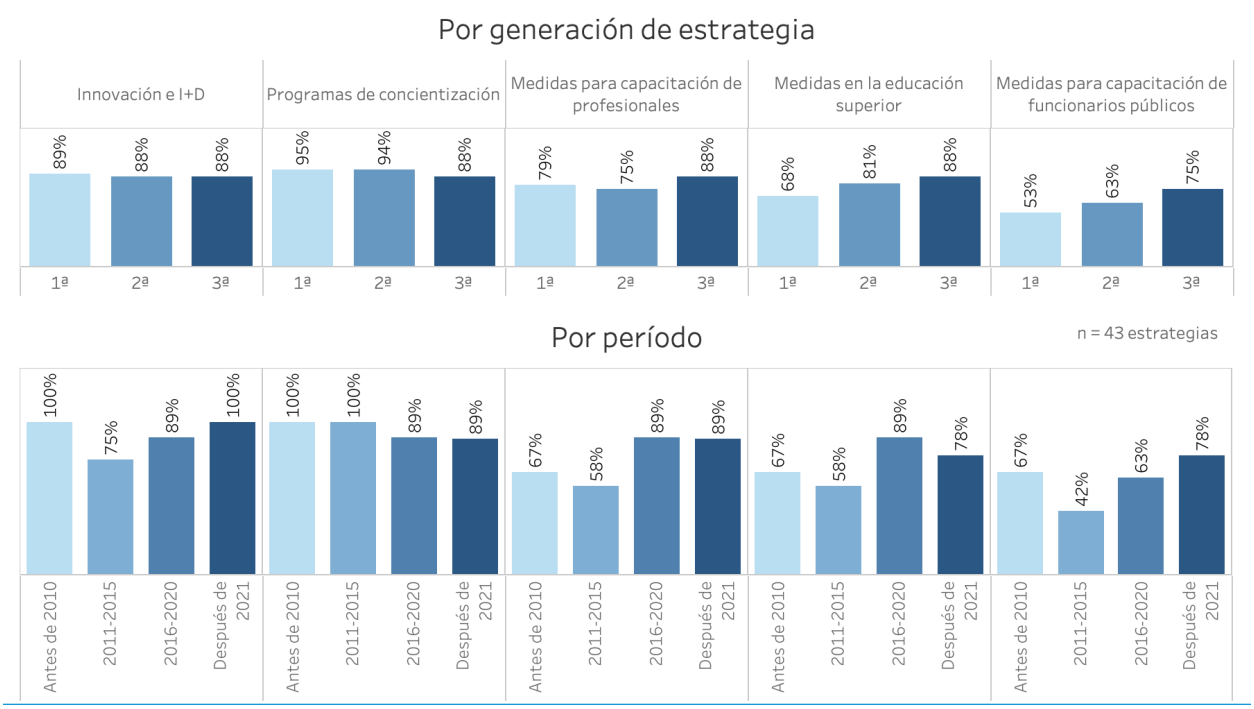
El análisis comparativo también permite verificar la tendencia por incluir con más frecuencia medidas para el desarrollo de la industria, especialmente con el objetivo de aumentar la soberanía (pasa del 42% en la primera generación de estrategias al 75% en la tercera).

**GRÁFICO 18 – ÁREA DE INTERÉS: CAPACIDADES Y CONCIENTIZACIÓN** *(continuación)*



## GRÁFICO 19 – EVOLUCIÓN DEL ÁREA DE INTERÉS: CAPACIDADES Y CONCIENTIZACIÓN

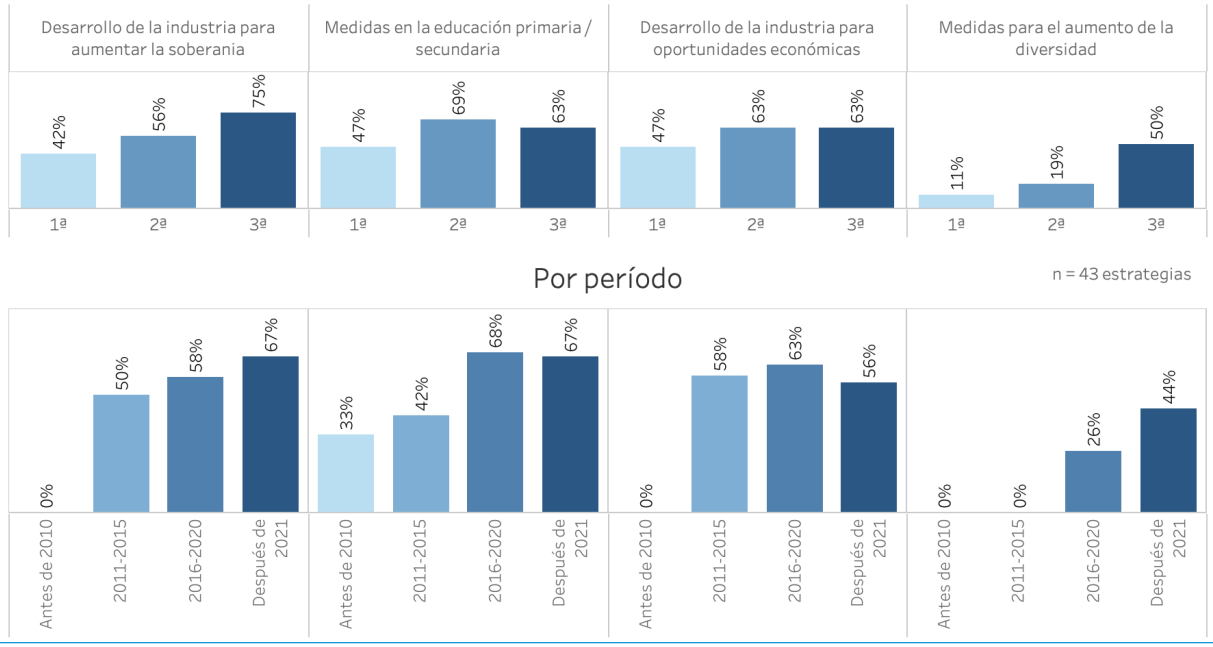
Evolución de la presencia de los mecanismos en las estrategias analizadas




## GRÁFICO 20 – EVOLUCIÓN DEL ÁREA DE INTERÉS: CAPACIDADES Y CONCIENTIZACIÓN

*(continuación)*

Evolución de la presencia de los mecanismos en las estrategias analizadas



Por último, aunque todavía incipiente en las estrategias, una tendencia notable es la creciente preocupación por la diversidad en el ámbito de la ciberseguridad. Si bien este tema era prácticamente inexistente en generaciones de estrategias anteriores, en las de tercera generación, el 50% de las estrategias analizadas en la muestra mencionan este tipo de medidas. Esto sugiere un cambio de mentalidad, con el creciente reconocimiento de la importancia de promover la inclusión y la diversidad en el sector de la ciberseguridad. A continuación, se incluyen dos ejemplos de cómo se mencionan estas medidas.

- Se dará prioridad a una serie de acciones específicas destinadas a aumentar la diversidad de la fuerza de trabajo en el sector cibernético. No se trata solo de garantizar que estos empleos y carreras estén disponibles para todos, sino también de una misión crítica para la seguridad nacional, a fin de garantizar que se aprovechen el talento y las habilidades de toda la población (Reino Unido, 2022).
- Esta estrategia enfrentará directamente la falta de diversidad en la fuerza de trabajo del sector de ciberseguridad. Los empleadores contratan dentro de un grupo muy reducido de talentos y redes profesionales que carecen de la capacidad de aprovechar toda la diversidad del país. Las mujeres, las personas afrodescendientes, los profesionales e inmigrantes de primera generación, las personas con discapacidad y los individuos LGBTQI+ se encuentran entre las comunidades que están subrepresentadas en este campo (Estados Unidos, 2023).

### 5.7.5. *Área de interés: cooperación internacional*

Todas las estrategias, de alguna manera, mencionan el carácter global de la ciberseguridad y la necesidad de cooperación con otros países para lograr los resultados esperados. Las estrategias, dependiendo de su madurez y generación, varían en el alcance del papel que se espera del país en la esfera internacional. En algunos casos, se limitan a garantizar la participación de los países en los foros internacionales, mientras que, en otros, aspiran a ocupar una posición de influencia en esos foros.

Además del eje de la intensidad de la participación, las estrategias también varían en la manera que se refieren al tipo de actuación internacional. En algunos casos, citan foros u organizaciones internacionales específicas, y en otros, priorizan las relaciones bilaterales. En relación con los países de Europa, existe un fuerte alineamiento con la actuación de la Unión Europea en el tema.

