OPTIMICEMOS LA CIBERSEGURIDAD

Modelo de Madurez de Capacidad de Ciberseguridad para las Naciones

Panorama Nacional de Ciberseguridad

Argentina
2023

Secretaría de Innovación Pública

Jefatura de Gabinete de Ministros
Argentina

aws

OEA | Más derechos para más gente

Preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (cybersecurity@oas.org). Los contenidos expresados en este documento se presentan exclusivamente para fines informativos y no representan la opinión o posición oficial alguna de la Organización de los Estados Americanos, de su Secretaría General o de sus Estados Miembros.

Diseño y Diagramación
María Paula Lozano

Tabla de Contenido

Introducción

El programa **Optimicemos la Ciberseguridad**, es impulsado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), en conjunto con los equipos de Políticas Públicas y de Seguridad y Cumplimiento de Amazon Web Services (AWS) América Latina. Sus principales objetivos son: brindar apoyo técnico a los Estados Miembros de la OEA para desarrollar un marco integral y estratégico de planificación que les facilite avanzar en los objetivos socioeconómicos que dependen cada vez más de la seguridad del ciberespacio; facilitar la coordinación, sustentabilidad y escalada de los distintos esfuerzos de ciberseguridad contemplados a nivel nacional; y finalmente, desarrollar una hoja de ruta que, partiendo de las evaluaciones sobre el nivel de madurez actual de la ciberseguridad del país, logre definir estrategias y planes de acción que aceleren la madurez de la ciberseguridad. Para ello, se propone un modelo de alianza público-privado alineado con las mejores prácticas internacionales como plataforma de apoyo.

Como primer paso para el desarrollo de una hoja de ruta, el presente informe proporciona un estudio de análisis sobre el panorama actual de acuerdo con indicadores internacionales y el contexto nacional de Argentina en materia de ciberseguridad. El análisis está basado en estudios internacionales de referencia y en la investigación documental sobre políticas nacionales, mecanismos internos y documentación relevante proporcionada por el Gobierno de Argentina.

El documento está dividido en los siguientes capítulos:

- Como primer capítulo, esta introducción;

- El segundo capítulo presenta la estructura del Programa;

- El tercer capítulo presenta el Modelo de Madurez de Capacidad de Ciberseguridad para las Naciones (CMM) que es utilizado como marco de referencia para esta incitativa;

- El cuarto capítulo describe el contexto nacional junto con un diagnóstico del país en torno a temas relacionados con la ciberseguridad siguiendo el marco del CMM;

- Y finalmente, el quinto capítulo presenta la evolución y los avances en madurez de ciberseguridad que ha presentado Argentina entre el año 2016 y el año 2020, identificando avances y oportunidades basados en las dimensiones del CMM. El estudio está principalmente soportado en el reporte publicado por la OEA y el BID en el año 2016 “Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?”[1] y en el reporte “Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe” publicado en el año 2020.[2]

1. https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean
2. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

I. Programa: Optimicemos la Ciberseguridad

A medida que los países de la región avanzan en materia de ciberseguridad, la coordinación nacional es imperativa para encaminar los esfuerzos de forma coordinada y sustentable. **Optimicemos la Ciberseguridad** brinda un análisis estratégico que propone opciones para acelerar el nivel de madurez de ciberseguridad de un país. El impacto se verá reflejado en los próximos informes de la OEA y el BID que analizarán el progreso del nivel de madurez de ciberseguridad de los países de la región. Asimismo, el programa aspira a introducir al país beneficiario a evaluaciones de ciberseguridad relevantes, brindando apoyo técnico a los Estados Miembros de la OEA en la identificación de sus prioridades, desafíos y oportunidades para progresar en su respectivo nivel de madurez de ciberseguridad.

Durante la implementación del programa, se elaboran dos herramientas de estudio en colaboración con el Gobierno. El primer entregable es el presente informe sobre el panorama nacional y los avances del país entre 2016 y 2020 en materia de ciberseguridad. Una vez el informe es avalado por el Gobierno, dicho informe puede difundirse y/o presentarse a otras instituciones del sector público para generar concientización sobre el nivel actual de madurez de la ciberseguridad nacional y la priorización de la ciberseguridad a nivel gubernamental.

Panorama Nacional y Análisis CMM 2016 y 2020	Consulta de evaluación basada en una dimensión del CMM	Hoja de Ruta
Informe sobre el nivel actual de madurez de la ciberseguridad nacional y análisis comparativo sobre el progreso del nivel de capacidad nacional conforme al CMM entre 2016 y 2020.	Difusión de un breve cuestionario y consulta con las partes interesadas pertinentes para llevar a cabo una evaluación detallada de en una Dimensión del CMM que el Gobierno identifique como prioritaria.	Informe final que reúne el análisis de los datos recopilados, proporcionando recomendaciones y conclusiones accionables a fin de avanzar hacia el siguiente nivel de madurez en ciberseguridad deseado.

Figura 1.1 Proceso de implementación del Programa de Optimicemos la Ciberseguridad

Basado en el primer análisis, el Gobierno identifica una Dimensión del CMM prioritaria para llevar a cabo una evaluación nacional más detallada, a fin de identificar fortalezas, brechas y oportunidades para mejorar el nivel de madurez de la dimensión seleccionada. La evaluación de la Dimensión priorizada se lleva a cabo mediante una consulta con las entidades gubernamentales pertinentes y sectores relevantes. Para complementar la información adquirida en la consulta, se desarrolla y difunde entre las partes interesadas un breve cuestionario que permite la recopilación de datos cuantitativos y cualitativos que informan los resultados y recomendaciones para desarrollar un marco de acción para el mejoramiento de dicha dimensión.

La última fase del programa culmina en el desarrollo y presentación de la "Hoja de Ruta" como informe final. La Hoja de Ruta representa la segunda herramienta de estudio, la cual enmarca los resultados y el análisis de la consulta de la dimensión priorizada del CMM, evalúa los datos recopilados durante todo el transcurso del programa y proporciona recomendaciones accionables para avanzar el nivel de madurez de la ciberseguridad nacional.

II. Modelo de Madurez de Capacidad de Ciberseguridad para las Naciones (CMM)

La metodología CMM fue publicada en 2013 y se somete a revisión periódica para garantizar que se mantenga actualizada. La revisión más reciente fue publicada en 2021.[3] El Programa de Optimicemos la Ciberseguridad utiliza la última edición de la metodología del CMM con distintos propósitos y usos, entre ellos:

- Comparar la madurez de la capacidad de ciberseguridad del país;
- Detallar un conjunto pragmático de acciones necesarias para contribuir al avance de las brechas de madurez;
- Determinar prioridades para la inversión y el fomento de capacidades actuales y futuras sobre la base de las necesidades específicas del país.

El CMM es un marco metódico diseñado por el Centro de Capacidades de Ciberseguridad Global (GCSCC, por sus siglas en inglés) de la Universidad de Oxford para evaluar la capacidad de ciberseguridad de un país como mecanismo para lograr una mejor comprensión del estado de su capacidad actual en materia de ciberseguridad y que sea de utilidad en el diseño de las políticas e iniciativas que contribuyan a incrementar su nivel de ciber-resiliencia.

La evaluación permite conocer en que etapa de madurez de ciberseguridad se encuentra un país en una escala del 1 al 5; 1 significando etapa inicial y 5 representando una etapa avanzada (Figura 2.1).

[3] https://gcscc.ox.ac.uk/the-cmm

»Dinámica (5): En esta etapa existen mecanismos claros para modificar la estrategia nacional según las circunstancias predominantes como la tecnología del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación (por ejemplo, ciberdelincuencia o privacidad). También hay evidencia de liderazgo global en temas de ciberseguridad. Los sectores clave, al menos, han elaborado métodos para cambiar las estrategias en cualquier etapa de su desarrollo. La toma de decisiones rápida, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.

Figura 2.1 Las cinco Etapas de madurez de la capacidad de ciberseguridad

»Estratégica (4): Se han hecho elecciones sobre qué partes del aspecto son importantes y cuáles son menos importantes para la nación. La etapa estratégica refleja el hecho de que se han hecho estas elecciones, condicionadas a las circunstancias particulares del país.

»Consolidada (3): Los indicadores del aspecto están establecidos y la evidencia muestra que están funcionando. Sin embargo, no existe una consideración bien pensada de la asignación relativa de recursos. Se han tomado pocas decisiones de compensación con respecto a la inversión relativa en los diversos elementos del aspecto, pero el aspecto es funcional y está definido.

»Formativa (2): Algunas características del aspecto han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizadas, mal definidas o simplemente nuevas. Sin embargo, la evidencia de esta actividad se puede demostrar claramente.

»Inicial (1): En esta etapa no existe madurez de ciberseguridad o es de naturaleza muy embrionaria. Puede haber discusiones iniciales sobre el desarrollo de capacidades en ciberseguridad, pero no se han tomado medidas concretas. Puede haber una ausencia de evidencia observable en esta etapa.

La estructura del modelo del CMM esta divido en las siguientes cuatro (4) secciones: dimensión, factor, aspecto e indicador (figura 2.2).

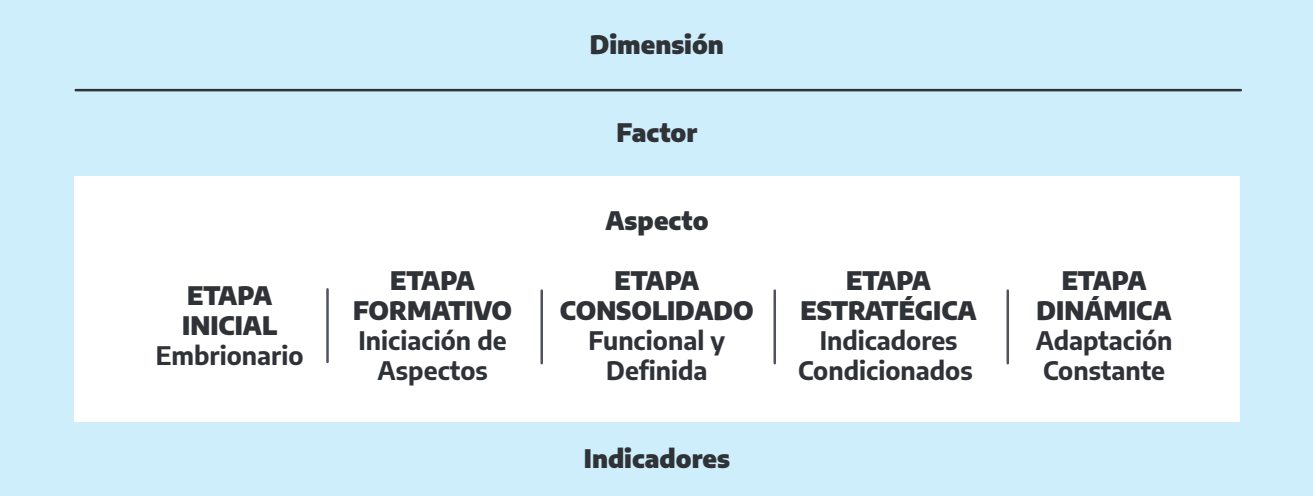
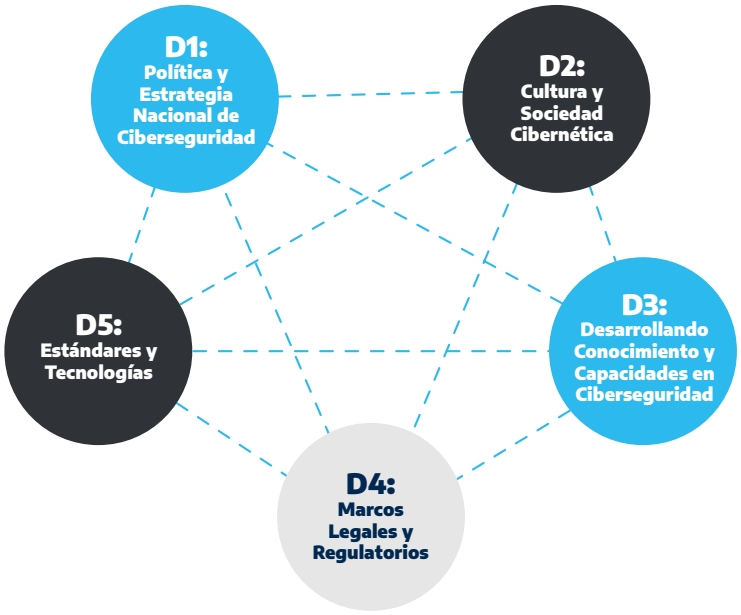


