Instituto de Desarrollo Digital
de Latinoamérica y el Caribe

DISEÑO DE POLÍTICAS PÚBLICAS MULTISECTORIALES EN CIBERSEGURIDAD

MARZO 2025

AUTOR: Andrés Piazza

CONTRATO DE OBRA EX-2024-00055285- -CFI-GES#DC Hoja Nº7 PROVINCIA: Córdoba TÍTULO: Diseño de Políticas Públicas Multisectoriales en Ciberseguridad e Inteligencia Artificial. FUNDACIÓN: Fundación Instituto de Desarrollo Digital de América Latina y El Caribe (IDDLAC)

ABSTRACT

El presente informe analiza el estado de la ciberseguridad en la provincia de Córdoba y propone una hoja de ruta para fortalecer sus políticas públicas. A partir de un enfoque multisectorial, se identifican desafíos clave: infraestructura tecnológica insuficiente, escasez de profesionales especializados, falta de actualización normativa y ausencia de coordinación entre actores públicos y privados. También se evidencian vulnerabilidades en la seguridad de datos estatales y privados, una baja adopción de estándares internacionales y dificultades en la implementación de estrategias de protección.

Para abordar estos problemas, el informe propone la creación del Consejo Provincial de Políticas Digitales, un organismo que coordine políticas en ciberseguridad e inteligencia artificial, con participación del sector privado y la academia. Sus objetivos incluyen mejorar la resiliencia digital del Estado y las empresas, fortalecer la formación de talento especializado y actualizar el marco regulatorio en protección de datos. Se plantea además la necesidad de potenciar el CSIRT Córdoba, promoviendo su uso y su legitimidad como entidad central en la respuesta a incidentes.

El documento compara estrategias de ciberseguridad de Argentina, Chile, Colombia y Brasil, extrayendo lecciones aplicables a Córdoba. Se presentan recomendaciones concretas, como la actualización normativa, el fortalecimiento de la infraestructura de seguridad y la implementación de programas de formación especializada. Finalmente, se destaca la necesidad de generar conciencia sobre la ciberseguridad en la ciudadanía y los sectores productivos, asegurando una estrategia sostenible que permita a la provincia mejorar su competitividad y protección digital.

Palabras clave: Ciberseguridad, políticas públicas, infraestructura digital, seguridad de la información.

Mesa Provincial de Ciberseguridad

Tabla de Contenidos

Mesa Provincial de Ciberseguridad
Tabla de Contenidos

1. INTRODUCCIÓN

Este reporte presenta la ejecución del proyecto de la Mesa provincial de Ciberseguridad. El objetivo del mismo es diseñar una estrategia para futuras políticas provinciales en materia de ciberseguridad, fundamentada en entregables previos que sirven como insumo: diagnósticos exhaustivos de la problemática elaborados de manera participativa con los sectores público, privado, sociedad civil y académico.

El trabajo comenzó con la elaboración anticipada de una versión preliminar de los mapas de actores en el ámbito de la ciberseguridad y con la constitución de una mesa provincial multisectorial dedicada a este tema. Esta mesa tiene como objetivo facilitar la interacción con los actores relevantes en el diseño de la hoja de ruta y en los diagnósticos previos. Dichos procesos de diagnóstico se nutrieron no solo de información, sino también de un diálogo interactivo con los actores involucrados. El resultado se vio enriquecido por este proceso, aunque requirió un replanteo en la metodología

El enfoque interactivo permitió la co-creación de políticas públicas a través de un diagnóstico unificado que refleja no solo la opinión del Instituto de Desarrollo Digital de América Latina y el Caribe, sino también el consenso entre los diversos actores. Este proceso es fundamental para priorizar la ciberseguridad como un área clave en las políticas gubernamentales, asegurando que las estrategias desarrolladas respondan efectivamente a las amenazas y vulnerabilidades actuales del entorno digital