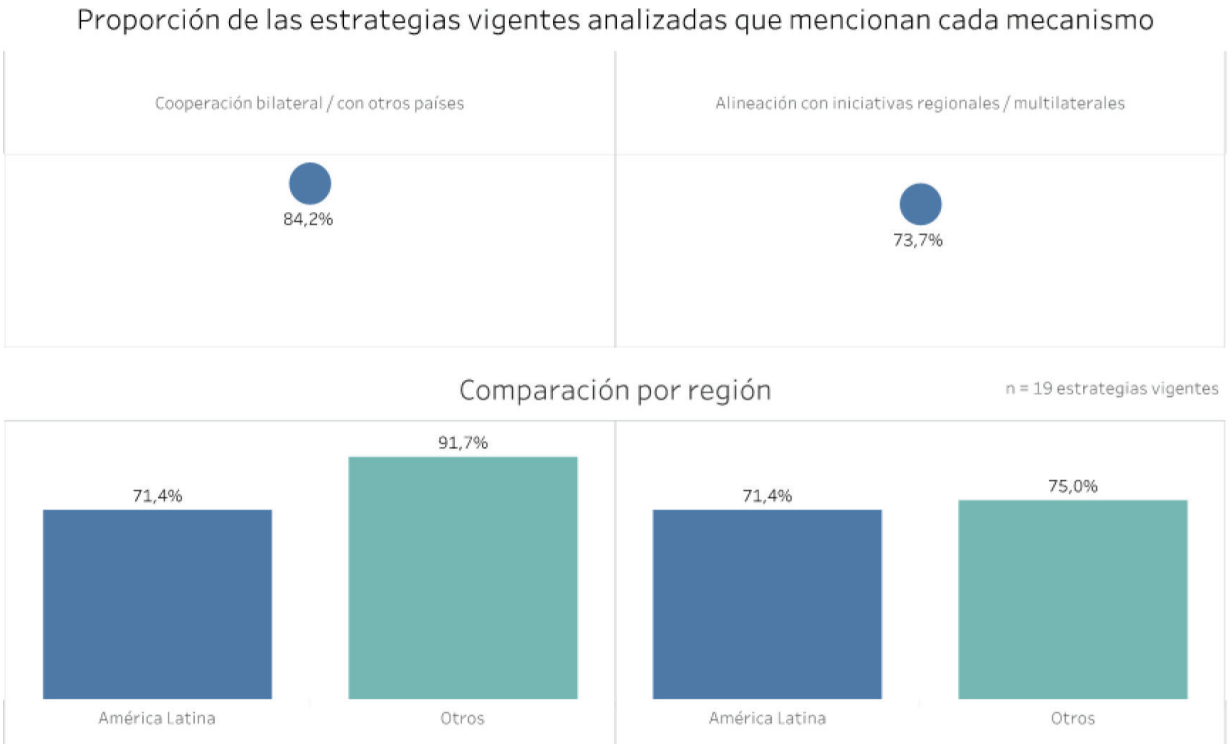
Sobre la base de las categorías de la Guía de la UIT, en esta sección, se analiza la frecuencia de dos categorías asociadas al área de interés de la cooperación internacional.

i. Cooperación con otros países. Se observa que el 91,7% de las estrategias del Norte Global incluyen medidas relacionadas con este frente de trabajo.
ii. Alineamiento con iniciativas regionales/multilaterales. El 73,7% de las estrategias vigentes analizadas citan la necesidad de actuar en bloques regionales o multilaterales.

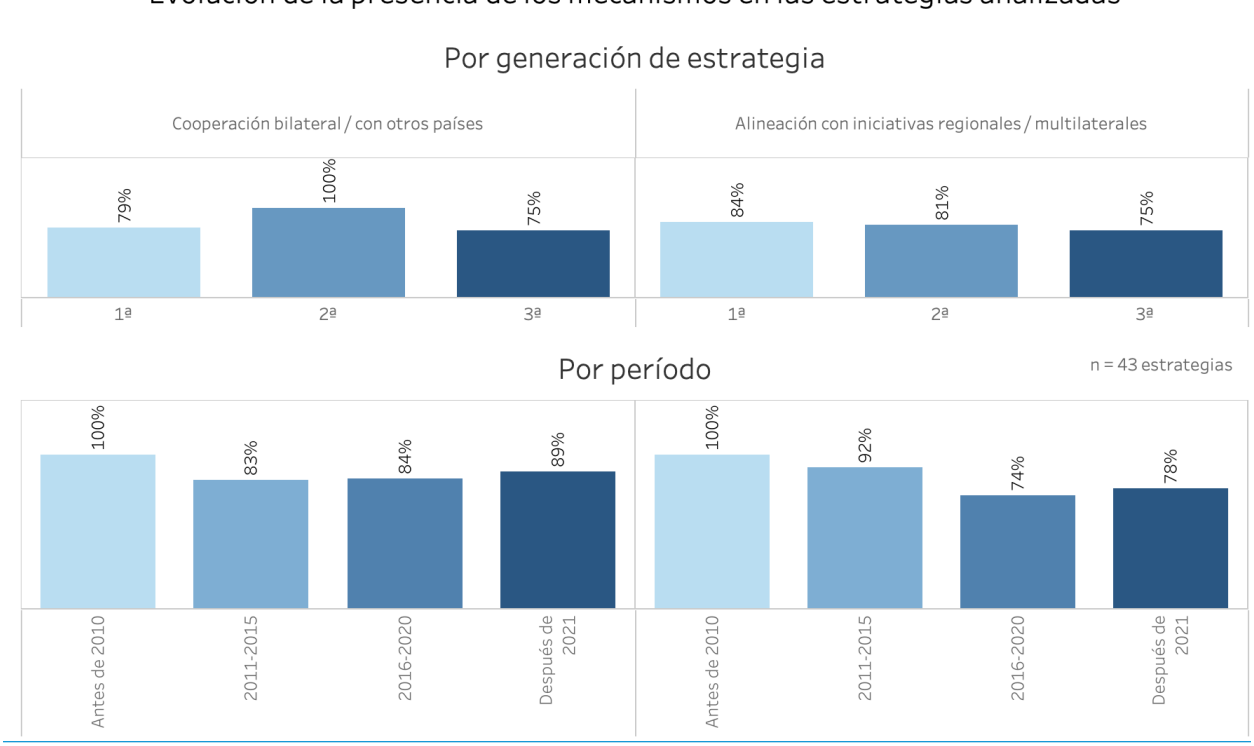
**PUNTOS CLAVE DE LA SECCIÓN**

- **Fuerte presencia de la cooperación internacional.** La cooperación con otros países en el ámbito de la ciberseguridad es una constante en todas las estrategias y se mantiene presente a lo largo del tiempo y de las generaciones de estrategias. En algunos casos, se enfatiza en la acción bilateral y, en otros, en la multilateral.