Figura 2.2: Estructura del modelo del CMM

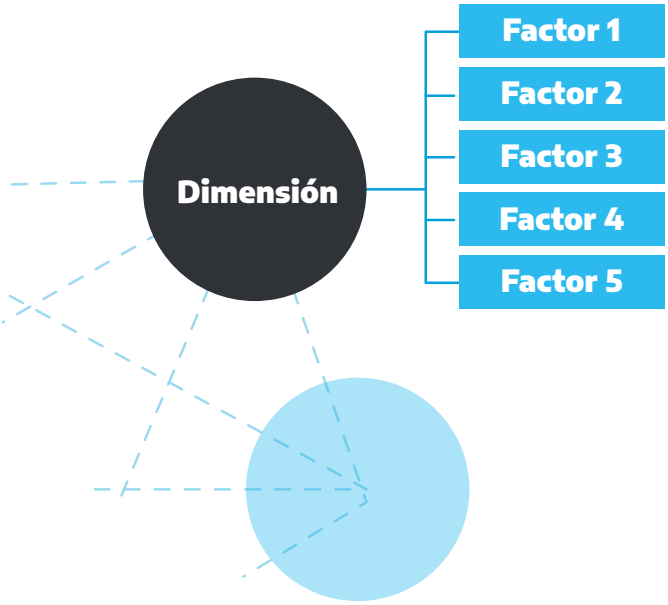
Dimensión:

Las cinco dimensiones en su conjunto cubren la amplitud de la capacidad nacional de ciberseguridad evaluada por el CMM. Cada dimensión está constituida por una gama de factores, que capturan las capacidades básicas requeridas para informar la dimensión, en conjunto representan las diferentes perspectivas a través de las cuales se puede evidenciar y analizar la capacidad de ciberseguridad. El CMM considera cinco dimensiones que en su conjunto constituyen la amplitud de la capacidad nacional que un país requiere para integrar la ciberseguridad a nivel nacional:



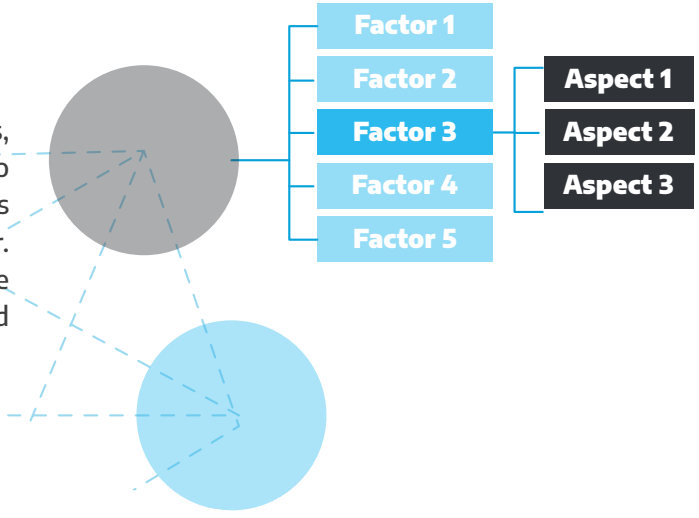
Factores:

Dentro de las cinco dimensiones, los factores describen lo que significa poseer capacidad de ciberseguridad. Estos son los elementos esenciales de la capacidad nacional, que luego se miden para la etapa de madurez. La lista completa de factores busca incorporar todas las necesidades de capacidad de ciberseguridad de una nación. La mayoría de los factores se componen de una serie de aspectos que estructuran los indicadores del factor en partes más concisas (que se relacionan directamente con la recopilación y medición de evidencia). Sin embargo, algunos factores que tienen un alcance más limitado no tienen aspectos específicos.



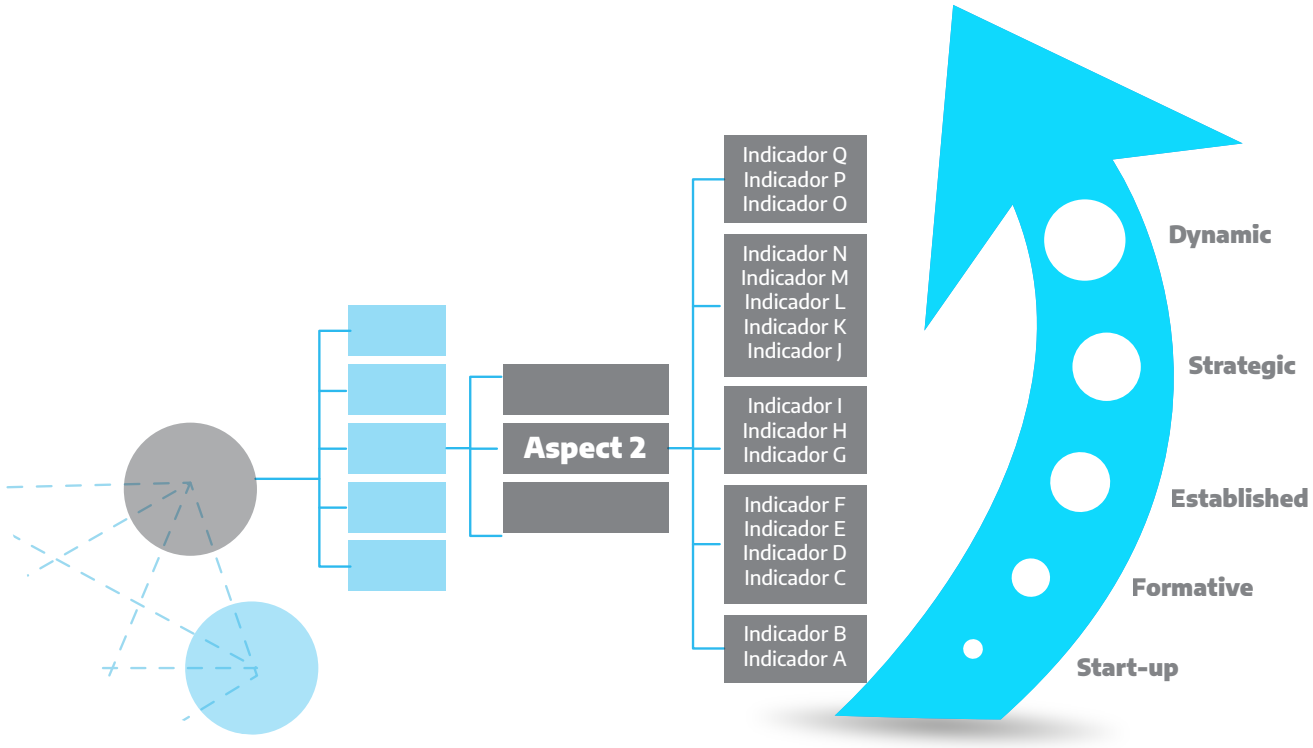
Aspecto:

Cuando un factor posee múltiples componentes, estos son aspectos. Los aspectos son un método organizativo para dividir los indicadores en grupos más pequeños que son más fáciles de comprender. El número de aspectos depende de los temas que surgen en el contenido del factor y la complejidad general de este.



Indicador:

Los indicadores representan la parte más básica de la estructura de CMM. Cada indicador describe los pasos, acciones o componentes básicos que son indicativos de una etapa específica de madurez. Para haber alcanzado con éxito una etapa de madurez, un país necesita evidenciar cada uno de los indicadores y para elevar la madurez de la capacidad de ciberseguridad de un país, se deberán haber cumplido todos los indicadores dentro de una etapa en particular.



2.1 Modelo CMM 2021

En esta sección se proporciona la descripción correspondiente para cada dimensión, factor y aspecto conforme al modelo de CMM edición 2021.

Dimensión 1:
Política y Estrategia Nacional de Ciberseguridad

Dimensión 2:
Cultura y Sociedad Cibernética

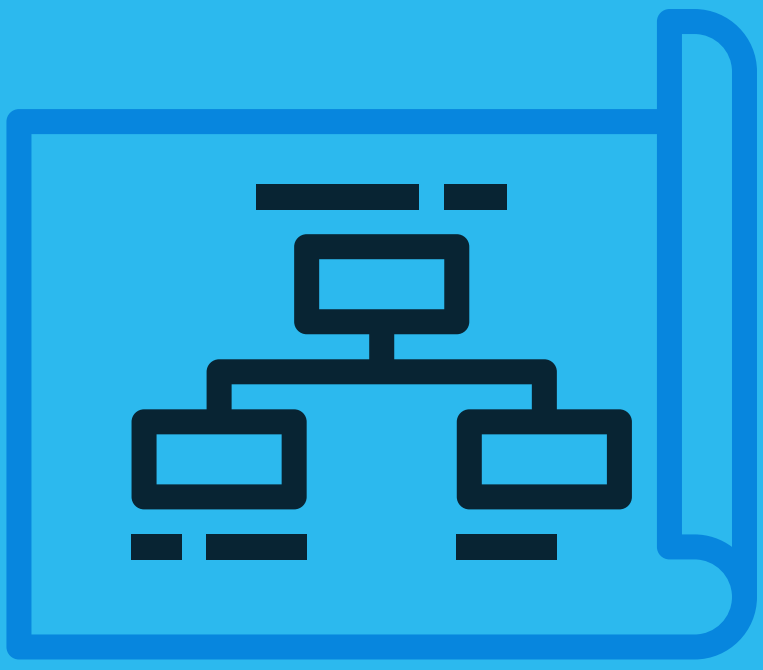
Dimensión 3:
Desarrollando Conocimiento y Capacidades en Ciberseguridad

Dimensión 4:
Marcos Jurídicos y Reglamentarios

Dimensión 5:
Estándares y Tecnologías

Dimensión 1:
Política y Estrategia Nacional de Ciberseguridad

La primera dimensión explora la capacidad del país para desarrollar y publicar una estrategia nacional de ciberseguridad, así como mejorar su resiliencia en ciberseguridad a través de la mejora de su respuesta a incidentes, ciberdefensa y capacidades de protección de infraestructura crítica. De igual manera, la presente dimensión considera la efectividad de la estrategia y política para brindar capacidad nacional de ciberseguridad, mientras se mantienen los beneficios de un ciberespacio vital para el gobierno, las empresas internacionales y la sociedad en general.



Factor D 1.1: Estrategia Nacional de Ciberseguridad

La estrategia de ciberseguridad es esencial para la transversalización de una agenda de ciberseguridad en todo el gobierno, dado que contribuye a priorizar la ciberseguridad como un área de política clave, determina responsabilidades y mandatos de actores gubernamentales claves en materia de ciberseguridad, y determina la asignación de recursos para problemas emergentes, existentes y prioridades en ciberseguridad.

Aspectos

• **Desarrollo de la Estrategia:** este aspecto aborda el desarrollo de una estrategia nacional, la asignación de autoridades de implementación entre los sectores y la sociedad civil, y una comprensión de los riesgos y amenazas de la ciberseguridad nacional que impulsan el desarrollo de capacidades a nivel nacional.

• **Contenido:** este aspecto aborda el contenido de la estrategia nacional de ciberseguridad y si está vinculada explícitamente a los riesgos, prioridades y objetivos nacionales tales como seguridad nacional, concientización pública y mitigación del ciberdelito, capacidad de respuesta a incidentes y protección de la infraestructura crítica a nivel nacional.

• **Implementación y Revisión:** este aspecto aborda la existencia de un programa integral para la coordinación de la ciberseguridad, incluyendo un propietario departamental o un organismo coordinador con un presupuesto consolidado.

• **Compromiso Internacional:** este aspecto explora el alcance de concientización del país sobre la existencia de discusiones y debates internacionales relacionadas con la política de ciberseguridad y temas relacionados que afectan los intereses del país y su postura internacional.

Factor D 1.2: Respuesta a Incidentes y Gestión de Crisis

Este factor aborda la capacidad del gobierno para identificar y determinar las características de los incidentes a nivel nacional de manera sistemática. Igualmente revisa la capacidad del gobierno para organizar, coordinar y operacionalizar la respuesta a incidentes, y si la ciberseguridad se ha integrado en el marco nacional de gestión de crisis.

Aspectos

• **Identificación y Categorización de Incidentes:** este aspecto identifica si existen mecanismos internos para identificar y categorizar incidentes.

• **Organización:** este aspecto aborda la existencia de un organismo central designado para recopilar información sobre incidentes y su relación con el sector público y privado para la respuesta a incidentes a nivel nacional.

• **Integración Cibernética en la Gestión Nacional de Crisis:** este aspecto explora el alcance en el que la ciberseguridad está integrada en el marco nacional de gestión de crisis.

Factor D 1.3: Protección de Infraestructura Crítica (IC)

Este factor estudia la capacidad del gobierno para identificar activos de IC, los requisitos regulatorios específicos de ciberseguridad de la IC y la implementación de buenas prácticas en materia de ciberseguridad por parte de los operadores de IC.

Aspectos

• Identificación: este aspecto aborda la existencia de una lista general de activos, sectores y operadores de IC, y una auditoría de los activos de IC de forma periódica;

• Requisitos regulatorios: este Aspecto aborda la existencia de requisitos regulatorios específicos para la ciberseguridad de la IC.

• Requisitos regulatorios: este aspecto aborda la existencia de requisitos regulatorios específicos para ciberseguridad de IC.