2. DIAGNÓSTICO SOBRE EL ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN EN LA PROVINCIA DE CÓRDOBA

a. Panorama General

Este informe presenta un diagnóstico sobre el estado actual de las políticas públicas de la seguridad de la información en la provincia de Córdoba. En tal sentido, el objetivo principal es identificar los desafíos, fortalezas y áreas críticas que permitan desarrollar una política pública integral en materia de ciberseguridad

El diagnóstico incluye una percepción del grado de evolución de **tres ejes** fundamentales del ecosistema de ciberseguridad de la provincia de Córdoba:

- El nivel de desarrollo de los proveedores de servicios de ciberseguridad
- La calidad de la transformación digital de las industrias privadas.
- La gestión administrativa del gobierno electrónico por parte del Estado.

Los actores clave del ecosistema –tanto del sector público, como del privado y el académico– coincidieron en identificar **deficiencias** en tres áreas fundamentales:

LIMITACIONES EN INFRAESTRUCTURA TECNOLÓGICA

FALTA DE REGULACIONES ACTUALIZADAS

ESCASEZ DE PROFESIONALES ESPECIALIZADOS EN LA MATERIA

Luego de realizar numerosas entrevistas y consultas personales y analizar encuestas con personas destacadas del ecosistema, se detectó un consenso respecto de las vulnerabilidades y aspectos clave en la gestión de la ciberseguridad en la provincia.

En este plano, es evidente que existe una enorme cantidad de delitos informáticos, como así también de estafas y casos de ransomware. La situación global es acuciante. Tal es así, que el Foro Económico Mundial de 2024 en su Reporte de Riesgos Globales[1].

De manera lógica, Argentina no es la excepción. En un relevamiento sobre incidentes[2] en las bases de datos críticas del país desde 2017 se puede observar un importante crecimiento de las vulnerabilidades en bases públicas y privadas. Algunos rankings globales[3] le dan, por su parte, una posición aceptable al país mientras que otros[4] le otorgan bajas calificaciones.

En el caso de Córdoba, el relevamiento de la investigadora Marcela Pallero documenta vulnerabilidades casos de bases de datos críticas de Estado[5] de la provincia, de empresas privadas[6] y especialmente de empresas concesionarias de servicios públicos[7].

1 Global Risk Report, World Economic Forum, 2024: https://assets.weforum.org/editor/responsive_large_webp_6D5m57mKtQKA7ugUygfOOd7u6Xy QkOLom4zuae4Xb7A.webp

2 Relevamiento de Ciberincidentes a bases de datos críticas de Argentina, Marcela Pallero: https://time.graphics/es/line/630567

3 Ranking comparativo de NCSI https://ncsi.ega.ee/compare/

4 Indice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

5 Se citan los casos del Poder Judicial de la Provincia de Córdoba en 2022 y de la Municipalidad de Colonia Caroya.

6 Entre las que destacan Globant, Aceitera General Deheza o la Fintech NaranjaX.

7 Se relevan los casos de Caminos de las Sierras, Movipark, Red Bus, etc

Entre las deficiencias y falencias puntuales que aparecieron a lo largo del diagnóstico pueden destacarse los siguientes puntos que atentan contra el desarrollo de la seguridad informática de la provincia:

- La infraestructura y los recursos tecnológicos que dan protección a las bases de datos o redes públicas y privadas (software, hardware, servicios de red, licencias y otros recursos) son limitados.
- La legislación vigente, incluida la de Protección de Datos Personales, no se ajusta a las amenazas actuales.
- El personal especializado en ciberseguridad es escaso o insuficiente.
- Existe una baja adopción de estándares internacionales, como ISO 27001 y NIST.
- Si bien no es uniforme, hay percepciones comunes acerca de la necesidad de evolución en tres ejes fundamentales del ecosistema en Córdoba: el nivel de desarrollo de los proveedores de servicios de ciberseguridad, la calidad de la transformación digital de las industrias privadas y la gestión administrativa del gobierno electrónico por parte del Estado.
- En la mayoría de las organizaciones públicas y privadas faltan políticas de seguridad documentadas y actualizadas.
- No se percibe articulación institucional entre el sector público y el privado.
- Diversos actores y entidades sostienen que el apoyo estatal es insuficiente.