## GRÁFICO 21 – ÁREA DE INTERÉS: COOPERACIÓN INTERNACIONAL




## GRÁFICO 22 – EVOLUCIÓN DEL ÁREA DE INTERÉS: COOPERACIÓN INTERNACIONAL



### 5.7.6. *Área de interés: legislación y marco normativo*

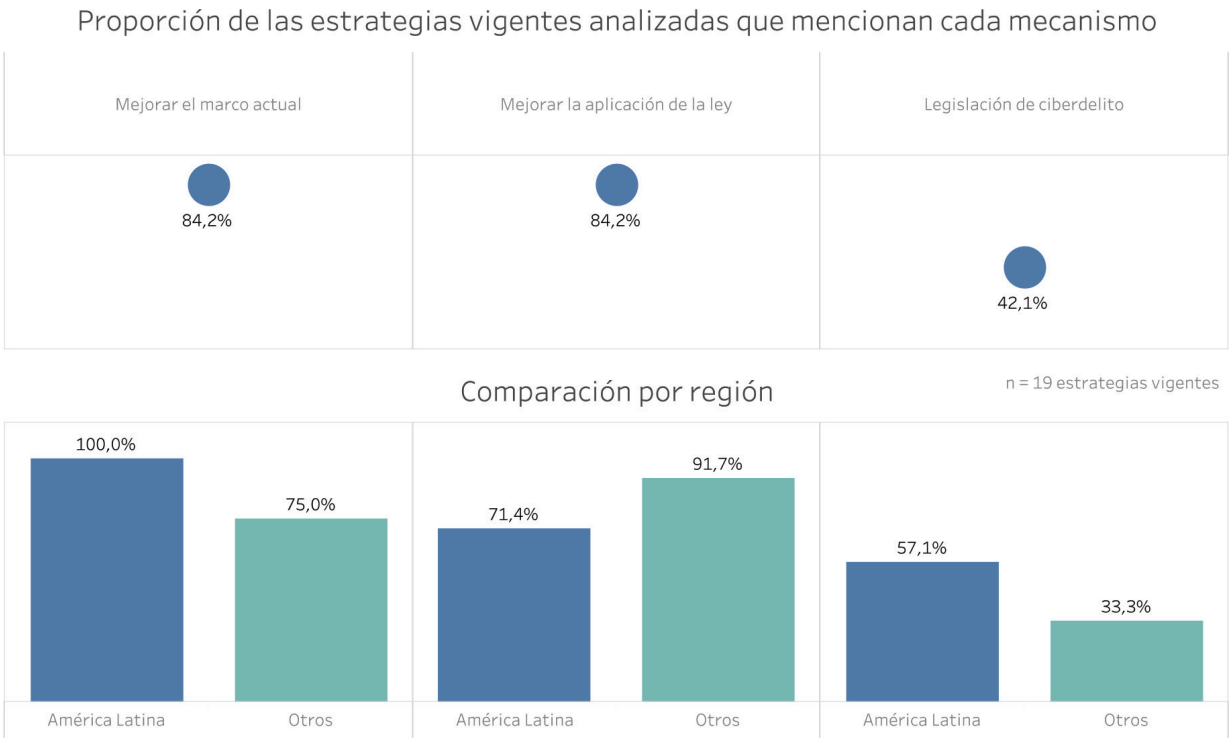
**PUNTOS CLAVE DE LA SECCIÓN**

- **Mejora del marco normativo actual.** La gran mayoría de las estrategias vigentes analizadas (84,2%) presentan alguna medida para mejorar la estructura normativa actual, ya que es imposible lograr mejoras sustanciales sin una estructura regulatoria que respalde los cambios y les otorgue sostenibilidad a lo largo del tiempo.
- **Aplicación de la ley.** La gran mayoría de las estrategias vigentes analizadas (84,2%) incluyen alguna medida para mejorar la aplicación de la ley en cuestiones de ciberseguridad.
- **Legislación sobre delitos cibernéticos.** Prácticamente todos los países analizados en este estudio son signatarios del Convenio de Budapest; por lo tanto, deben promover iniciativas para combatir el ciberdelito según los lineamientos de dicho convenio. Específicamente, cerca del 42,1% de los signatarios mencionan medidas relacionadas con la legislación sobre el ciberdelito en su estrategia.

En esta área de interés, se evalúan aspectos relacionados con el desarrollo de un marco legal y regulatorio, no solo para proteger a la sociedad contra la ciberdelincuencia y promover un entorno cibernético seguro, sino también como base para el desarrollo de los objetivos deseados por la estrategia. No se pueden lograr mejoras sustanciales sin un marco normativo que respalde los cambios y permita su sostenibilidad en el tiempo.

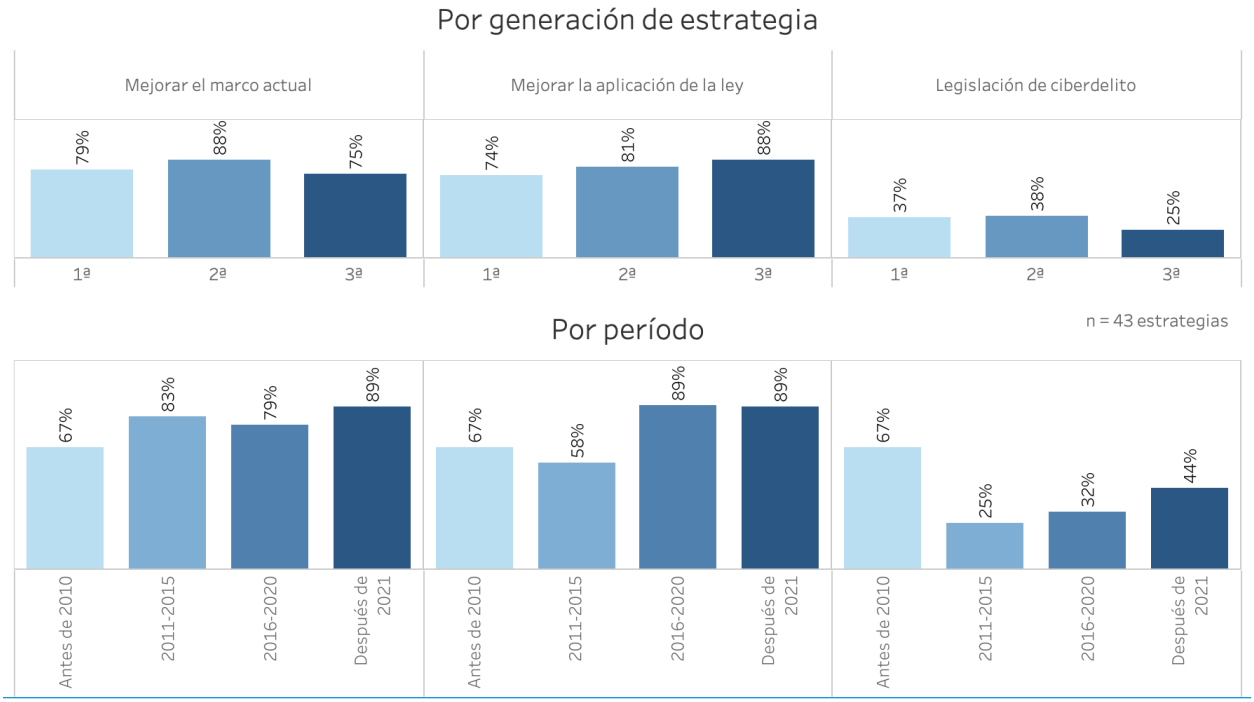
La importancia de mejorar el marco normativo es evidente, tanto es así que el 84,2% de

**GRÁFICO 23 – ÁREA DE INTERÉS: LEGISLACIÓN Y MARCO NORMATIVO**



## GRÁFICO 24 – EVOLUCIÓN DEL ÁREA DE INTERÉS: LEGISLACIÓN Y MARCO NORMATIVO

Evolución de la presencia de los mecanismos en las estrategias analizadas




las estrategias vigentes mencionan este tema. Algo similar ocurre cuando se observa la mención de este tema en las estrategias por generación, donde su inclusión es, en su mayoría, alta. Es interesante ver cómo las estrategias mejoran su estructura actual de diferentes maneras y con diferentes alcances. Por ejemplo, en su tercera estrategia, el plan de acción de Colombia, en el marco de la actividad "Fortalecer las capacidades de seguridad digital de los ciudadanos, el sector público y el sector privado para aumentar la confianza digital en el país" declara, en el punto diez, que "El Ministerio de Justicia y del Derecho, con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, la Procuraduría General de la Nación, el Ministerio de Defensa Nacional, con el apoyo de las entidades públicas y privadas que consideren apropiadas, diagnosticará y recomendará soluciones para los posibles problemas existentes en el marco normativo actual que puedan afectar (i) el ejercicio libre y pacífico de la ciudadanía digital; (ii) la defensa y la seguridad nacionales, y (iii) la prosecución, investigación y sanción de la comisión de conductas punibles mediante el uso de Tecnologías de la Información y las Comunicaciones (TIC)". Argentina, por su parte, establece el objetivo número 6 exclusivamente para el desarrollo de un marco normativo. Este objetivo busca generar, adaptar, actualizar y adoptar marcos regulatorios, normas y protocolos para enfrentar los desafíos generados por los riesgos del ciberespacio, y así garantizar el respeto a los derechos fundamentales.

Una mejor aplicación de la ley es un tema presente en el 84,2% de las estrategias vigentes. Es interesante notar el aumento de la presencia de la aplicación de la ley a lo largo del tiempo y de las generaciones de estrategias, mientras que disminuye la mención de la legislación contra el ciberdelito también a lo largo del tiempo y de las generaciones de estrategias. Esto podría indicar que, inicialmente, los países se concentran en

fortalecer la legislación y, al alcanzar este objetivo, incrementan la aplicación de la ley y fortalecen las fuerzas de investigación y combate. La estrategia de los Estados Unidos menciona este tema en varias ocasiones y lo presenta como un esfuerzo transversal, integrado en varios de los objetivos, ya sea a través de la capacitación, de los organismos nacionales o de acuerdos internacionales.

Con respecto a la legislación sobre ciberdelitos, se observa una baja presencia en las estrategias vigentes; únicamente el 42,1% de las estrategias mencionan este tema. También se observa una mención decreciente tanto por año como por generación de estrategia. Cabe señalar que prácticamente todos los países de este estudio son signatarios del Convenio de Budapest. Solo Nueva Zelanda y Corea no son miembros plenos, pero están invitados a unirse, ya que actualmente participan como observadores. Para adherirse al Convenio de Budapest, es esencial cumplir con varios requisitos. Entre ellos, se incluye la necesidad de crear una legislación que esté en conformidad con las disposiciones del convenio sobre ciberdelitos. Por consiguiente, si bien el porcentaje de menciones de este tema es bajo, este debe abordarse en otro contexto, es decir, en la legislación sobre ciberdelitos.