• Práctica operativa: este aspecto explora si los operadores IC implementan estándares reconocidos de la industria, y la existencia de acuerdos de colaboración entre sectores y dentro de los sectores.

Factor D 1.4: Ciberseguridad en defensa y seguridad nacional

Este factor explora si el gobierno tiene la capacidad de diseñar e implementar una estrategia de ciberseguridad dentro de la seguridad y defensa nacional. También revisa el nivel de capacidad de ciberseguridad dentro de la seguridad nacional y establecimiento de defensa, y los acuerdos de colaboración en ciberseguridad entre entidades civiles y de defensa.

Aspectos

•Estrategia de ciberseguridad de la fuerza de defensa: este aspecto aborda la existencia de una estrategia de apoyo hacia la ciberseguridad dentro de la seguridad nacional y la defensa, y si está respaldado por las autoridades legales apropiadas y doctrina operativa relevante y reglas de compromiso;

•Capacidad de ciberseguridad de la fuerza de defensa: este aspecto revisa el nivel de capacidad de ciberseguridad y estructuras organizativas dentro de la seguridad nacional establecida;

•Coordinación de la defensa civil: este aspecto examina la colaboración en ciberseguridad entre entidades civiles y de defensa, y la existencia de recursos adecuados establecidos.

Dimensión 2:
Cultura y Sociedad Cibernética

La segunda dimensión revisa elementos importantes sobre la adquisición de una cultura de ciberseguridad responsable, como la comprensión de los riesgos relacionados con la ciberseguridad en la sociedad, el nivel de confianza en los servicios de Internet, los servicios de gobierno electrónico y de comercio electrónico, y la comprensión de los usuarios sobre la protección de la información personal en línea. Esta dimensión explora la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios informen el ciberdelito. Adicionalmente, la revisión del rol de los medios de comunicación y las redes sociales en inducir valores, actitudes y comportamiento en ciberseguridad es contemplado dentro de dicha dimensión.

Factor 2.1: Mentalidad de ciberseguridad

Este factor evalúa el grado en que la ciberseguridad se prioriza e incorpora en los valores, actitudes y prácticas del gobierno, el sector privado y los usuarios en toda la sociedad. Una mentalidad de ciberseguridad consiste en valores, actitudes y prácticas, incluidos los hábitos de usuarios individuales, expertos y otros actores, en el ecosistema de ciberseguridad que aumentan la capacidad de los usuarios para protegerse asimismo en línea.

Aspectos

• **Conciencia de los riesgos:** este aspecto examina el nivel de conciencia de los riesgos de ciberseguridad dentro del gobierno, sector privado y usuarios;

• **Prioridad de seguridad:** este aspecto examina el grado de prioridad que el gobierno, el sector privado y los usuarios le dan a la ciberseguridad; y

• **Prácticas:** este aspecto examina si el gobierno, el sector privado y los usuarios siguen prácticas seguras de ciberseguridad.

Factor D 2.2: Confianza y seguridad en los servicios en línea

Este factor revisa las habilidades críticas, la administración de la desinformación, el nivel de confianza y seguridad de los usuarios en el uso de los servicios en línea en general y en particular, del gobierno electrónico y servicios de comercio electrónico.

Aspectos

• **Capacitación y habilidades digitales:** este aspecto examina si los usuarios de Internet evalúan críticamente lo que ven o reciben en línea;

• **Seguridad y Confianza del usuario en la búsqueda en línea e información:** este aspecto examina si los usuarios confían en el uso seguro de Internet basado en indicadores de la legitimidad del sitio web;

• **Desinformación:** este aspecto examina la existencia de herramientas y recursos para abordar la desinformación en línea;

• **Confianza del usuario en los servicios de gobierno electrónico:** este aspecto examina si se ofrecen servicios electrónicos gubernamentales, si existe confianza en la provisión segura de tales servicios, y si se realizan esfuerzos para promover dicha confianza en la aplicación de medidas de seguridad;

• **Confianza del usuario en los servicios de comercio electrónico:** este aspecto examina si los servicios de comercio electrónico se ofrecen y se establecen en un entorno seguro y de confianza para los usuarios.

Factor 2.3: Comprensión del usuario de la protección en línea de la información personal

Este factor analiza si los usuarios de Internet y las partes interesadas dentro del sector público y privado reconocen y comprenden la importancia de proteger información personal en línea, y si son conscientes de sus derechos de privacidad.

Aspectos

• **Protección de información personal en línea:** analiza si los usuarios de Internet y las partes interesadas dentro del sector público y privado reconocen y comprenden la importancia de proteger información personal en línea, y si son conscientes de sus derechos de privacidad.

Factor D 2.4: Mecanismos de notificación

Este factor explora la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios denuncien delitos relacionados con Internet tales como fraude en línea, acoso cibernético, abuso infantil en línea, robo de identidad, violaciones a la privacidad y la seguridad, y otros incidentes.

Aspectos

• **Mecanismos de notificación:** explora la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios denuncien delitos relacionados con Internet tales como fraude en línea, acoso cibernético, abuso infantil en línea, robo de identidad, violaciones a la privacidad y la seguridad, y otros incidentes.

Factor D 2.5: Plataformas en línea y medios de comunicación

Este factor explora si la ciberseguridad es un tema común de discusión en los principales medios de comunicación, y un tema para una amplia discusión en las redes sociales. Además, este factor analiza el papel de los medios de comunicación en la transmisión al público de información sobre ciberseguridad, dando forma a sus valores y actitudes de ciberseguridad y comportamiento en línea.

Aspectos:

• **Medios de comunicación y redes sociales:** explora si la ciberseguridad es un tema común de discusión en los principales medios de comunicación, y un tema para una amplia discusión en las redes sociales. Además, se analiza el papel de los medios de comunicación en la transmisión al público de información sobre ciberseguridad, dando forma a sus valores y actitudes de ciberseguridad y comportamiento en línea.

Dimensión 3:
Desarrollando Conocimiento y Capacidades en Ciberseguridad

La tercera dimensión revisa la disponibilidad, calidad y aceptación de programas para varios grupos de partes interesadas, incluido el gobierno, el sector privado y la población en general, y se relaciona con programas de concienciación sobre ciberseguridad, programas oficiales educativos en ciberseguridad, así como programas de formación profesional.

Factor 3.1: Desarrollo de Concientización en Ciberseguridad

Este factor se centra en la disponibilidad de programas que crean conciencia sobre la ciberseguridad en todo el país, concentrándose en los riesgos y amenazas de ciberseguridad y las formas para abordarlos.

Aspectos

• **Iniciativas gubernamentales de sensibilización:** este aspecto examina la existencia de un programa coordinado a nivel nacional de sensibilización en ciberseguridad impulsado por el gobierno, cubriendo una amplia gama de datos demográficos y cuestiones, desarrolladas en consulta con las partes interesadas de varios sectores;

• **Iniciativas de sensibilización del sector privado:** este aspecto examina la existencia de programas de sensibilización impulsados por el sector privado y la medida en que son alineados con iniciativas gubernamentales y de la sociedad civil;

• **Iniciativas de sensibilización de la sociedad civil:** este aspecto examina la existencia de programas de sensibilización impulsados por la sociedad civil y el grado en que son alineados con iniciativas gubernamentales y del sector privado; y

• **Sensibilización ejecutiva:** este aspecto examina los esfuerzos para sensibilizar a los ejecutivos sobre los problemas de ciberseguridad en los sectores público, privado, académico y de la sociedad civil, además de cómo se pueden abordar los riesgos de ciberseguridad.

Factor D 3.2: Educación en ciberseguridad

Este factor aborda la disponibilidad y provisión de programas de educación en ciberseguridad de alta calidad y suficientes profesores e instructores cualificados. Adicionalmente, este factor examina la necesidad de mejorar la educación en ciberseguridad a nivel nacional e institucional y la colaboración entre el gobierno y la industria para asegurar que las inversiones educativas satisfagan las necesidades del entorno educativo en ciberseguridad en todos los sectores.

Aspectos

• **Provisión:** este aspecto explora si existen ofertas de programas de alta calidad en ciberseguridad y suficientes profesores cualificados disponibles que brindan una comprensión de los riesgos actuales y los requisitos de las habilidades; y

• **Administración:** este aspecto explora la coordinación y recursos para desarrollar y mejorar los marcos educativos en ciberseguridad con presupuesto y gastos asignados basados en la demanda nacional.

Factor D 3.3: Formación profesional en ciberseguridad

Este factor aborda y revisa la disponibilidad y provisión de programas asequibles de formación profesional en ciberseguridad para construir un organismo de profesionales de ciberseguridad. Además, este factor revisa la adopción de la formación horizontal y vertical del conocimiento en ciberseguridad y la transferencia de habilidades dentro de las organizaciones, y cómo esta transferencia de habilidades se traduce en un aumento continuo de organismos de profesionales de ciberseguridad.

Aspectos

• **Provisión:** este aspecto examina el desarrollo, disponibilidad y provisión de programas de capacitación en ciberseguridad para mejorar habilidades y capacidades;

• **Admisión:** este aspecto examina la aceptación y la disponibilidad de tales programas para producir un organismo de profesionales certificados en ciberseguridad. Los problemas investigados incluyen iniciativas para registrarse en dichos programas, iniciativas para permanecer en el país después de completar con éxito, compartir conocimientos después de completar un programa, y la existencia de un registro nacional de estudiantes exitosos y certificados.

Factor D 3.4: Investigación e innovación en ciberseguridad

Este factor aborda el énfasis puesto en la investigación sobre ciberseguridad e innovación para abordar los retos tecnológicos, sociales y empresariales y avanzar en la construcción de conocimientos y capacidades de ciberseguridad en el país.

Aspectos

• **Investigación y desarrollo en ciberseguridad:** este aspecto investiga la existencia de una cultura de investigación e innovación en el país, relacionado con proyectos nacionales actuales y terminados, apoyo financiero, incentivos y resultados de investigación utilizables.

Dimensión 4:
Marcos Legales y Regulatorios

Esta dimensión examina la capacidad del gobierno para diseñar y promulgar legislación nacional que se relacione directa e indirectamente con la ciberseguridad, con un énfasis particular en los temas de los requisitos regulatorios para la ciberseguridad, la legislación relacionada con el delito cibernético y la legislación relacionada. La capacidad para hacer cumplir tales leyes se examina a través de la aplicación de la ley, el enjuiciamiento, los órganos reguladores y los tribunales. Además, esta dimensión observa cuestiones como los marcos de cooperación formales e informales para combatir el ciberdelito.

Factor D 4.1: Disposiciones legales y regulatorias

Este factor aborda diversas leyes y provisiones de regulación relativas a la ciberseguridad, incluidos los requisitos legales y regulatorios, legislación sustantiva y procesal sobre ciberdelincuencia e impacto y evaluación sobre los derechos humanos.

Aspectos

• **Legislación sustantiva sobre ciberdelincuencia:** este aspecto explora si la legislación existente penaliza una variedad de delitos cibernéticos en legislación específica o derecho penal general;

• **Requisitos legales y regulatorios para la ciberseguridad:** este aspecto revisa la existencia de marcos legales y regulatorios en ciberseguridad;

• **Legislación procesal sobre ciberdelincuencia:** este aspecto examina si es implementado el derecho procesal penal integral con poderes procesales para la investigación del delito cibernético y requisitos probatorios para disuadir, responder y enjuiciar el ciberdelito y los delitos que involucran evidencia electrónica, y

• **Evaluación de impacto en derechos humanos:** este aspecto examina si se llevan a cabo las evaluaciones de impacto sobre si la legislación procesal sobre ciberdelincuencia y las regulaciones de ciberseguridad cumplen con los estándares internacionales de protección de derechos humanos y otros derechos fundamentales.

Factor D 4.2: Marcos legislativos relacionados

Este factor aborda los marcos legislativos relacionados con ciberseguridad, incluida la protección de datos, protección infantil, protección del consumidor y propiedad intelectual.

Aspectos

• **Legislación de protección de datos:** este aspecto examina la existencia e implementación de un marco legal para asegurar la protección de datos;

• **Protección infantil en línea:** este aspecto se centra en el marco legal para asegurar la protección de niños y niñas en línea, incluida la protección de sus derechos en línea y la criminalización de abuso infantil en línea;

• **Legislación de Protección al Consumidor:** este aspecto aborda la existencia y aplicación de la legislación que protege consumidores en línea del fraude y otras formas de negligencia empresarial;

• **Legislación de Propiedad Intelectual:** este aspecto está relacionado con la existencia e implementación de la legislación de propiedad intelectual en línea.

Factor D 4.3. Capacidad y habilidad legal y regulatoria

Este factor estudia la capacidad de aplicar la ley para investigar el delito cibernético, la capacidad de la fiscalía para presentar casos de ciberdelincuencia y pruebas electrónicas, y capacidad del tribunal para presidir casos de ciberdelincuencia y que involucre evidencia electrónica. Finalmente, este factor revisa la existencia de organismos reguladores intersectoriales para supervisar el cumplimiento de normativas específicas de ciberseguridad.