En ese contexto, es interesante resaltar que existe avidez –de parte de los múltiples actores del ecosistema– de participar del diseño de políticas y del abordaje de los problemas estructurales del sector. Coordinar, alinear y ecualizar esos intereses es fundamental para el ecosistema general.

Una de las premisas centrales del Córdoba Cyber Security Conference de 2024[8] puede resumir el consenso de este diagnóstico:

"La falta de políticas y marcos de referencia claros en materia de ciberseguridad deja a las instituciones vulnerables a ataques cada vez más sofisticados y perjudica la confianza en el gobierno y en las instituciones públicas en su conjunto".

8 Cordoba Cybersecurity Conference 2024, co-organizada por la UE SXXI y el CSIRT Cordoba https://21.edu.ar/identidad21/gobierno-y-ciberseguridad-la-urgencia-de-politicaspublicas-y-gestion-de-incidentes

b. Dificultades centrales

INFRAESTRUCTURA Y RECURSOS TECNOLÓGICOS

Son instrumentos que dan protección a las bases de datos y redes públicas y privadas (software, hardware, servicios de red, licencias y otros recursos) tienen limitaciones y dependen de inversiones puntuales. Sin un marco sostenible y sin mejoras a largo plazo, las instituciones, empresas y ciudadanos estarán expuestos a una preocupante tasa de vulnerabilidad.

Este problema se ve exacerbado por las dificultades para adquirir equipamientos de seguridad debido a limitaciones presupuestarias y a la volatilidad económica.

MARCO NORMATIVO

La falta de un marco normativo robusto y actualizado reduce la capacidad de protección del Estado y de las empresas frente a ciberataques. Dicho encuadre no debe ser extremadamente ambicioso – como el de ISO o NIST–, sino adecuado al desarrollo posible en Argentina. La situación se torna más preocupante al comprender que, sin esa actualización, el gobierno provincial no puede ejercer su potestad sancionatoria ante incumplimientos en bases de datos privadas o frente a infracciones de proveedores de servicios del Estado

CULTURA DE CIBERSEGURIDAD

La falta de auditorías y la baja regulación dificultan el desarrollo de una cultura de seguridad en las organizaciones. El bajo nivel de conciencia y de conocimiento por parte de líderes de organizaciones no tecnológicas también debe ser abordado como un desafío en materia de cultura de seguridad de la información.

PERSONAL

La escasez de personal especializado en la materia –los recursos humanos de alto nivel son insuficientes– limita de manera significativa el desarrollo de una cultura de seguridad efectiva, tanto en el sector público como en el privado. Córdoba no podrá erigirse en referente exportador de servicios si no amplía el número de profesionales enfocados en seguridad informática.

c. Obstáculos para los diferentes actores del ecosistema de ciberseguridad

El ecosistema de ciberseguridad en Córdoba está compuesto por diversos actores que juegan roles centrales en el desarrollo y la implementación de políticas y prácticas de seguridad de la información. Estos actores desarrollan sus actividades en los sectores público y privado y en las instituciones educativas y de formación.

La falta de estándares de seguridad transversales y la insuficiente capacitación del personal de las agencias gubernamentales y la administración provincial –responsables de implementar políticas de ciberseguridad y proteger los datos de los ciudadanos– limitan la efectividad de estas instituciones para responder a amenazas cibernéticas.

Asimismo, las empresas que ofrecen servicios de ciberseguridad y las que son usuarias de sistemas digitales son escasas en cantidad y tamaño. Tampoco desarrollaron plenamente sus capacidades, lo que les hace perder terreno frente a competidores internacionales.