### 5.7.7. *Área de interés: privacidad y datos*

**PUNTOS CLAVE DE LA SECCIÓN**

- **Protección de datos y privacidad.** Aunque no suele ser la sección principal de las estrategias, se menciona la protección de datos y la privacidad en casi el 80% de las estrategias vigentes analizadas.
- **Seguridad por diseño.** Con una evidente tendencia creciente, el concepto asumió un papel protagónico de manera rápida, ya que está presente en el 67% de las estrategias publicadas después de 2020.

En el área de interés de la privacidad de datos, se abordan diversos temas que, aunque están relacionados, presentan perspectivas significativamente diferentes. Esto se debe a que algunos de ellos, como la propiedad intelectual, existen desde hace mucho tiempo, mientras que otros, como la privacidad por diseño, surgieron en la última década. En términos generales, la protección de datos tuvo un gran avance en los últimos años; muchos países dictaron leyes relacionadas con el tema y definieron iniciativas que cambiaron el paradigma de cómo deben protegerse los datos. El principal ejemplo es el Reglamento General de Protección de Datos (RGPD) de la UE,[24] que se refiere a la protección de los individuos con respecto al procesamiento de sus datos personales y a la libre circulación de dichos datos dentro de la UE y del Espacio Económico Europeo, así como a la transferencia de datos personales fuera de ellos. El objetivo principal es mejorar el control y los derechos de los individuos sobre sus datos personales y simplificar el entorno regulatorio para los negocios internacionales.

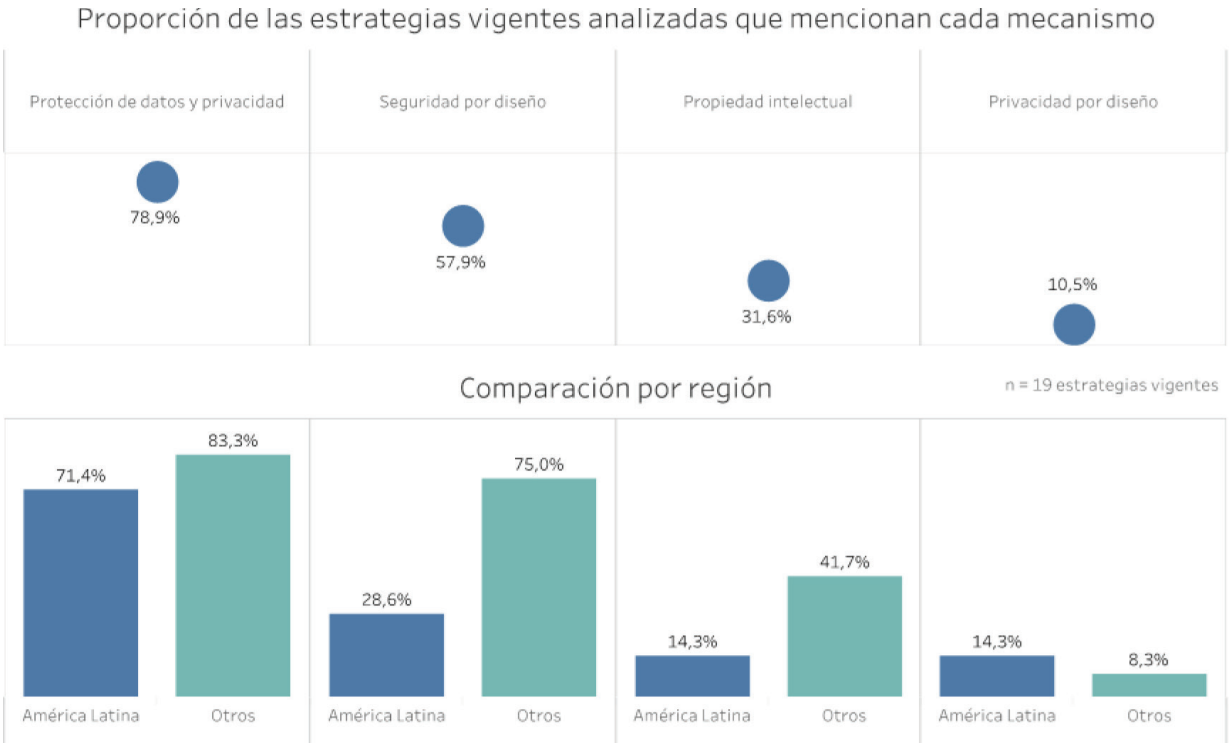
En relación con la presente área de interés, la Organización de los Estados Americanos (OEA), en su publicación *Principios actualizados sobre la Privacidad y la Protección de Datos Personales*,[25] establece los siguientes 13 principios que reflejan los diferentes enfoques predominantes en los Estados miembros sobre las cuestiones centrales de la protección de los datos personales.

- Objetivos legítimos y justicia
- Transparencia y consentimiento
- Relevancia y necesidad
- Procesamiento y retención limitados
- Confidencialidad
- Seguridad de los datos

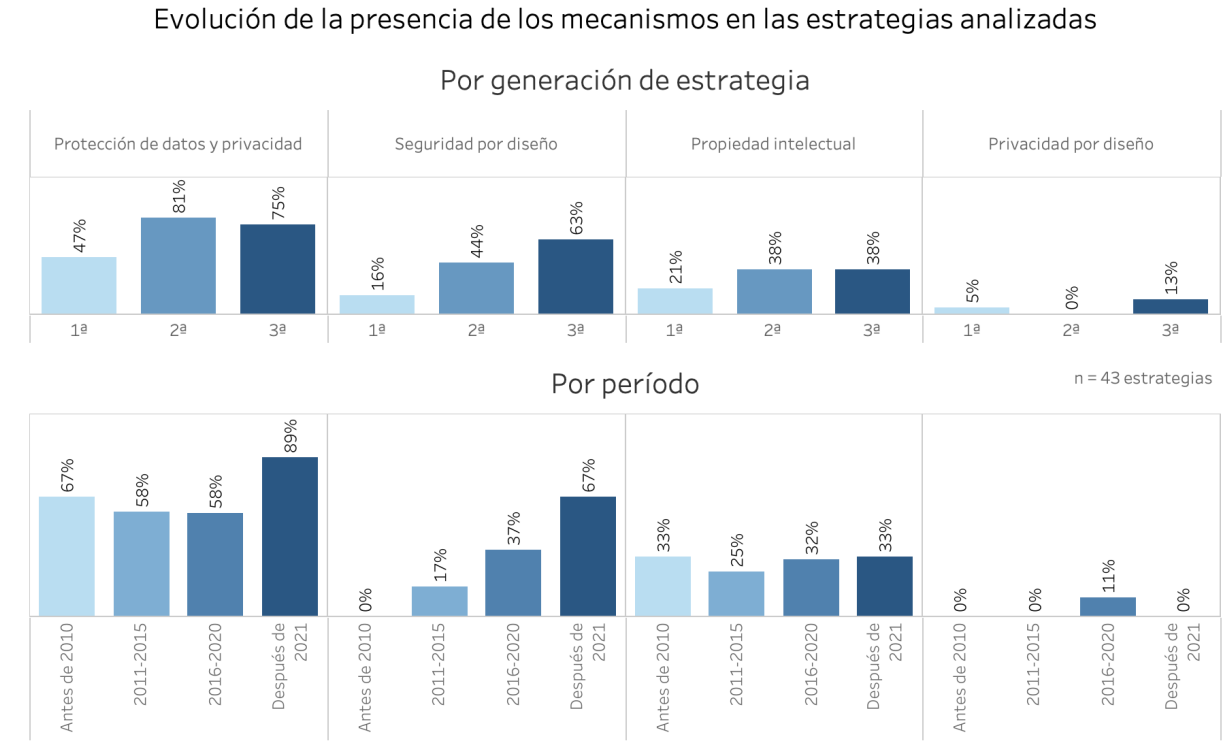
[24] Reglamento General de Protección de Datos. https://gdpr.eu/tag/gdpr/.

[25] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, OEA. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf.

## GRÁFICO 25 – ÁREA DE INTERÉS: PRIVACIDAD Y DATOS




## GRÁFICO 26 – EVOLUCIÓN DEL ÁREA DE INTERÉS: PRIVACIDAD Y DATOS



- Exactitud de los datos
- Acceso, rectificación, supresión, cancelación, oposición y portabilidad
- Datos personales sensibles
- Responsabilidad y obligación
- Flujo de datos transfronterizos y responsabilidad
- Excepciones
- Autoridad de protección de datos

El tema de la protección de datos y la privacidad se aborda, aunque superficialmente, en el 78,9% de las estrategias vigentes, con un margen ligeramente menor en América Latina (71,4%) que en el Norte Global (83,3%). La presencia de este tema se registra desde hace cierto tiempo y continúa creciendo a partir de la segunda generación de estrategias. Colombia, en el punto 5.3.3 de su plan de acción de la estrategia, define: "Analizar la adopción de modelos, estándares y estructuras de seguridad digital, con énfasis en nuevas tecnologías para preparar al país para los desafíos de la cuarta revolución industrial (4RI)" y establece lo siguiente en relación con la protección de datos: "En primer lugar, la Secretaría Administrativa de la Presidencia de la República, a través del coordinador nacional de seguridad digital, formulará el decreto reglamentario para la aplicación y el uso de estándares, modelos, normas y herramientas que permitan la adecuada gestión de los riesgos de seguridad digital y la respuesta a incidentes en el sector. Lo anterior tiene como objetivo generar confianza en los procesos de las entidades públicas, garantizar la protección de los datos personales y la inclusión, así como actualizar permanentemente las políticas de seguridad y confianza digital".