Aspectos

• **Aplicación de la ley:** este aspecto examina si los agentes y organismos encargados de hacer cumplir la ley han recibido la formación en la investigación y gestión de casos de ciberdelincuencia, y casos de delitos informáticos que involucran evidencia electrónica, y si hay suficientes recursos humanos, procedimentales y tecnológicos;

• **Enjuiciamiento:** este aspecto examina si los fiscales han recibido formación sobre el manejo de casos de ciberdelincuencia y casos que involucran evidencia electrónica, y si hay suficientes recursos humanos, procedimentales y tecnológicos;

• **Tribunales:** este aspecto examina si los tribunales tienen suficientes recursos y formación para garantizar un enjuiciamiento efectivo y eficiente de casos de ciberdelincuencia y casos que involucren evidencia electrónica;

• **Órganos reguladores:** este aspecto revisa la existencia de organismos reguladores intersectoriales para supervisar el cumplimiento de normativas específicas de ciberseguridad.

Factor D 4.4: Marcos de Cooperación formal e informal para combatir la ciberdelincuencia

Este factor aborda la existencia y función de los mecanismos formales e informales que permitan la cooperación entre actores nacionales y transfronterizos para disuadir y combatir ciberdelito.

Aspectos

• **Cooperación de la aplicación de la ley con el sector privado:** este aspecto examina el mecanismo de intercambio de información sobre la ciberdelincuencia entre los sectores público y privado nacional, incluida la cooperación con el servicio de Internet y otros proveedores de tecnología;

• **Cooperación con homólogos extranjeros encargados de hacer cumplir la ley:** este aspecto examina la existencia de mecanismos formales de cooperación internacional en materia de aplicación de la ley;

• **Colaboración entre el gobierno y el sector de la justicia penal:** este aspecto revisa los canales formales de comunicación entre el gobierno y los actores de la justicia penal.

Dimensión 5:
Estándares y Tecnologías

Esta dimensión aborda el uso de tecnología en ciberseguridad de forma eficaz y difusiva para proteger individuos, organizaciones e infraestructura nacional. La dimensión examina específicamente la implementación de estándares y buenas prácticas en materia de ciberseguridad, la ejecución de procesos y controles, además del desarrollo de tecnologías y productos para reducir los riesgos asociados a la ciberseguridad.

Factor D 5.1: Cumplimiento de los estándares

Este factor revisa la capacidad del gobierno para promover, evaluar, implementar y monitorear el cumplimiento de estándares y buenas prácticas internacionales de ciberseguridad.

Aspectos

• **Estándares de seguridad ICT:** este aspecto examina si los estándares y buenas prácticas internacionales relacionadas con la ciberseguridad se adoptan e implementan ampliamente en todo el sector público y organizaciones de infraestructura critica;

• **Estándares en Adquisiciones:** este aspecto aborda la implementación de estándares y buenas prácticas en todos los sectores para orientar los procesos de adquisiciones, incluido el riesgo de gestión, gestión del ciclo de vida, aseguramiento de software y hardware, subcontratación y uso de servicios en la nube;

• **Estándares para la provisión de productos y servicios:** este aspecto aborda el uso de estándares y buenas prácticas por proveedores locales de bienes y servicios, incluyendo software, hardware, servicios gestionados y servicios en la nube.

Factor D 5.2: Controles de seguridad

Este factor revisa la evidencia con respecto al despliegue de controles de seguridad por parte de usuarios y sectores público y privado, y si el conjunto de control de ciberseguridad tecnológica es basado en marcos de ciberseguridad establecidos.

Aspectos

• **Controles de seguridad tecnológica:** este aspecto explora en qué medida los controles de seguridad tecnológicos actualizados, incluidos parches y copias de seguridad, se implementan en todos los sectores.

• **Controles criptográficos:** este aspecto revisa el despliegue de técnicas criptográficas en todos los sectores y usuarios para protección de datos en reposo o en tránsito, y el grado en que estos controles criptográficos cumplen con normas y directrices internacionales y se mantienen actualizadas.

Factor D 5.3: Calidad del software

Este factor examina la calidad de la implementación de software y los requisitos funcionales en los sectores público y privado. Además, este factor revisa la existencia y mejora de políticas y procesos para actualizaciones de software y mantenimiento basado en evaluaciones de riesgo y la naturaleza crítica de los servicios.

Aspectos

• **Calidad y garantía del software:** examina la calidad de la implementación de software y los requisitos funcionales en los sectores público y privado. Además, se revisa la existencia y mejora de políticas y procesos para actualizaciones de software y mantenimiento basado en evaluaciones de riesgo y la naturaleza crítica de los servicios.

Factor D 5.4: Comunicaciones e Internet

Resiliencia de la infraestructura

Este factor aborda la existencia de infraestructura y servicios de Internet confiables en el país, así como procesos de seguridad rigurosos en los sectores público y privado. Además, este factor revisa el control que el gobierno podría tener sobre su infraestructura de Internet y la medida en que se subcontratan las redes y los sistemas.

Aspectos

• **Confiabilidad de la Infraestructura de Internet:** este Aspecto examina la confiabilidad y protección de los servicios e infraestructura de Internet en los sectores público y privado; y

• **Monitoreo y respuesta:** este aspecto examina si existen mecanismos para realizar evaluaciones de riesgo y monitorear la resiliencia de la red en los sectores público y privado.

Factor D 5.5: Mercado de ciberseguridad

Este factor aborda la disponibilidad y el desarrollo de tecnologías de ciberseguridad competitivas, productos de ciberseguros, servicios y experiencia en ciberseguridad, y las implicaciones de seguridad de la subcontratación.

Aspectos

• **Tecnologías de ciberseguridad:** este aspecto examina si existe un mercado nacional para tecnologías de ciberseguridad y si está respaldado e informado por la demanda nacional;

• **Servicios y experiencia en ciberseguridad:** este aspecto explora la disponibilidad de servicios de consultoría en ciberseguridad para organizaciones públicas y privadas;

• **Implicaciones de seguridad de la subcontratación:** este aspecto examina si se realizan evaluaciones de riesgo para determinar cómo mitigar los riesgos de subcontratar TI a un tercero o servicios en la nube; y

• **Seguros de ciberseguridad:** este aspecto explora la existencia de un mercado de seguros cibernéticos, su cobertura y productos adecuados para diversas organizaciones.

Factor D 5.6: Divulgación responsable

Este factor explora el establecimiento de un marco de divulgación responsable para la recepción y difusión de información de vulnerabilidad en todos los sectores, y si existe la capacidad suficiente para revisar y actualizar continuamente este marco.

Aspectos

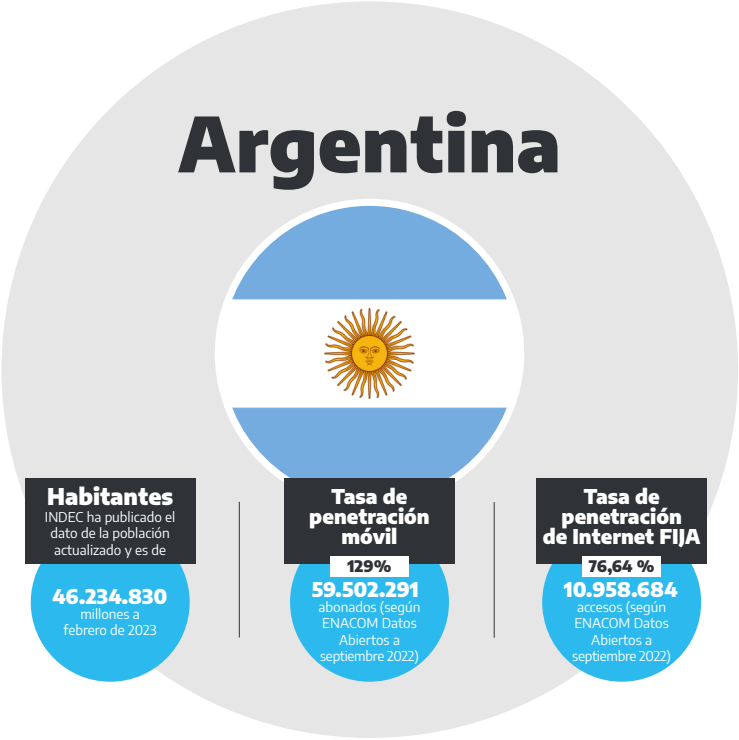
•**Compartir información sobre vulnerabilidades:** este aspecto explora los mecanismos o canales existentes para compartir información sobre los detalles técnicos de las vulnerabilidades entre las partes interesadas; y

• **Políticas, Procesos y Legislación para la divulgación responsable de fallas de seguridad:** este aspecto explora la existencia de una política o marco de divulgación responsable en organizaciones del sector público y privado y el derecho a la protección legal para quienes divulgan fallas de seguridad.

III. Perfil del País – Diagnóstico Nacional

3.1 Evolución Digital en Argentina – Indicadores Internacionales

El detrimento económico causado por la pandemia de COVID-19 tuvo impactos negativos en la economía global. La región de América Latina y el Caribe se ha visto particularmente perjudicada al ser la más afectada económicamente entre las seis regiones de economías emergentes en el mundo.[4] Sin embargo, la crisis sanitaria, actuó como catalizador de la transformación digital de la región, y también se hizo evidente que la economía digital será elemento clave en la recuperación post pandemia. Las Tecnologías de la Información y la Comunicación (TIC) son la fuerza impulsora detrás de la evolución de la economía digital y la ciberseguridad es fundamental para sostener un modelo tecnológico robusto e innovador. En este sentido, como también lo confirma el informe "Perspectivas Económicas de América Latina", la transformación digital puede contribuir a la recuperación económica de América Latina y el Caribe y transformar la economía de la región.[5]



Argentina es una de las economías más grandes de América Latina, con un Producto Interno Bruto (PIB) de aproximadamente 632.298 millones de dólares. A raíz de los impactos por la pandemia de COVID-19, la actividad económica nacional se ha recuperado considerablemente rápido, con un incremento del 10.4% del PIB en 2021, luego de una caída de 9.9% en 2020 en el marco de la pandemia.[6] La estimación preliminar del PIB total para el 2022, muestra un crecimiento anual de 5.2%. Respecto a la variación interanual del cuarto trimestre, el crecimiento fue del 1,9%.[7]

4. https://news.un.org/es/story/2021/03/1489112
5. https://www.cepal.org/es/comunicados/america-latina-caribe-la-transformacion-digital-es-clave-acelerar-la-recuperacion
6. https://www.indec.gob.ar/uploads/informesdeprensa/pib_03_239490F448D8.pdf
7. https://www.indec.gob.ar/indec/web/Nivel4-Tema-3-9-47

En el ámbito de la economía digital, el Índice de Inteligencia Digital 2020 que evalúa el progreso de 90 países en materia de evolución y confianza digital, otorgó a Argentina el puesto 57 en el eje sobre estado actual y en el eje referente al impulso económico el puesto 36.[8] Dicho índice refleja que Argentina, en conjunto con Costa Rica, ha logrado avances significativos en su evolución digital, particularmente en el entorno institucional, uniéndose a Uruguay y Chile con desempeños históricos de la región.

Igualmente, el Índice de Inteligencia Digital 2020, dentro del marco de la evolución digital, clasifica a las economías de los países en cuatro zonas: destacadas, estancadas, emergentes y vigilantes.[9] La economía de Argentina se considera en la categoría de emergentes, indicando que los países en esta zona tienen una infraestructura digital limitada, sin embargo, su proceso de digitalización avanza rápidamente. El estudio señala que las economías emergentes exhiben algunas de las actitudes más optimistas hacia la digitalización y la tecnología, no obstante, frecuentemente se ven obstaculizadas por una infraestructura relativamente débil y una calidad institucional deficiente. Por consiguiente, Argentina, junto con otros países categorizados dentro de las economías emergentes, se beneficiaría en fomentar mejores instituciones que puedan contribuir a nutrir y sostener la innovación e inversión en la digitalización.

El informe *Digital in the time of COVID* indica que varias naciones medianas, incluidas Kenia, Vietnam, Bangladesh, Ruanda y Argentina, han estado utilizando tecnologías digitales para dar un salto y transformar sus economías. Estos avances constituyen modelos a seguir y puntos de referencia ideales para otras economías sobre cómo utilizar la economía digital como palanca para crear un cambio radical en su trayectoria de crecimiento.

Las economías de la región de América Latina y el Caribe (ALC) siguen avanzando en la reducción de las desigualdades digitales y en el fomento de una adopción tecnológica más amplia. Costa Rica y Argentina han dado pasos excepcionales hacia la mejora de su entorno institucional, uniéndose a las filas de los países con mejor desempeño histórico de la región en relación a las Instituciones[10].