Israel se refiere a los temas de protección de datos cuando menciona los desafíos de seguridad relacionados con la inteligencia artificial. En la sección sobre la preparación para las tecnologías emergentes de su estrategia, se indica lo siguiente: "A menudo, los datos para el entrenamiento se crearon antes de que se entendiera el aprendizaje automático y, a veces, provienen de fuentes desinformadas. Esto representa un desafío de seguridad porque los individuos se convierten en microobjetivos de los ataques de una manera sin precedentes. Los datos biométricos son particularmente sensibles, de modo que las bases de datos biométricos de Israel para la identificación segura están sumamente protegidas y reguladas por ley. Se está trabajando en la recopilación segura de datos y en el entrenamiento de la inteligencia artificial (IA). Se investigan los ataques a la privacidad. Se estudian soluciones técnicas de anonimización".

En cuanto al tema de seguridad por diseño, se observa un aumento notable de su presencia a lo largo de los años. No se lo mencionaba en las estrategias anteriores a 2010 y, actualmente, está presente en el 67% de las más recientes. Como se indicó anteriormente, este es un ejemplo de un tema que, si bien se desarrolló en la década de 1970, cobró especial importancia en el ámbito de las estrategias nacionales en los últimos años. Por ejemplo, las normas ISO/IEC 27000 mencionan este principio. En el objetivo 3 "Protección y recuperación de los sistemas de información del sector público" de su segunda estrategia, Argentina establece: "Promover la seguridad desde el diseño y en todas las fases de la implementación y adopción de proyectos tecnológicos del sector público nacional, garantizando estándares adecuados para la protección de datos personales y seguridad de la información".

En cuanto al tema de la propiedad intelectual, se observa poca presencia en las estrategias actuales (31,6%). En América Latina, la mención de la propiedad intelectual es aún menor, lo cual se corrobora por la tendencia de los países del Norte Global a ser productores más fuertes de nuevas tecnologías. Si bien es un tema que se mantiene en el tiempo, el aumento de su abordaje en las estrategias es notable cuando se consideran las diferentes

generaciones de estrategias. España establece una medida clara para la línea de acción 5 de su segunda estrategia. Allí define: "Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad y seguridad por diseño, fomentando específicamente aquellas que apoyen las necesidades de interés nacional para fortalecer la autonomía digital y la propiedad intelectual e industrial".

La privacidad por diseño es un tema relativamente nuevo, poco presente en las estrategias actuales (se menciona únicamente en el 13% de las que están vigentes). Estonia, en su tercera estrategia, define una de sus actividades prioritarias de la siguiente manera: "El desarrollo de nuevos servicios y bases de datos cumplirá con los principios de seguridad y privacidad desde la concepción. Se abandonarán las plataformas obsoletas (principio de sin sistemas heredados [*no legacy*]). Con este fin, se desarrollará un recurso de consultoría de arquitectura de seguridad central".

### 5.7.8. *Área de interés: defensa y capacidad militar*

**PUNTOS CLAVE DE LA SECCIÓN**

- **Capacidades militares.** Si bien el 42,1% de las estrategias actuales mencionan la mejora de las capacidades militares, se debe tener en cuenta que esto no siempre se aborda en las estrategias de ciberseguridad, sino más bien, en las estrategias de defensa o seguridad nacional.

Los temas de mejora de las capacidades militares y la ciberdefensa ofensiva no son los más populares entre las estrategias analizadas. Es importante tener en cuenta dos aspectos principales a la hora de analizar estas cuestiones. En primer lugar, al igual que con otros temas, es posible que la cuestión se aborde en otra estrategia,

**GRÁFICO 27 – ÁREA DE INTERÉS: DEFENSA Y CAPACIDAD MILITAR**

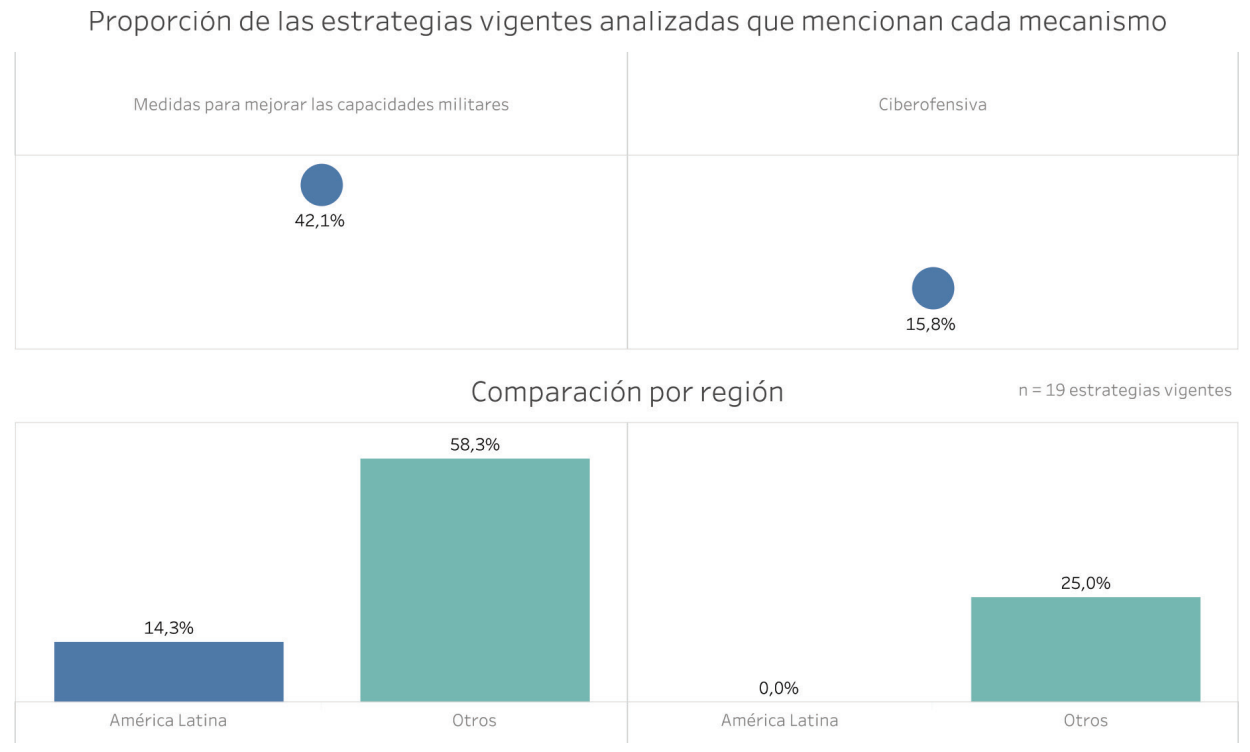
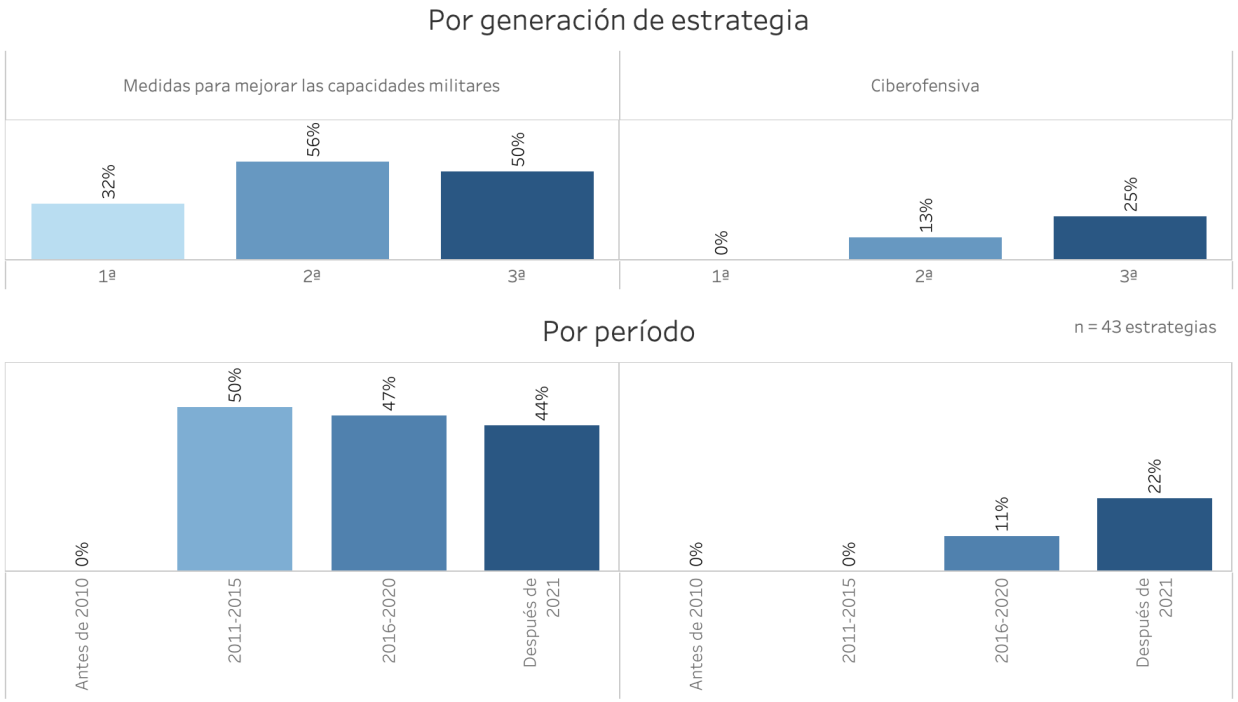