El estudio de evaluación destaca que la inversión en la capacidad nacional de la ciberseguridad, incluyendo las habilidades necesarias de higiene digital y alfabetización para combatir la desinformación y las amenazas cibernéticas, es una medida determinante en la mejora de las economías digitales emergentes. Las asociaciones público-privadas centradas en soluciones de ciberseguridad, tanto del lado de la oferta como del lado de la demanda, pueden fortalecer la confianza y la resiliencia del ecosistema digital.

Argentina ha mostrado un impulso creciente en materia de digitalización, sugiriendo potencial de avanzar rápidamente, tanto para la recuperación económica posterior al COVID-19, como para la transformación digital a largo plazo. En este contexto, la ciberseguridad es un elemento clave para salvaguardar los beneficios y oportunidades que ofrece la digitalización.

8. https://sites.tufts.edu/digitalplanet/files/2021/countrydashboards/Digital_Intelligence_Dashboard_AR.pdf
9. https://sites.tufts.edu/digitalplanet/files/2021/03/digital-intelligence-index.pdf
10. https://sites.tufts.edu/digitalplanet/files/2021/03/digital-intelligence-index.pdf

Tabla 3.1: Panorama nacional: Indicadores clave de la economía digital en Argentina

<table>
<tr><th>Referencia</th><th>Evaluación más reciente</th><th>Relevancia</th></tr>
<tr><td>Población (2022)</td><td>Argentina tiene una población estimada de 46.234.830 habitantes (febrero 2023)
Es considerado un país con ingresos medios altos según la clasificación del Banco Mundial. Actualmente, el Producto Interno Bruto es de 632.298 millones de dolares.[11]</td><td>En términos de población el país es comparable con España o Corea del Sur, países más avanzados con respecto a la economía digital[12]
<table><tr><th>País</th><th>Población</th><th>Índice de Crecimiento</th><th>Densidad/ km2</th></tr><tr><td>Argentina</td><td>46.234.830</td><td>0.89%%</td><td>17/km2</td></tr></table></td></tr>
<tr><td>Suscripciones a telefonía móvil (2022)</td><td>129 por cada 100 habitantes.</td><td>59.713.503 accesos al servicio de telefonía móvil (septiembre 2022)</td></tr>
<tr><td>Penetración de Internet (2022)</td><td>76,64% es la Penetración por hogares nacional de Internet fijo.</td><td>Indicador positivo para el crecimiento de la comunidad de usuarios de Internet y el desarrollo de los servicios digitales. En el tercer trimestre de 2022 se registraron, en promedio, 7.915.077 accesos a internet fijos. Esto significó un aumento de 1,5% respecto al tercer trimestre de 2021. Por otro lado, los accesos fijos residenciales crecieron 1,9%, lo que suma un total de 7.516.997; y los accesos fijos de organizaciones totalizaron 398.080, con una caída de 4,7%.</td></tr>
<tr><td>Hogares con acceso a computadoras (2022)</td><td>64,2% de hogares urbanos.</td><td>La brecha de hogares sin acceso a computadores es de un poco más de 32%.</td></tr>
<tr><td>Clasificación en el Índice de preparación para la red (IPR) 2022</td><td>Ocupa el puesto 57 entre 130 países participantes en el estudio. Argentina ocupa el quinto puesto en Latinoamérica, precedido por Chile, Uruguay, Brasil, Costa Rica y superando a países como México y Colombia.</td><td>El índice IPR es holístico y combina indicadores de desarrollo en aspectos de tecnología, capital humano, gobernanza e impacto. Argentina logra su mejor posición dentro de la clasificación del pilar de recurso humano, con una posición de 50 de 134.[13]
En términos de aspectos para mejorar se destaca la inversión en ciberseguridad, nuevas tecnologías, calidad regulatoria, entorno regulatorio de las TIC y desigualdad en ingresos.
Algunos aspectos sobresalientes incluyen la legislación de comercio electrónico, exportación de servicios TIC, matrícula en educación universitaria, porcentaje de alfabetización de personas adultas y uso de redes sociales digitales.</td></tr>
</table>

11. https://datos.bancomundial.org/pais/argentina
12. Fuente: Total Population by Country 2022 (worldpopulationreview.com)
13. Índice de preparación para la red (IPR): https://networkreadinessindex.org/nri-2022-edition-press-release/

Tabla 3.1: Panorama nacional: Indicadores clave de la economía digital en Argentina

Referencia	Evaluación más reciente	Relevancia
Encuesta de las Naciones Unidas sobre la administración electrónica en 2020	Ocupa el puesto 41 de 193 países participantes, desempeñando el segundo lugar en Latinoamérica, precedido por Uruguay, y le siguen Chile, Brasil, Costa Rica, México, Colombia, Perú, Ecuador, entre otros.	Mide la eficacia de la administración electrónica en la prestación de servicios públicos e identifica los patrones de desarrollo y rendimiento de la administración electrónica, así como las áreas en las que el potencial de las TIC y la administración electrónica aún no se ha aprovechado plenamente y en las que podría ser útil el apoyo al desarrollo de capacidades. Considerando que el tema de Gobierno Digital es parte de la Agenda Digital 2030 y, se anticipa que en los próximos años Argentina podría tener un crecimiento y avance importantes en el proceso de digitalización del sector público, la necesidad de priorizar la ciberseguridad a nivel gubernamental y nacional es vital.
Índice de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD por sus siglas en ingles) (2020)	Ocupa el puesto 82 de 152 países participantes, ejerciendo el octavo lugar en Latinoamérica, precedido por Costa Rica, Chile, Brasil, República Dominicana, Colombia, Uruguay y Perú.	Mide el nivel de preparación de una economía para admitir las compras en línea. El posicionamiento de octavo lugar en la región indica un nivel de avance relativamente importante en este sector.
Índice de innovación global (2022)	Ocupa el puesto 69 de 132 países participantes, al tener el octavo puesto en Latinoamérica, precedido por Chile, México, Costa Rica, Brasil, Uruguay, Colombia y Perú.	Presenta las tendencias mundiales y resultados de innovación de 132 economías. Argentina desempeña positivamente en temas relacionados con recurso humano y la infraestructura TIC, sin embargo, se considera que existe oportunidad de mejora en aspectos de innovación en las instituciones públicas, lo cual incluye el marco regulatorio, así como el nivel de sofisticación del mercado nacional.

3.2 Panorama nacional – Indicadores internacionales en ciberseguridad

Como consecuencia de la transformación digital, el sector de la ciberseguridad ha ganado cada vez más visibilidad por su potencial económico, social y de seguridad en la nueva economía digital. Según ReportLinker, se estima que la industria de la ciberseguridad duplicará su valor de mercado, alcanzando una tasa de crecimiento anual compuesto (TCAC) del 14,5% durante el período 2021-2026, y el valor de mercado de ciberseguridad en América Latina se estima que tendrá un crecimiento del 10,8% durante este período de tiempo.[14] Además, la inversión tecnológica en una economía en recuperación tiene el potencial de crear nuevas oportunidades laborales. Según el Foro Económico Mundial, se estima que la escasez de profesionales de ciberseguridad es de más de 3 millones a nivel global y de más de medio millón en América Latina y el Caribe.[15] La alta tasa de desempleo en América Latina y el Caribe es de aproximadamente 28,8 millones en 2022, así como la alta población joven de aproximadamente el 20% de la población total, demuestra el potencial que tiene el sector de la ciberseguridad para contribuir a cerrar la brecha de la fuerza laboral en la región.[16]

Asimismo, la falta de ciberseguridad pone en riesgo las oportunidades que ofrece la economía digital, particularmente para los países en desarrollo que necesitan alcanzar un crecimiento sostenible y un entorno que permita fomentar la confianza. Según una encuesta del Foro Económico Mundial a organizaciones y sectores involucrados en la economía digital de 20 países, la economía digital se ha visto particularmente afectada por las crecientes tasas de ciberdelincuencia, destacando que cada organización expuso alrededor de 270 ataques cibernéticos en 2021. Si bien el costo económico exacto de los ataques cibernéticos es difícil de evaluar, dada la cantidad de costos directos e indirectos, se estima que en 2020 los ataques cibernéticos representaron una pérdida de 4% del PIB mundial. En América Latina y el Caribe, en promedio, la región pierde entre $15 y $30 mil millones de dólares cada año por causa de delitos cibernéticos, lo que representa alrededor del 0,5 % de su PIB. La seguridad nacional, la estabilidad económica y social dependen de un marco de ciberseguridad competente, así como de legislación y cooperación entre sectores para proteger los activos nacionales de los efectos devastadores de los ataques cibernéticos.

14. https://www.reportlinker.com/p06062816/Cybersecurity-Market-Growth-Trends-COVID-19-Impact-and-Forecasts.html?utm_source=GNW
15. https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/
16. https://news.un.org/es/story/2022/01/1502672

Tabla 3.2: Posicionamiento de Argentina a nivel regional: Índices internacionales en ciberseguridad

Referencia	Evaluación más reciente	Relevancia
Unión Internacional de Telecomunicaciones (UIT) Índice mundial de ciberseguridad) 2020	Ocupa el puesto 91 de 182 países que participaron en el estudio y ocupa el puesto 13 en América Latina.	Mide el compromiso de los países con la ciberseguridad a nivel mundial, para crear conciencia sobre la importancia de la materia y sus diferentes dimensiones. Este índice ayuda a establecer expectativas sobre la apertura del gobierno del país para promover la ciberseguridad y expone la necesidad de generar mayor impulso a la ciberseguridad nacional.
Reporte Ciberseguridad de la OEA y el Banco Interamericano de Desarrollo (2020)	Con un índice promedio de 2.21, de un máximo de 5, equivalente a un estado de madurez formativo de acuerdo con la estructura del modelo del CMM.	El modelo del CMM mide el nivel de madurez de la ciberseguridad del país en cinco dimensiones. Este estudio indica que Argentina en el 2016 tenía niveles de madurez muy bajos y en 4 años (2020) ha avanzado en algunos factores, pero todavía sin lograr un nivel óptimo de un estado establecido. Es importante destacar que Argentina entre los años 2016 y 2020 logró un avance importante en la Dimensión 4 – Marcos Legales y Regulatorios, convirtiéndose en un referente regional en esta dimensión.
Índice nacional de ciberseguridad de Estonia (2021)	Dentro de un puntaje de 100, Argentina obtiene un puntaje de 48.05, ocupando el puesto 71 de 160 países estudiados. A nivel regional, el país se establece en el sexto puesto, precedido por Paraguay, Chile, República Dominicana, Costa Rica y Panamá y superando a países como Uruguay, Colombia, Brasil y Perú.	Mide la preparación de los países para prevenir amenazas cibernéticas y gestionar incidentes cibernéticos. Pese a que el estudio indica que Argentina ha atendido algunos factores de ciberseguridad mejor que otros países de la región, hay temas como la protección a infraestructuras esenciales que reporta una calificación de cero.
Índice de Riesgo Cibernético (2020)	Argentina tiene un índice de riesgo cibernético del 0.601, lo que lo constituye en un país de riesgo alto, al igual que Chile (0.621). En comparación con Brasil (0.519) y México (0.450) que son considerados países de riesgo moderado.	El índice de riesgo cibernético contempla a 50 países y evalúa en una escala de 0 a 1 el riesgo del país de ser afectado por el cibercrimen, entre más alta la calificación más alta es la posibilidad de que los ciudadanos sufran un incidente cibernético.

En los últimos cinco años, Argentina ha dado pasos sustanciales para mejorar su capacidad de ciberseguridad, incluyendo legislación y políticas relacionadas con las TIC, como la Estrategia Nacional de Ciberseguridad y la Agenda Digital 2030, que han permitido avances en la materia. Esta apreciación se avala por distintos índices de ciberseguridad en los cuales el país generalmente se ubica por encima de sus contrapartes regionales en términos de ciberseguridad y capacidad de TIC. Por ejemplo, de acuerdo con Varieties of Democracy, los índices de capacidades de ciberseguridad de Argentina están por encima de las tasas promedio a nivel regional y global (1,05 en capacidades en ciberseguridad, versus 0.2 a nivel regional y 0.09 a nivel global. El desarrollo de políticas y marcos de ciberseguridad robustos fomentan un entorno digital más seguro y confiable, lo cual representa una oportunidad para la prosperidad de un país.

IV. Contexto legislativo, marco legal y regulatorio

El impacto de la pandemia es una oportunidad para acelerar la agenda digital, y con ello la ciberseguridad como eje principal para garantizar la optimización de oportunidades económicas y sociales. La digitalización ha aumentado exponencialmente en Argentina y, en respuesta, el gobierno ha priorizado distintas iniciativas y legislaciones en la materia de ciberseguridad y dentro del marco de las TIC. La siguiente sinopsis resume algunas de legislaciones en materia de ciberseguridad desde 2017 hasta 2022:

LEYES

»Ley 25.506 de Firma Digital.

»Ley 25.520 (t.o. Ley 27.126) – Ley de Inteligencia Nacional.

»Ley 26.388 de Delitos Informáticos, que incorpora modificaciones al Código Penal, sancionada en 2008.