**GRÁFICO 28 – EVOLUCIÓN DEL ÁREA DE INTERÉS: DEFENSA Y CAPACIDAD MILITAR**

Evolución de la presencia de los mecanismos en las estrategias analizadas




como la de seguridad nacional o la de defensa nacional; por lo tanto, el hecho de que no esté presente en la estrategia no significa que no sea una preocupación del país. En segundo lugar, si bien estos son temas comunes a todos los países, la prioridad y la urgencia de abordar esta cuestión dependen, en gran parte, del contexto. Al contrario de otros temas, como el desarrollo de capacidades o la resiliencia, que son claros e igualmente importantes para todos los países, la importancia de estos puede estar abierta a discusión.

Específicamente sobre el tema de la mejora de las capacidades militares, el 42,1% de las estrategias actuales lo mencionan. Si bien, en general, esta cuestión se trata en una proporción similar en las estrategias, en distintos períodos, se observa un aumento desde el punto de vista de las generaciones de estrategias. Esta variación oscila entre un 32%, en la primera generación de estrategias, y un 50% en la tercera generación. A continuación, se incluyen algunos ejemplos ilustrativos.

- "La ciberseguridad se incluirá continuamente como parte de la defensa nacional. Con este fin, se integrará aún más en los documentos de planificación de la seguridad nacional (el plan de desarrollo y el plan de actividades de defensa nacional) y se llevarán a cabo regularmente ejercicios conjuntos con proveedores de servicios esenciales, formuladores de políticas sénior y organizaciones de defensa nacional" (actividad prioritaria, Estonia, 2022).
- "Mejorar la defensa cibernética y las capacidades de inteligencia cibernética"[...] "Implementar medidas activas de defensa cibernética en el sector público con el objetivo de mejorar las capacidades de respuesta" (línea de acción 1, medidas 6 y 12, España, 2019).

Existe una diferencia significativa entre las regiones, con una alta presencia del tema fuera de América Latina (58,3%) y baja en la región (14,3%).

El tema de la ciberseguridad ofensiva en el contexto militar tiene una presencia reducida; solo se menciona en el 15,8% de las estrategias vigentes. Si bien hay un aumento en su mención en las estrategias, cuando se observa desde el punto de vista de las generaciones de estrategias, pocos países lo incluyen y estos siempre pertenecen al Norte Global. Por ejemplo, en las estrategias estudiadas, este tema se menciona a continuación.

- "Los Estados que no comparten los desafíos impuestos por una Internet libre y abierta aprovechan el tema de la ciberseguridad para promover sus visiones autoritarias del ciberespacio, con el pretexto de defender la seguridad. El Reino Unido adoptará un enfoque más proactivo, y trabajará con aliados y socios para garantizar que las reglas y estructuras internacionales se alineen con sus valores democráticos. El objetivo es apoyar el crecimiento económico nacional y mundial y la seguridad colectiva, incentivar el uso responsable de herramientas cibernéticas ofensivas y consecuencias reales para las herramientas maliciosas e irresponsables. Para 2025, se alcanzarán los siguientes resultados" (párrafo 160, objetivo 2, Reino Unido, 2022).

## RECUADRO 10 – ESTUDIO DE CASO
### EVOLUCIÓN DE LAS ESTRATEGIAS DE CIBERSEGURIDAD EN EL REINO UNIDO

El Reino Unido ya cuenta con su tercera estrategia de ciberseguridad publicada y el enfoque de cada estrategia es una ilustración interesante de la evolución de algunos aspectos clave. Al comparar la primera y la segunda estrategia, se observan algunos cambios significativos, especialmente en relación con el papel del sector privado. Mientras que, en la transición de la segunda a la tercera estrategia, se observa un papel más asertivo del Reino Unido y un cambio del enfoque de la ciberseguridad al poder cibernético. A continuación, se incluye una breve reseña de la evolución de las estrategias.

Primera estrategia (2011)
La primera estrategia de ciberseguridad de 2011 estableció las bases para el enfoque del Reino Unido hacia el ciberespacio. En esencia, priorizó el valor económico del ciberespacio y organizó los objetivos en torno a la ciudadanía, el empresariado y el Gobierno. Los principales objetivos incluían combatir el delito cibernético de modo que el país fuera un lugar seguro para los negocios en línea, aumentar la resiliencia contra los ataques, fomentar un ciberespacio abierto y estable, y garantizar que la nación tuviera el conocimiento y las habilidades necesarias para alcanzar estas metas. De manera pionera, la estrategia estableció un presupuesto específico destinado al Programa Nacional de Ciberseguridad y destacó la importancia de la cooperación entre el sector privado y el sector público. En general, la estrategia presentó un enfoque más orientado a incentivos y lineamientos con la esperanza de que el sector privado fortaleciera su postura con respecto a la seguridad.

Segunda estrategia (2016)
Con base en la estrategia de 2011 y en el lanzamiento del Centro Nacional de Ciberseguridad, la estrategia de 2016 reconoció los avances logrados, pero menciona la necesidad de que el Gobierno asuma

*(continúa en la página siguiente)*

**RECUADRO 10 – ESTUDIO DE CASO** *(continuación)*

un papel más proactivo. La estrategia menciona que "un enfoque basado en el mercado para la promoción de la ciberseguridad no produjo ni el ritmo ni la escala de cambio necesarios; por lo tanto, el Gobierno necesita liderar el camino e intervenir de manera más directa, a través del ejercicio de su influencia y el uso de sus recursos para enfrentar las amenazas cibernéticas". La propia creación del Centro Nacional de Ciberseguridad indica la búsqueda de un papel más proactivo del Gobierno. Además de los lineamientos, como en la primera estrategia, ahora se enfatiza más en los incentivos y en las reglamentaciones.

Tercera estrategia (2021)

La estrategia más reciente, lanzada en 2021, cambia el énfasis de la ciberseguridad al poder cibernético. En esta tercera generación, redactada con un lenguaje más asertivo, el Reino Unido entiende el ciberespacio como un escenario central en donde compiten países democráticos y autocráticos. Desde este punto de vista, también hay un cambio en el alcance, ya que la segunda estrategia mencionaba un enfoque de todo el Gobierno y ahora, pasa a la visión de toda la sociedad. Este enfoque se materializa en la creación de una Junta Asesora Cibernética Nacional, que respalda al Gobierno en la implementación de la estrategia. En este sentido, además de la atención en la seguridad, la estrategia se centra especialmente en cómo utilizar el ciberespacio para obtener ventajas económicas y sociales.

La evolución de las estrategias nacionales de ciberseguridad del Reino Unido demuestra una transición de enfoques impulsados por el mercado hacia un papel más proactivo del Gobierno, que culmina con la priorización del poder cibernético como un activo nacional esencial. Esta evolución representa un reconocimiento más amplio de la importancia del ciberespacio, no solo en términos de seguridad, sino también como ámbito de competencia y cooperación económica, social y geopolítica.