»Ley 27411, Argentina aprobó el Convenio de Budapest como parte de su legislación. El mismo fue ratificado en 2018 y entró en vigor ese mismo año, con reservas.

»Ley 27.436 – Material ASI – Modificación art. 128 Código Penal.

»Ley 26.904 de Grooming – Modificación art. 131 Código Penal.

»Ley 27.590 – Creación del Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes.

DECRETOS

»Decreto No. 577 del 2017 y modificatorios - creación del Comité de Ciberseguridad con la misión de elaborar Estrategia Nacional de Ciberseguridad (ENC).
»Decreto 996/2018 aprobó la Agenda Digital 2030.

»Decreto 50/2019 (Texto actualizado) Se le asignó a la Secretaría de Innovación Pública de Jefatura de Gabinete de Ministros, la responsabilidad primaria en materia de ciberseguridad y protección de infraestructuras críticas de información y comunicaciones asociadas del Sector Público Nacional y de los servicios de información y comunicaciones.

A través de este decreto, también se creó la Subsecretaría de Tecnologías de Información, cuya función es proponer a la Secretaría de Innovación Pública estrategias, estándares y regulaciones para la ciberseguridad y protección de infraestructuras críticas de la información.

DECISIONES ADMINISTRATIVAS

»Decisión Administrativa No. 1865 del 2020 se creó y aprobó, entre otros temas, la determinación de las competencias de la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública, dependencia de la Jefatura de Gabinete de Ministros.

»Decisión Administrativa No 641 del 2021 establece los requisitos mínimos de seguridad para los organismos que componen la Administración Nacional y la obligatoriedad de reportar los incidentes de seguridad.

RESOLUCIONES

»Resolución 1291/2019 del Ministerio de Justicia y Derechos Humanos - creó la Unidad 24/7 de Delitos Informáticos y Evidencia Digital, la cual engloba economías digitales emergentes. Las asociaciones público-privadas centradas en soluciones de ciberseguridad, tanto del lado de la oferta como del lado de la demanda, pueden fortalecer la confianza y la resiliencia del ecosistema digital.

»Resolución 829/2019 de la entonces Secretaría de Gobierno de Modernización - aprobó la primera Estrategia Nacional de Ciberseguridad y creó la Unidad Ejecutiva del Comité de Ciberseguridad cuyas funciones fueron detalladas en el Anexo II.

»Resolución 1523/2019 de la ex Secretaría de Gobierno de Modernización estableció la definición y los criterios de identificación de las Infraestructuras Críticas e Infraestructuras Críticas de Información. Dicha resolución indica una lista de sectores críticos identificados: energía, tecnologías de información y comunicaciones, transportes, hídrico, salud, alimentación, finanzas, nuclear, químico, espacio y estado.

»Resolución 86/2022 del Ministerio de Seguridad - creó el Programa de Fortalecimiento en Ciberseguridad y en Investigación del Cibercrimen.

»Resolución 75/2022 del Ministerio de Seguridad - estableció el "Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos.

»Resolución 119/2022 de la Agencia de Acceso a la Información Pública - consulta pública sobre la propuesta de actualización de la Ley 25.326 de Protección de Datos Personales.

»Resolución 28/2022 - Política de Seguridad de la Información de la Secretaría Legal y Técnica de la Presidencia de la Nación.

DISPOSICIONES

»Disposición 1 / 2021 de la Dirección Nacional de Ciberseguridad creó el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.Ar).

»Disposición 07/2021 de la Dirección Nacional de Ciberseguridad - creó el registro de Puntos Focales de Ciberseguridad del Sector Público Nacional, en el marco de la DA 641/2021, los cuales deben reportar a la Dirección Nacional de Ciberseguridad los incidentes cibernéticos.

»Disposición 08/2021 de la Dirección Nacional de Ciberseguridad - aprobó la "Guía introductoria a la Seguridad para el Desarrollo de Aplicaciones WEB".

»Disposición N° 1/2022 de la Dirección Nacional de Ciberseguridad - aprobó un Modelo Referencial de Política de Seguridad de la Información, con el objetivo de orientar a los organismos para la elaboración de sus propias políticas y dar cumplimiento a la Decisión Administrativa nro. 641/2021 JGM.

V. Ecosistema nacional de ciberseguridad: modelo de gobernanza

La definición de un modelo de gobernanza de ciberseguridad adecuado para un país inicia con la identificación de los actores que conforman el ecosistema del país y su correspondiente clasificación. Esta fase implica identificar y priorizar a los actores clave a nivel nacional e internacional en función de los objetivos específicos de la iniciativa y del nivel de madurez actual del país, considerando la transversalidad de la ciberseguridad y un enfoque de múltiples partes interesadas.

Una vez que se identifiquen las partes interesadas, se debe definir cuál es la función que desempeña cada uno de estos actores en el ecosistema de ciberseguridad del país, sus responsabilidades particulares y sus expectativas. De esta forma, la propuesta de modelo tendrá insumos que permitan la formulación de principios, objetivos, procesos y actividades, así como de mecanismos e instrumentos que permitan la participación de estas partes, procurando la satisfacción de sus expectativas y la maximización de los beneficios a obtener de su interacción.

Figura 5.1: Clúster de partes interesadas a nivel nacional para la creación de un marco de gobernanza

Para la identificación y clasificación de partes interesadas se definen distintas instituciones en cada sector para su tipificación de la siguiente manera:

Figura 5.2: Actores relevantes que constituyen grupos de partes interesadas

Academia, grupos de la sociedad civil y representantes de la gobernanza de Internet
- Universidades Públicas Nacionales
- Universidades Privadas
- Ministerio de Educación
- Secretaría de Innovación Pública
- CONICET
- Ente Nacional de Comunicaciones

Justicia penal y aplicación de la ley
- Ministerio de Seguridad de la Nación y organismos provinciales de Seguridad
- Ministerio de Justicia y Derechos Humanos de la Nación
- Fiscalías especializadas federales y provinciales
- Procuración General de la Nación
- Cuerpos policiales federales y provinciales

Comunidad de Defensa e Inteligencia
- Ministro de Defensa
- Fuerzas Armadas
- Fuerzas de Seguridad
- Agencia Federal de Inteligencia

Ministerios de Gobierno
- Ministerio de Ciencia y Tecnología
- Ministerio de Educación
- Ministerio de Economía
- Ministerio de Relaciones Exteriores, Comercio Internacional y Culto
- Ministerio de Transporte
- Ministerio de Salud
- Ministerio de Justicia y Derechos Humanos
- Ministerio de Defensa
- Ministerio de Seguridad
- Otros ministerios

CSIRT y Líderes de TI del Gobierno y el Sector Privado
- Puntos Focales de Seguridad de la Administración Nacional
- Referentes de ciberseguridad de los Gobiernos Provinciales
- Principales empresas de tecnología de la información
- Equipos de respuesta a incidentes nacionales y/o sectoriales

Legisladores / propietarias de políticas
- Legisladores Nacionales
- Legisladores provinciales
- Miembros de comités especiales

Cooperación internacional
Representantes de organizaciones internacionales (p. ej., oficinas de las Naciones Unidas, Banco Mundial), organizaciones no gubernamentales (ONG) internacionales y socios de embajadas relevantes

Grupo de trabajo de ciberseguridad
Integrantes del Comité de Ciberseguridad creado por Decreto N° 577/2017 (t.a.)

Sector privado y empresa
- Principales industrias y empresas de alta tecnología
- Pequeñas y medianas empresas (PYME)
- Asociaciones profesionales
- Cámaras del sector

Infraestructura Crítica Nacional
- Sector TIC
- Sector financiero
- Sector Energía
- Sector Hídrico
- Sector de Salud
- Sector Transportes
- Sector Alimentación
- Sector Nuclear
- Sector Químico
- Sector Espacio
- Sector Estado

En el caso de Argentina, el país cuenta con un conjunto amplio de partes interesadas que son relevantes para los esfuerzos nacionales de ciberseguridad. La siguiente lista ejemplifica e ilustra de forma no exhaustiva distintos actores y partes interesadas son importantes en el ecosistema de ciberseguridad de Argentina. Esta puede incorporar nuevos actores con base en la dimensión que se seleccione para la etapa posterior del **Programa de Optimicemos la Ciberseguridad.**

Tabla 5.1: Base de ecosistema de influencia en materia de ciberseguridad – Argentina

Grupo de partes interesadas	Actores clave
Ministerios de Gobierno	• Presidencia de la República • Congreso de la Nación • Jefatura de Gabinete de Ministros • Ministerio de Ciencia, Tecnología e Innovación • Ministerio de Economía • Ministerio del Interior • Secretaría de Innovación Pública • Centro Nacional de Respuesta a Incidentes Informáticos • Ministerio de Seguridad • Policía Federal Argentina • Ministerio de Defensa • Comando Conjunto de Ciberdefensa • Agencia Federal de Inteligencia • Ministerio de Relaciones Exteriores y Culto • Ministerio de Justicia y Derechos Humanos • Ministerio Público Fiscal • Unidad Fiscal Especializada en Ciberdelincuencia
Tipo de interacción	
Relación directa a través de líderes expertos en la materia, entre los que son clave en la formulación de políticas.	
Relevancia	
El establecimiento de un marco de gobernanza, comunicación y colaboración entre distintas entidades gubernamentales es primordial para maximizar recursos públicos y consolidar temas relacionados con la ciberseguridad como prioridad nacional.	

Grupo de partes interesadas	Actores clave
Socios Internacionales	• Brasil • Canadá • Chile • China • Corea del Sur • Estados Unidos • Reino Unido • Unión Europea • Uruguay • Paraguay • Perú • México
Tipo de interacción	
Alianzas y cooperación con otros gobiernos generan diversos canales de influencia y mutuo beneficio. La posición política del país es de apertura amplia al diálogo y la cooperación con todos los países. Históricamente, los principales vínculos de influencia y comercio han sido con Estados Unidos y España. Sin embargo, los cambios en la geopolítica y la atención a temas como la ciberseguridad han expandido este grupo de relaciones a nuevos influenciadores como la Unión Europea, Estonia e Israel.	
Relevancia	
Establecer una relación estratégica y en temas de mutuo interés en materia de ciberseguridad.	

Grupo de partes interesadas	Actores clave
Instituciones multilaterales y organismos internacionales	• OEA • BID • Banco de desarrollo de América Latina (CAF) • Consejo de Europa • Organización de las Naciones Unidas • Consejo Latinoamericano de Ciencias Sociales (CLACSO) • Comisión Económica para América Latina y el Caribe (CEPAL) • Interpol • Ameripol • Europol • Mercado Común del Sur (MERCOSUR) • Comunidad de Estados Latinoamericanos y Caribeños (CELAC) • Secretaria General Iberoamericana (SEGIB) • Instituto Nacional de Ciberseguridad de España (INCIBE) • Foro Global sobre Ciber Experiencia (GFCE por sus siglas en inglés) • CSIRTAmericas • Grupo de Trabajo de composición abierta sobre la seguridad y el uso de las tecnologías de la información y las comunicaciones (OEWG por sus siglas en inglés) • Banco Mundial • Red GEALC
Tipo de interacción	
Canal de influencia en la formulación de políticas, el consenso internacional y la cooperación financiera.	
Relevancia	
Examinar sus ofertas de apoyo técnico y financiero en materia de ciberseguridad.	

Grupo de partes interesadas	Actores clave
Academia y Sociedad Civil **Tipo de interacción** A partir de la oferta de educación en materia de ciberseguridad se puede asegurar la sostenibilidad de distintas iniciativas en la materia, así como proporcionar los recursos humanos necesarios para avanzar en la capacidad de ciberseguridad del país. **Relevancia** La academia y la sociedad civil son sectores clave de la sociedad y un entorno fundamental para que prospere la cultura e industria de la tecnología y la innovación, mediante el desarrollo de conocimientos, investigación e innovación.	• Universidad Católica Argentina • Universidad de Palermo • Universidad Fasta • Universidad CEDSA • Instituto Universitario de la Policía Federal Argentina • Universidad de Buenos Aires • Universidad Tecnológica Nacional • Universidad Austral • Universidad Católica de Salta (UCASAL) • Universidad del Gran Rosario • Universidad Nacional de La Plata • Centro Europeo de Postgrado (CEUPE) • Argentina Cibersegura • Adecuarse • ECyT-ar • CARI • CIPPEC

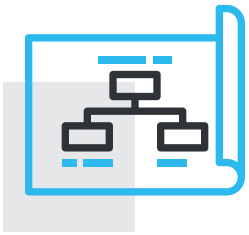
Grupo de partes interesadas	Actores clave
Industria tecnológica **Tipo de interacción** Líderes tecnológicos clave que pueden colaborar en áreas como la ciberdelincuencia e impulsar posibles alianzas de ciberseguridad. **Relevancia** Sector importante para multiplicar impacto y sinergias con distintos esfuerzos gubernamentales que contribuyan a acelerar la madurez de la ciberseguridad en el país.	• Asociación Gremial de Computación • Cámara Argentina de Comercio y Servicios • Consejo Profesional de Ciencias Informáticas de Buenos Aires • Asociación Argentina de Usuario de la Informática y las Comunicaciones • Cámara de Cooperativas de Telecomunicaciones (CATEL) • Cámara Argentina de PyMES Proveedoras de la Industria de las Telecomunicaciones (CAPPITEL) • Federación de Comercio e Industria de la Ciudad Autónoma de Buenos Aires (FECOBA) • Cámara Argentina de Telefonía IP y Comunicaciones Convergentes (CATIP) • Cámara de Comercio de los Estados Unidos en Argentina (Amcham Argentina) • Cámara Argentina de Internet (CABASE) • Cámara de la Industria Argentina del Software (CESSI)

Grupo de partes interesadas	Actores clave
Proveedores públicos y privados de servicios críticos o esenciales **Tipo de interacción** Establecer mecanismos de cooperación con proveedores y operadores que brindan servicios esenciales a la sociedad, dado que en caso de disrupción podrían generar un impacto económico y social. **Relevancia** Siendo que este grupo de actores es relevante para el buen funcionamiento de la sociedad, es importante monitorear la agenda regulatoria y compromisos en materia de ciberseguridad a efectos de garantizar la disponibilidad de los servicios esenciales.	• Instituciones gubernamentales • Compañía Administradora del Mercado Eléctrico Mayorista (CAMMESA) • Principales empresas de transporte de hidrocarburos por poliductos, oleoductos y gasoductos • Principales empresas de transporte marítimo, aéreo y terrestre • Principales empresas de distribución de agua potable • Principales entidades bancarias y financieras del sistema financiero supervisadas por el Banco Central • Principales instituciones del sistema de salud y seguridad social • Principales empresas de satélites geoestacionarios (ARSAT) y no estacionarios (CONAE) • Principales empresas gestoras de las centrales nucleares (Atucha, Atucha II y Embalse) • Principales empresas de la industria petroquímica • Principales proveedores de servicios de comunicación • Principales empresas proveedoras de servicios de alimentación

VI. Análisis comparativo del avance en madurez de ciberseguridad basado en la evaluación CMM 2016 y 2020

Argentina ha sido valorado en dos (2) oportunidades bajo el modelo del CMM. La primera con ocasión de haber participado entre los países en los que se desplegó por primera vez el modelo como insumo del reporte: "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?" (OEA & BID, 2016); la segunda como insumo del reporte "Ciberseguridad- Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe" (OEA & BID, 2020). El objetivo de los reportes es ofrecer a los países de la región no sólo una evaluación de investigación documental sobre el estado de la ciberseguridad, sino también recomendaciones que se podrían considerar para fortalecer las capacidades nacionales en esta materia. Cabe destacar que en comparación con el Programa de Optimicemos la Ciberseguridad que opta por la implementación de la edición 2021 del modelo del CMM, ambos estudios utilizan la edición previa del 2016 (Figura 4.1).

Modelo CMM 2016 – dimensiones y factores



Dimensión 1: Política y Estrategia de Ciberseguridad

Diseño de estrategia y resiliencia de ciberseguridad

D1. 1 Estrategia Nacional de Ciberseguridad
D1. 2 Respuesta a Incidente
D1. 3 Protección de Infraestructura Crítica (IC)
D1. 4 Gestión de Crisis
D.1 5 Defensa Cibernética

» Capacidad del país para desarrollar y aplicar una estrategia de ciberseguridad
» El desarrollo, adopción y aplicación de políticas públicas en materia de ciberseguridad

Dimensión 2: Cultura y Sociedad Cibernética

Fomentar una cultura de ciberseguridad responsable en la sociedad

D2. 1 Mentalidad de Ciberseguridad
D2. 2 Confianza y Seguridad en Internet
D2. 3 Comprensión del Usuario de la Protección de Información Personal en Línea
D2. 4 Mecanismos de Presentación de Informes
D2. 5 Medios y Redes Sociales

» Nivel de alfabetización digital en la sociedad
» Comprensión de riesgos y posibles impactos de ciberataques
» Confianza en servicios de internet, comercio electrónico, administración pública electrónica, entre otros

Dimensión 3: Educación, Capacitación y Habilidades en Ciberseguridad

Desarrollo del conocimiento de ciberseguridad

D3. 1 Sensibilización
D3. 2 Marco para la Educación
D3. 3 Marco para la Formación Profesional

» Disponibilidad de programas de concientización sobre ciberseguridad
» Oferta educativa y de capacitación profesional

Dimensión 4: Marcos Legales y Regulatorios

Creación de marcos legales y regulatorios efectivos

D4. 1 Marcos Legales

D4. 2 Sistema de Justicia Penal

D4. 3 Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético

» Capacidad gubernamental para diseñar y promulgar legislación nacional directa e indirectamente relacionada con la ciberseguridad

» Capacidad de implementación legislativa, en función de las competencias de las autoridades del sistema judicial

Dimensión 5: Estándares, Organizaciones y Tecnologías

Control de riesgos a través de estándares, organizaciones y tecnologías

D5. 1 Adhesión a los Estándares

D5. 2 Resiliencia de Infraestructura de Internet

D5. 3 Calidad del Software

D5. 4 Controles Técnicos de Seguridad

D5. 5 Controles Criptográficos

D5. 6 Mercado de Ciberseguridad

D5. 7 Divulgación Responsable

» La aplicación de estándares y mejores prácticas de ciberseguridad y la implementación de procesos y controles

» Desarrollo de tecnologías y productos para reducir los riesgos de ciberseguridad

La siguiente tabla comparativa evalúa de manera general los avances de cada dimensión del CMM correspondiente a Argentina, basándose en los dos estudios regionales de la OEA y el BID (2016 y 2020). El presente análisis tiene como objetivo identificar áreas de oportunidad que tiene el país para avanzar progresivamente hacia el nivel cinco (5) del CMM en todas las dimensiones, centrándose en las principales fortalezas y oportunidades identificadas, así como su relevancia e implicaciones en el nivel de madurez de ciberseguridad del país.

Tabla 6.1: Análisis Comparativo del CMM: Argentina 2016-2020

Dimensión 1 | Política y Estrategia Nacional de Ciberseguridad

Puntaje	Fortalezas	Oportunidades	
2016: 2.04 **2020:** 2.21 ⬆	La adopción de la Estrategia Nacional de Ciberseguridad en 2019 es un importante logro que se refleja en el factor de Estrategias Nacionales de Ciberseguridad, particularmente palpado en el avance del aspecto referente a la organización. La mejora en el factor de respuesta a incidente es evidente, dado que dos aspectos (coordinación y modelo de operación) alcanzan un nivel más alto de capacidad.	Con la excepción de dos aspectos de dos distintos factores, la primera dimensión no exhibe avances relevantes. El desarrollo de un Plan de Acción derivado de la Estrategia Nacional de Ciberseguridad 2019 a fin de desarrollar un marco de gobernanza e implementación que permita accionar los objetivos de la Estrategia Nacional es clave para obtener un progreso significativo y palpable en esta dimensión.	

Dimensión 2 | Cultura cibernética y sociedad

Puntaje	Fortalezas	Oportunidades	
2016: 0.80 **2020:** 2.10 ⬆	Esta es una de las dimensiones con una mejora evidente, destacando la mejora en el factor de mentalidad de ciberseguridad en el sector privado. Asimismo, el factor relacionado con la compresión del usuario de la protección de la información en línea ha tenido una mejora en todos sus aspectos incluyendo mecanismos de denuncia y medios y redes sociales.	En el factor de confianza y seguridad en Internet no hubo mejora de 2016 a 2020, al igual que no se observan avances en el nivel de concientización a nivel de gobierno y de los usuarios.	

Tabla 6.1: Análisis Comparativo del CMM: Argentina 2016-2020

Dimensión 3 | Formación, capacitación y habilidades en seguridad cibernética			
Puntaje	**Fortalezas**	**Oportunidades**	
2016: 2.10 **2020:** 2.30 ⬆	La tercera dimensión tuvo un avance en el aspecto de capacitación profesional, particularmente en el aspecto de apropiación. En general, Argentina cuenta con una oferta importante de cursos y programa académicos sobre ciberseguridad, sin embargo, esta oferta debería estar alineada a las necesidades de los sectores y las demandas económicas.	Del 2016 al 2020, Argentina no logró un avance sustancial en la formación, capacitación y habilidades de ciberseguridad, una dimensión que es la base para el desarrollo de otras dimensiones. La cooperación y alianzas públicas, privadas y académicas son esenciales para poder definir las necesidades del país y trazar objetivos comunes.	

Tabla 6.1: Análisis Comparativo del CMM: Argentina 2016-2020

Dimensión 4 | Marcos legales y regulatorios			
Puntaje	**Fortalezas**	**Oportunidades**	
2016: 1.30 **2020:** 2.50 ⬆	En 2016, Argentina reportaba un marco regulatorio poco homogéneo, con la ausencia de legislaciones respecto a protección de datos, defensa del consumidor en línea, entre otros temas relacionados con la ciberseguridad. Los avances en los marcos legales y regulatorios son notables con avances en marcos legales en la privacidad, libertad de expresión y otros derechos humanos en línea, así como la promulgación de legislación sobre protección de datos, protección infantil en línea, legislación de protección al consumidor y legislación de propiedad intelectual. Adicionalmente, el factor correspondiente a marcos de cooperación formales e informales para combatir el delito cibernético muestra que ha sido fortalecido en aspectos como la cooperación formal e informal. Estos avances han logrado que la cuarta dimensión tenga uno de los niveles de madurez más avanzados en el país.	Pese a que en 2016 el sistema de justicia penal era un factor de resaltar, en comparación con el resto de los países de la región, cuatro años después, en el 2020, no se observa mayor avance en la materia. Siendo la dimensión donde el país más destaca a nivel regional es importante mantener el liderazgo, además de abordar la brecha para alcanzar el nivel más alto de madurez de ciberseguridad. Esta dimensión, además del trabajo técnico en diseño de políticas, legislación, también requiere de un fuerte compromiso gubernamental e institucional para continuar progresando en la materia.	

Tabla 6.1: Análisis Comparativo del CMM: Argentina 2016-2020

Dimensión 5 | Estándares, organizaciones y tecnologías			
Puntaje	**Fortalezas**	**Oportunidades**	
2016: 1.0	En la quinta dimensión se determinan avances partiendo de ningún nivel a dos niveles de progreso en los factores de calidad del software, controles técnicos de seguridad y controles criptográficos. Asimismo, en el factor de mercado de ciberseguridad existe un incremento en el aspecto de divulgación responsable.	La quinta dimensión presenta áreas de oportunidad, ante el estancamiento de avances en los factores de cumplimiento de estándares y el mercado de ciberseguridad. Asimismo, los indicadores son precarios y exhibe el área de oportunidad para mejorar los estándares, organizaciones y tecnologías del país.	
2020: 2.0 ⬆			

Hoja de ruta en ciberseguridad para Argentina para la Dimensión 3: Desarrollando Conocimiento y Capacidades en Ciberseguridad

El análisis de las secciones anteriores ha proporcionado una perspectiva general de desarrollo de la economía digital del país, el posicionamiento internacional en los estudios globales sobre ciberseguridad, un mapa del ecosistema de influencia de la ciberseguridad, y una revisión de la evaluación del CMM a partir de los estudios de 2016 y 2020. Asimismo, también se identifican las fortalezas, oportunidades y la cobertura que las directrices gubernamentales en implementación ofrecen con relación al modelo CMM.

En este apartado se presenta la hoja de ruta basada en el CMM edición 2021, en particular sobre la Dimensión 3 "Desarrollando Conocimiento y Capacidades en Ciberseguridad" la cual revisa la disponibilidad, la calidad y la aceptación de los programas para varios grupos de partes interesadas, incluidos el gobierno, el sector privado y la población en general.

El objetivo de este apartado es la de presentar las mejores prácticas internacionales para que dichas partes interesadas puedan contar con programas que a) aumenten la conciencia sobre seguridad cibernética en todo el país, b) programas de educación en seguridad cibernética de alta calidad y suficientes maestros y instructores calificados, c) programas asequibles de capacitación profesional en ciberseguridad para crear un cuadro de profesionales en ciberseguridad y d) la suficiente investigación y la innovación en seguridad cibernética para abordar los desafíos tecnológicos, sociales y comerciales y para avanzar en la construcción de conocimientos y capacidades en seguridad cibernética en el país.