Fuentes:

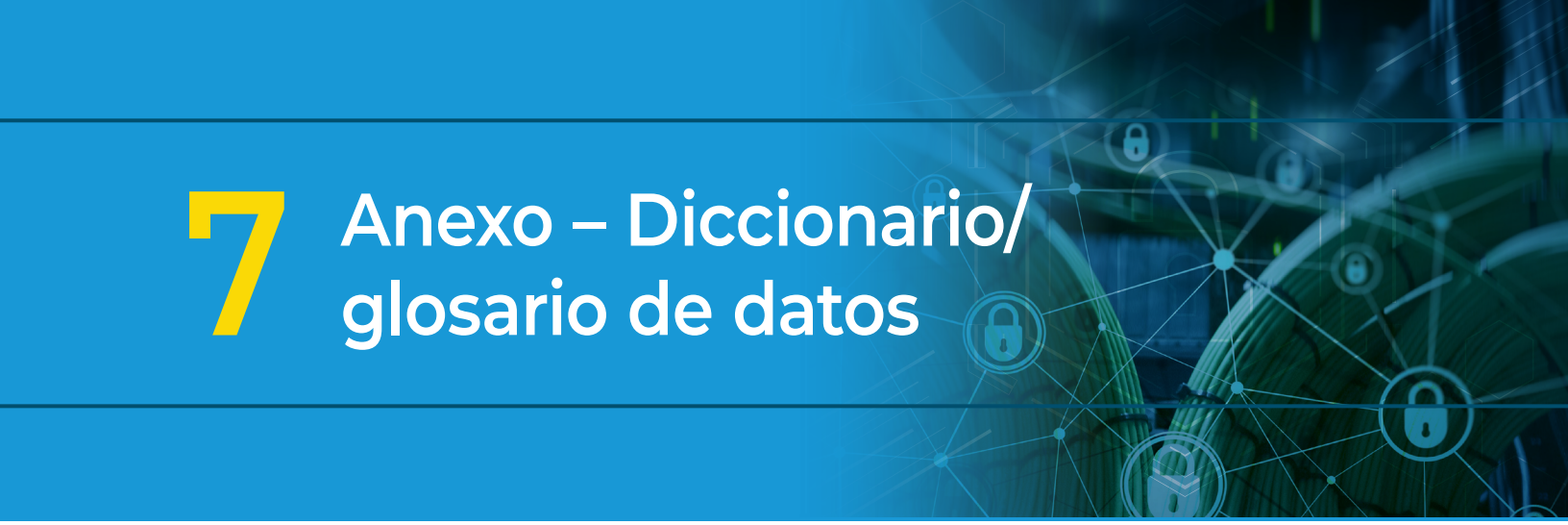
- Análisis de las tres estrategias
- https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037
- https://www.holyrood.com/news/view,the-uks-national-cyber-strategy-2022-an-evolution

# 6 Consideraciones finales

Este estudio, basado en un análisis documental de 43 estrategias, logró identificar macrotendencias en la evolución de las estrategias de ciberseguridad en el mundo. Como se demostró, las nuevas estrategias no solo son más ejecutivas y orientadas a la acción, sino que también suelen apuntar a un universo más amplio en términos de ciberseguridad. Además, se entiende que la ciberseguridad es un concepto amplio que sobrepasa las cuestiones de seguridad nacional e incluye la prosperidad y el desarrollo socioeconómico. A lo largo del estudio, se identificaron patrones de cambio y tendencias en diferentes áreas de interés y se presentaron ejemplos de la dirección adoptada por los países que alcanzaron mayor madurez en esta temática.

Si bien existen tendencias importantes, cada país debe efectuar un análisis específico según su situación, prioridades y capacidades individuales. En este proceso, la consulta y la inclusión de diversas partes interesadas, como el Gobierno, la sociedad civil, la academia y el sector privado, se convierten en pasos esenciales para garantizar la legitimidad de la estrategia de ciberseguridad en el país, y la transforman en un documento de referencia para estas partes.

Por este motivo, adoptar un proceso colaborativo que incorpore los avances y las lecciones aprendidas de la implementación de las primeras estrategias se presenta como un enfoque crucial para los países que están desarrollando sus segundas o terceras estrategias. Este camino no solo fortalece el compromiso y la cooperación, sino que también contribuye a la evolución continua y a la adaptabilidad de las estrategias de ciberseguridad en un escenario dinámico y en constante cambio.



# 7 Anexo – Diccionario/ glosario de datos

En este anexo, se detallan las categorías de análisis utilizadas para definir los criterios que permitieron determinar si las estrategias cumplían un determinado aspecto o no. El orden del glosario se correlaciona con el orden en que aparecen los gráficos en este documento.

## Gráfico 1 – Estructura

- **Tiene objetivos.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente los objetivos estratégicos, los objetivos generales, los pilares estratégicos, los subobjetivos o alguna categoría similar.
- **Tiene principios.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente el uso de principios.
- **Tiene una visión.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento enuncia explícitamente una visión o incluye la visión en alguna sección. En algunas estrategias, se consideró el propósito, siempre y cuando el texto mencionara la orientación futura en el área.
- **Tiene indicadores/métricas.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento utiliza explícitamente indicadores cuantitativos o métricas cualitativas para medir el éxito y verificar el logro de las propuestas de la estrategia. No se tuvieron en cuenta aquellas estrategias que indicaban que los indicadores se elaborarían en una etapa posterior.

## Gráfico 2 – Área de interés: gobernanza e institucionalidad

- **Mecanismos de coordinación intragubernamental.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona líneas de acción, intervenciones u objetivos destinados a aumentar la coordinación entre diferentes organismos y departamentos del Gobierno. Cabe destacar que los mecanismos son más específicos en algunas estrategias (por ejemplo, consejos, comités o grupos de trabajo), mientras que son más genéricos en otras.
- **Mecanismos de coordinación público-privada.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona líneas de acción, intervenciones u objetivos destinados a aumentar la coordinación entre los sectores público y privado. Cabe destacar que los mecanismos son más específicos en algunas estrategias (por ejemplo, consejos, comités o grupos de trabajo), mientras que son más genéricos en otras.
- **Reconocimiento de una autoridad en ciberseguridad.** Se consideró que una

estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente el nombre del organismo o departamento responsable de la ciberseguridad (en caso de que ya estuviese creado) o sirve de base para definir al organismo o departamento responsable. Asimismo, se consideró que una estrategia cumplía los criterios de esta categoría cuando la autoridad aborda los temas de ciberseguridad de forma amplia y específica para la implementación de la estrategia.

- **Definición de un plan operativo (actual o futuro).** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento incluye un plan operativo actual o futuro o menciona explícitamente que la elaboración de un plan de acción será un resultado de la publicación de la estrategia.
- **Cita de entidades subnacionales.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona al menos una acción que incluye a los gobiernos subnacionales (provincias, regiones, estados, municipalidades, gobiernos locales, comarcas o divisiones similares, según el país).
- **Norma asociada.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona el instrumento (decreto, resolución o similar), incluido el número que permite identificarlo, que autorizó la publicación de la estrategia. No se efectuó ninguna investigación externa adicional de la estrategia para verificar la existencia de una norma asociada.
- **Indicación clara de los responsables.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente quién es el responsable de la implementación de las acciones indicadas. Asimismo, se consideró que una estrategia señala claramente a los responsables cuando una sección del documento describe los pasos de implementación en detalle e identifica a los actores.
- **Presupuesto asociado.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente la asignación de un presupuesto, la estimación de los costos para la implementación de la estrategia (o la confirmación de que se realizará una estimación en breve, poco tiempo después). No se analizaron los presupuestos propiamente dichos.

## Gráfico 4 – Tipos de amenaza

- **Ciberdelitos/ciberataques.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente los ciberdelitos o ciberataques como amenazas en el ciberespacio.
- **Otros países/guerra cibernética.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente las amenazas provenientes de otros estados o las guerras en el ciberespacio.
- **Espionaje.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente el espionaje como una amenaza. A menudo, este concepto se correlacionaba con la categoría anterior.
- **Terroristas.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente al terrorismo o a los terroristas como amenaza.
- **Ataques a la democracia.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona las amenazas relacionadas con la manipulación de las elecciones o las creencias

democráticas, la desinformación destinada a socavar la democracia o categorías similares.

- **Extremistas.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente a los extremistas o a la polarización política o religiosa en el ciberespacio.
- ***Hacktivistas.*** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente el término *hacktivistas* o *hackers*.
- **Desastres naturales.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente los riesgos naturales (terremotos, deslizamientos de tierra, inundaciones) como tipos de amenaza para el ciberespacio del país.

## Gráfico 6 – Tipos de principios

- **Derechos humanos.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento menciona los derechos humanos, los valores democráticos, los derechos fundamentales o algún concepto relacionado con las libertades civiles en la sección correspondiente a los principios. No se incluyeron aquellas estrategias en que alguno de estos temas se menciona en una sección diferente.
- **Visión holística/coordinada.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento, en la sección correspondiente a los principios, menciona la necesidad de contar con un enfoque integrado u holístico o algún principio centrado en aumentar la coordinación entre los diferentes actores involucrados.
- **Cooperación internacional.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona algún principio rector centrado en la cooperación internacional o la acción global en la sección correspondiente a los principios.
- **Ciberseguridad como parte de la seguridad nacional.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye alguna mención más amplia relacionada con la seguridad nacional en la sección correspondiente a los principios.
- **Prosperidad económica.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún principio orientado a la prosperidad económica o, al menos, utiliza términos como prosperidad económica, oportunidad económica, promoción industrial, desarrollo económico o similares en la sección correspondiente a los principios.
- **Concientización/responsabilidad individual.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún principio orientado al ciudadano o usuario final y/o hace hincapié en la sensibilización o concientización de los riesgos del ciberespacio en la sección correspondiente a los principios.
- **Transparencia/confianza.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún principio orientado al aumento de la transparencia o confianza en el ciberespacio y/o de las políticas de ciberseguridad en la sección correspondiente a los principios.
- **Proporcionalidad.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún principio que menciona el término proporcionalidad o el sentido de calibrar las acciones de ciberseguridad en relación con la magnitud del riesgo en la sección correspondiente a los principios.

## Gráfico 8 – Tipos de objetivos

- **Preparación y resiliencia.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento menciona explícitamente mejoras en la resiliencia, disponibilidad o preparación para responder a los ataques entre los objetivos de más alto nivel.
- **Capacidades/desarrollo de capacidades.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún objetivo orientado a mejorar las capacidades (del país o Gobierno), ampliar el conocimiento en el país, ampliar la capacidad de respuesta o las acciones relacionadas con los profesionales y la educación entre los objetivos de más alto nivel.
- **Cooperación internacional.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento menciona algún objetivo orientado a la cooperación internacional o acción global entre los objetivos de más alto nivel.
- **Cooperación público-privada.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento menciona algún objetivo para ampliar la cooperación con el sector privado entre los objetivos de más alto nivel.
- **Infraestructura crítica.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye el concepto de infraestructura crítica entre los objetivos de más alto nivel.
- **Promoción industrial.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún objetivo orientado al sector económico de la ciberseguridad en el país o a expandir la prosperidad económica de forma más abarcadora entre los objetivos de más alto nivel.
- **Cultura de ciberseguridad/concientización.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún objetivo orientado a la cultura de forma amplia y/o a la necesidad de aumentar la concientización de las diferentes partes, en especial de los usuarios individuales, entre los objetivos de más alto nivel.
- **Desarrollo normativo.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento menciona de alguna forma las mejoras en el marco legal, normativo o regulatorio entre los objetivos de más alto nivel.
- **Confianza/transparencia.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento menciona de alguna forma el aumento de la confianza o transparencia en el ciberespacio o en las políticas de ciberseguridad entre los objetivos de más alto nivel.
- **Ciberespacio abierto.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento menciona la necesidad de un ciberespacio abierto o libre (o menciona explícitamente la Internet abierta o libre) entre los objetivos de más alto nivel.
- **Gestión de riesgos.** Se consideró que una estrategia cumplía los criterios de esta categoría solo si el documento incluye algún objetivo relacionado con la gestión de riesgos en cuestiones de ciberseguridad entre los objetivos de más alto nivel.

## Gráfico 11 – Gestión de riesgos

- **Define un enfoque para la gestión de riesgos.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona la necesidad de contar con un enfoque para la gestión de los riesgos en cuestiones de ciberseguridad. En

esta categoría, no se exigió la definición de la metodología, sino solamente el reconocimiento de la importancia de abordar la gestión de riesgos.

## Gráfico 13 – Preparación y resiliencia

- **Capacidad de respuesta a incidentes.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona la capacidad operativa de respuesta en caso de incidentes, incluidos los equipos de respuesta a incidentes, equipos de emergencia o similares (equipos de respuesta ante emergencias informáticas [CERT, por sus siglas en inglés], equipos de respuesta ante incidentes informáticos [CIRT, por sus siglas en inglés] y equipos de respuesta ante incidentes de seguridad informática [CSIRT], entre otros).
- **Promoción del intercambio de información.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona medidas (o intenciones) para aumentar el intercambio de información (ya sea intragubernamental o entre los sectores público-privado).
- **Ejercicios de ciberseguridad.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento fomenta la realización de ejercicios de ciberseguridad, incluidas las simulaciones o los ejercicios en tiempo real.
- **Planes de contingencia/gestión de crisis.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona medidas (o intenciones) para elaborar planes de contingencia para la gestión de las crisis.

## Gráfico 15 – Infraestructura crítica y servicios esenciales

- **Medidas para proteger las infraestructuras críticas.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento establece medidas o intenciones de establecer medidas para la protección de este tipo de infraestructura.
- **Cooperación con el sector privado (p/IC).** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento fomenta la colaboración público-privada para la protección de las infraestructuras críticas.
- **Medidas de protección de los activos de gobierno digital.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona la digitalización de servicios o la expansión del gobierno digital y la importancia de su protección.
- **Medidas para identificar las infraestructuras críticas del país.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente una medida o acción dirigida a identificar y nombrar a las infraestructuras críticas del país.

## Gráfico 17 – Capacidades y concientización

- **Innovación e I+D.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona acciones o medidas destinadas a aumentar la investigación y el desarrollo en el área de ciberseguridad o menciona políticas de innovación en el área.
- **Programas de concientización.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento

menciona medidas destinadas a aumentar la concientización de los usuarios en temas de ciberseguridad, incluyendo campañas, cursos, programas de sensibilización y concientización en el área.

- **Medidas en la educación superior.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona medidas relacionadas con las universidades; por ejemplo, cambios en los planes de estudio, aumento en el número de profesionales con doctorado, etc.
- **Medidas en la educación primaria/secundaria.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona medidas destinadas a estimular el desarrollo de competencias en niñas o niños y/o en la educación primaria/secundaria.
- **Medidas para la capacitación de profesionales.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona medidas destinadas a estimular el desarrollo de profesionales y la fuerza de trabajo en materia de ciberseguridad, excluidas las inversiones en educación superior.
- **Medidas para las competencias de los funcionarios públicos.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona medidas destinadas a estimular el desarrollo de las competencias de los funcionarios públicos o, de forma más amplia, de los organismos públicos (incluidas capacitaciones o competencias más abarcadoras).
- **Desarrollo de la industria para aumentar la soberanía.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona la promoción de la industria cibernética a fin de reducir la dependencia de soluciones extranjeras.
- **Desarrollo de la industria para oportunidades económicas.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona la promoción de la industria cibernética en relación con los objetivos de oportunidades económicas.
- **Medidas para el aumento de la diversidad.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona medidas destinadas a aumentar el número de mujeres, personas LGBTQ+ y/u otros grupos vulnerables o tradicionalmente subrepresentados en las áreas de ciberseguridad.

## Gráfico 21 – Cooperación internacional

- **Cooperación bilateral/con otros países.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento contiene medidas destinadas a aumentar la cooperación bilateral o amplia entre diferentes países en materia de ciberseguridad.
- **Alineación con iniciativas regionales/multilaterales.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona específicamente bloques o iniciativas regionales o globales (por ejemplo, la Organización del Tratado del Atlántico Norte [OTAN], la Unión Europea, etc.).

## Gráfico 23 – Legislación y marco normativo

- **Mejorar el marco actual.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona ampliamente la necesidad de introducir mejoras en el marco normativo actual.

- **Legislación sobre el ciberdelito.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente medidas dirigidas a la legislación relacionada con el ciberdelito.
- **Mejorar la aplicación de la ley.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona mejoras para procesar, castigar, investigar el ciberdelito y/o utiliza explícitamente el término "cumplimiento de la ley" o *law enforcement* en las estrategias en inglés.

## Gráfico 25 – Privacidad y datos

- **Protección de los datos y la privacidad.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento incluye preocupaciones e intenciones de avanzar en el área de la protección de datos y la privacidad. La estrategia no cumplía los criterios de esta categoría si el documento menciona solo uno de los dos conceptos.
- **Seguridad por diseño.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento menciona explícitamente el concepto.
- **Propiedad intelectual.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento incluye iniciativas específicas para la protección de la propiedad intelectual o una preocupación específica relacionada.
- **Privacidad por diseño.** Se consideró que una estrategia cumplía los criterios de esta categoría solo cuando el documento menciona explícitamente el concepto.

## Gráfico 27 – Defensa y capacidad militar

- **Medidas para mejorar las capacidades militares.** Se consideró que una estrategia cumplía los criterios de esta categoría cuando el documento contiene medidas relacionadas con las capacidades militares o la defensa.
- **Ciberofensiva.** Se consideró que una estrategia cumplía los criterios de esta categoría solo cuando el documento menciona explícitamente el concepto.


BID
Mejorando vidas