Tabla 6.2: Basada en el CMM edición 2021
CMM D3 – Desarrollando conocimiento y capacidades de ciberseguridad

Factor	Aspectos
D3.1: Desarrollando concientización sobre la ciberseguridad	D3.1.1: Iniciativas de concientización lideradas por el gobierno D3.1.2: Iniciativas de concientización lideradas por el sector privado D3.1.3: Iniciativas de concientización lideradas por la sociedad civil D3.1.4: Concientización de altos ejecutivos
D3.1.2: Iniciativas de concientización lideradas por el sector privado	D3.2.1: Oferta D3.2.2: Gestión
D3.1.3: Iniciativas de concientización lideradas por la sociedad civil	D3.3.1: Oferta D3.3.2: Asequibilidad
D3.1.4: Concientización de altos ejecutivos	D3.4.1: Investigación e innovación en ciberseguridad

Recomendaciones

D3.1

Desarrollando concienciación sobre la ciberseguridad

1. Desarrollar e implementar un programa nacional de concientización sobre ciberseguridad, que abarque la campaña de concientización ya realizada, con una guía de implementación robusta y detallada, el cual deberá contener actividades que estén directamente relacionadas a las actividades u objetivos estratégicos de la nueva ENCS.

2. Nombrar un ente, comité, u órgano coordinador del programa, el cual deberá tener un mandato expreso -funciones y responsabilidades claras- y recursos suficientes para implementar las actividades del programa.

3. Ampliar los contenidos que hoy existen en el sitio web de la Dirección Nacional de Ciberseguridad, generando un portal (página web) dedicado para publicar información, documentos, videos, actividades y cualquier material del programa para desarrollar y mejorar las habilidades y conocimiento de la sociedad en general y que dicho portal sea ampliamente difundido en las diferentes actividades del programa.

4. Que dicho programa de concientización integre actividades/talleres/capacitaciones enfocadas a la industria, academia, sociedad civil y otros grupos vulnerable, tales como infantes, mujeres, adultos mayores e incluso PYMES, como los que ya realiza el Centro G+T dependiente de la Jefatura de Gabinete de Ministros, Justicia con voz en la web del Ministerio de Justicia y Derechos Humanos, etc.

5. Que las autoridades competentes tomen en consideración y evalúen periódicamente los riesgos emergentes de ciberseguridad para actualizar dicho programa de concientización.

6. Que el programa y/o guía de implementación contemple un proceso de revisión de las actividades, lo cual incluye la recolección y análisis de métricas y estadísticas, las cuales van a permitir revisar y medir la efectividad del programa en general y los recursos asignados. También se recomienda que los resultados de esas evaluaciones sean utilizados para actualizar y refinar las actividades tanto del programa de concientización como de la nueva ENCS.

7. Crear un grupo de trabajo conformado por el gobierno, actores del sector privado y de la academia, y de la sociedad civil, sobre la base del Grupo de Trabajo creado por el Comité de Ciberseguridad, para desarrollar políticas y/o actividades de apoyo o acompañamiento, aportar recursos, intercambiar información relevante e identificar soluciones y prácticas de ciberseguridad, etc. para el programa. En esa misma línea, también se recomienda que actores del sector privado, academia y de la sociedad civil se involucren activamente y sean impulsores o facilitadores de actividades u objetivos del programa, lo cual va a permitir una mejor coordinación entre el gobierno, sector privado, academia, y sociedad civil.

8. Que las colaboraciones entre el gobierno, el sector privado, academia, y la sociedad civil sean evaluadas regularmente y usadas como referencia para mejorar los procesos colaborativos del programa y otras actividades a nivel nacional.

Recomendaciones **D3.1** **Desarrollando concienciación sobre la ciberseguridad**	9. Desarrollar actividades/talleres/capacitaciones para ejecutivos de alto nivel, empresarios o administradores de organizaciones del sector público, sector privado, la academia y la sociedad civil, las cuales deben abordar al menos los siguientes temas: riesgos cibernéticos en general, algunos de los principales métodos de ataque, cómo las organizaciones abordan los problemas o desafíos de la ciberseguridad, e identificación de activos estratégicos y medidas y controles para protegerlos. 10. Impartir cursos de concientización para miembros del sector empresarial, los cuales deben ser obligatorios para todos los sectores del ecosistema. 11. Que los esfuerzos de concientización en la gestión de crisis cibernéticas en el sector empresarial alcance un nivel preventivo.

Recomendaciones **D3.2** **Educación en ciberseguridad**	1. Integrar cursos acreditados de ciberseguridad en los programas de estudio y grados académicos de la carrera de ciencias de la computación, ingenierías y carreras afines. 2. Continuar desarrollando e impulsando carreras acreditadas, en los diferentes grados académicos, enfocadas en temas de la ciberseguridad y seguridad de la información, las cuales deberán cubrir temas técnicos, no técnicos, jurídicos, política pública, entre otros aspectos afines. Así mismo, incentivar y promover la educación multidisciplinaria de la ciberseguridad en el país. 3. Crear un grupo de trabajo conformado por actores de la academia, de la industria y del gobierno para trabajar en conjunto en el diseño de planes de estudio que satisfagan las necesidades actuales del país y principalmente de la industria, y que esos resultados se contemplen en la nueva ENCS. 4. Crear, en la medida de lo posible, un presupuesto nacional dedicado a la educación y formación e investigación y laboratorios en temas de ciberseguridad en las universidades u otras instituciones académicas. También se recomienda que la administración y asignación de ese presupuesto esté basado en la demanda de la educación de ciberseguridad a nivel nacional. 5. Crear, junto con otros actores o socios, un fondo nacional de becas y/o préstamos estudiantiles para financiar el costo de las carreras y/o cursos de ciberseguridad, incluyendo certificaciones de la industria. Se recomienda a las autoridades competentes crear competencias, iniciativas y otros incentivos para promocionar la educación y formación profesional en temas de ciberseguridad y así incrementar la matricula en las carreras de ciberseguridad.

Recomendaciones D3.2 Educación en ciberseguridad	6. Que las autoridades competentes, y en especial a los actores de la industria, creen programas de pasantías en diferentes sectores de la industria a efectos de desarrollar y combinar el conocimiento con habilidades prácticas. 7. Que las autoridades competentes monitoreen y le lleven el pulso a la oferta y demanda de las carreras y/o cursos de ciberseguridad, y para ello se aconseja llevar métricas y estadísticas para mejorar el proceso de toma de decisiones y asignación de recursos. Así mismo, dichas métricas y estadísticas servirán para mejorar el cuadro de educadores o académicos en temas de ciberseguridad. 8. Que las universidades y otras instituciones académicas compartan información relevante y lecciones aprendidas con sus pares a nivel nacional e internacional. 9. Que las autoridades competentes creen un centro de excelencia en temas de ciberseguridad y que este centro sirva para desarrollar capacidades y formar expertos a nivel nacional, regional e internacional.

Recomendaciones D3.3 Capacitación profesional en ciberseguridad	1. Desarrollar e implementar un programa nacional de formación, retención y capacitación para desarrollar habilidades específicas. 2. Crear un registro nacional de profesionales con certificados y calificaciones excepcionales. Asegurarse que esos profesionales y expertos en ciberseguridad estén entrenados y dominan el análisis, planeamiento, procesos y problemáticas derivadas de la ciberseguridad. 3. Diseñar una amplia gama de cursos de capacitación, los cuales deben estar alineados con los requerimientos de la demanda nacional y las buenas prácticas internacionales. Asegurarse que los cursos de capacitación están enfocados en desarrollar las habilidades necesarias para comunicar temas complejos y desafíos a profesionales sin formación técnica, tales como gerentes y administradores. 4. Considerar los marcos vocacionales y mejores prácticas de ciberseguridad tanto nacionales, regionales como internacionales para diseñar el plan de estudio de cursos y otros programas académicos de formación de profesionales en ciberseguridad. 5. Promover la oferta de certificaciones de la industria en todos los sectores del país, y que existan facilidades, tales como becas, prestamos, etc., para incentivar a los profesionales en ciberseguridad a continuar su formación académica. Así mismo, se recomienda a las autoridades competentes identificar y entender las necesidades de la industria y del mercado en general y además documentar la lista de requisitos de capacitación.

Recomendaciones

D3.3

Capacitación profesional en ciberseguridad

6. Crear incentivos y otros beneficios tanto en el sector público como en el sector privado para retener en el país a los estudiantes y/o profesionales que hayan completado exitosamente los programas académicos y/o de formación profesional.

7. Que las autoridades competentes monitoreen y le lleven el pulso a la oferta y demanda de los cursos de capacitación de ciberseguridad, y para ello se aconseja llevar métricas y estadísticas para mejorar el proceso de toma de decisiones y asignación de recursos. Así mismo, dichas métricas y estadísticas servirán para mejorar la oferta y sostenibilidad de esos cursos.

8. Que las organizaciones públicas y privadas implementen políticas de transferencia de conocimiento para beneficiar a todo el staff/personal de la organización.

9. Que las organizaciones públicas y privadas implementen iniciativas para la creación de puestos de trabajo en ciberseguridad y además motiven a los empleadores a capacitar su staff/personal y que se conviertan en profesionales en ciberseguridad.

Recomendaciones

D3.4

Investigación e innovación en ciberseguridad

1. Que las autoridades competentes integren e implementen actividades de investigación y desarrollo en temas de ciberseguridad en la nueva ENCS. Así mismo, asegurarse que los procesos y recursos para la implementación de esas actividades estén identificados y además sean suficientes.

2. Analizar la posibilidad de desarrollar una estrategia independiente y enfocada en investigación y desarrollo en temas de ciberseguridad y asegurar los recursos necesarios para su implementación.

3. Que el país participe activamente en redes de colaboración relacionadas a investigaciones de ciberseguridad e innovación tanto a nivel regional como internacional. Así mismo, que participe en colaboraciones, principalmente en el desarrollo de comunidades o grupos de interés regionales e internacionales, donde se ponen en marcha prácticas y desarrollo de vanguardia y temas prioritarios de ciberseguridad e innovación.

4. Evaluar periódicamente los riesgos emergentes de ciberseguridad y que los resultados sean considerados en el desarrollo de futuros programas de la estrategia de investigación y desarrollo.

5. Desarrollar sinergias entre las universidades e instituciones académicas y la industria para apoyar técnica y financieramente actividades de investigación y de desarrollo, y además en el desarrollo y revisión de planes de estudio de carreras de ciberseguridad según las necesidades de la industria.

6. Que las autoridades competentes lleven métricas y estadísticas para medir el rendimiento de las actividades de investigación y de desarrollo, y el progreso y las capacidades del país en general y de los diferentes sectores.

Recursos de apoyo y mejores prácticas de interés

En este apartado se listan recursos de contenido y mejores prácticas internacionales que pueden servir de apoyo a los equipos de trabajo durante el proceso de diseño de la hoja de ruta, estrategias y planes de acción para el país en la Dimensión 4.

Tabla 6.3: Recursos para trabajos en D3: Desarrollando conocimiento y capacidades de ciberseguridad

Factor	Recursos de otras instituciones	Mejores prácticas internacionales
D3.1: Desarrollando concientización sobre la ciberseguridad	Gestión del Riesgo Cibernético Nacional Cybersecurity Capacity Maturity Model for Nations (CMM 2021 version) Cybersecurity: Risks, Progress, and the way forward in Latin America and the Caribbean OECD: Recommendation of the Council on OECD Legal Instruments Digital Security of Critical Activities	European Cybersecurity Challenge INCIBE: Día de la Internet Segura GFCE Cybersecurity Awareness Campaigns Session 2020 Cyber Security Awareness Campaigns: Why do they fail to change behaviour? The Cybersecurity Awareness Toolkit Building a Cybersecurity Awareness Program Cybersecurity awareness for children: A systematic literature review Development of a Cyber Security Awareness Strategy Using Focus Group Discussion
D3.1.2: Iniciativas de concientización lideradas por el sector privado	NIST 800-181 Workforce Framework for Cybersecurity CYBERSECURITY SKILLS DEVELOPMENT IN THE EU	IDB MOOCs: Fundamentos de Ciberseguridad: un enfoque práctico UK – Initial National Cybersecurity Skills Strategy How Governments Can Build Resiliency in a New Normal Cybersecurity awareness initiatives for school learners in South Africa and the UK

Factor	Recursos de otras instituciones	Mejores prácticas internacionales
D3.1.3: Iniciativas de concientización lideradas por la sociedad civil	NIST 800-181 Workforce Framework for Cybersecurity CYBERSECURITY SKILLS DEVELOPMENT IN THE EU	INCIBE: Cybersecurity Summer Boot Camp OEA – Creando una Trayectoria Profesional en Seguridad Digital Cybersecurity Professional Training- CISA Online cybersecurity courses of 2021: free and paid certification programs, degrees and masters
D3.1.4: Concientización de altos ejecutivos	FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN Aegis: White Paper on Research and Innovation in Cybersecurity	Red colombiana de Investigación en Ciberseguridad The Knowledge Portal for Cyber Capacity Building UK: Academic Centres of Excellence in Cyber Security Research CMU – SEI – Cybersecurity Center Development Free Labs Cybersecurity Skills - MITRE framework labs

OPTIMICEMOS LA CIBERSEGURIDAD

Modelo de Madurez de Capacidad de Ciberseguridad para las Naciones

Panorama Nacional de Ciberseguridad

Argentina
2023