En ese plano, ni la atracción de multinacionales que proveen servicios ni el surgimiento de empresas locales –alternativas que se barajaron durante algún tiempo– son posibles sin la generación de talento, más aún en un contexto en el cual los profesionales en seguridad tienen pleno empleo[9].

9 Cordoba Cybersecurity Conference 2024, co-organizada por la UE SXXI y el CSIRT Cordoba https://21.edu.ar/identidad21/gobierno-y-ciberseguridad-la-urgencia-de-politicaspublicas-y-gestion-de-incidentes

Además, como adoptante de innovación en seguridad informática, el sector privado enfrenta problemas de inversión en infraestructura y dificultades para obtener certificaciones en estándares reconocidos (ISO 27001, NIST).

La creación de nuevos puestos de trabajo en el sector tecnológico local está determinada, al mismo tiempo, por los trayectos formativos, en un escenario con múltiples y diversas complejidades. En el plano general, la oferta formativa de ciberseguridad en universidades e instituciones de Córdoba es limitada y poco accesible –por ser pagas y presentar barreras para el ingreso– para buena parte de los interesados.

Respecto de ciertas particularidades de este entorno, para que un egresado pase a un rol operacional es necesaria un recorrido experimental. La naturaleza de las actividades y especialmente, carácter confidencial de las vulnerabilidades con las que se encuentran dichos profesionales hace necesario ese recorrido.

Parece evidente que una mayor inversión en trayectos formativos debe generar una mayor empleabilidad y mejores capacidades de desarrollo para los sectores público y privado

Por último, los ciudadanos, como usuarios finales de los servicios digitales, son actores indirectos pero esenciales en ciberseguridad.

LA CIUDADANÍA NO SIEMPRE ESTÁ PREPARADA PARA PROTEGER SU INFORMACIÓN PERSONAL Y SER UN FACTOR ACTIVO EN LA SEGURIDAD COLECTIVA.

OBSTÁCULOS PARA EL SECTOR PRIVADO EXPORTADOR DE SERVICIOS TECNOLÓGICOS

- **INVERSIÓN Y CERTIFICACIONES**

  La falta de inversión en infraestructura y certificaciones para cumplir con los estándares internacionales y asegurar la calidad de los servicios.

- **COMPETENCIA INTERNACIONAL**

  Las empresas locales deben competir con firmas establecidas en los países destino, lo que dificulta la captación de clientes debido a la reputación y la lealtad que estas empresas ya cultivaron.

- **DESARROLLOS LOCALES**

  La falta de innovación en productos de computación afecta la competitividad.

- **ASPECTOS MACROECONÓMICOS DEL PAÍS**

  Las regulaciones nacionales y los impuestos complican el proceso de exportación, mientras que la volatilidad en los tipos de cambio puede afectar la rentabilidad y competitividad de los servicios.

OBSTÁCULOS PARA LA TRANSFORMACIÓN DIGITAL SEGURA DEL SECTOR PRIVADO

- **SUBESTIMACIÓN DE RIESGOS**

  Muchas empresas avanzan en su transformación sin considerar adecuadamente los riesgos asociados a la digitalización.

- **PRIORIDAD AL TIME TO MARKET**

  Incluso las empresas conscientes de los riesgos priorizan el lanzamiento rápido de productos sobre la implementación de medidas de seguridad.

- **RESISTENCIA AL CAMBIO CULTURAL**

  El rechazo a los cambios culturales internos dificulta la adopción de nuevas tecnologías y prácticas.

- **CONOCIMIENTO Y PRESUPUESTO**

  La falta de conocimiento especializado y de presupuesto limitan la capacidad de implementar soluciones seguras.

- **ENFOQUE EN EL CORE DEL NEGOCIO**

  La situación económica lleva a muchas empresas a enfocarse solo en sus actividades centrales, dejando de lado la transformación digital.

- **RELACIÓN RIESGO-RETORNO**

  No se percibe claramente la relación entre el riesgo y el retorno de la inversión en seguridad digital.

- **FALTA DE OBLIGACIÓN DE INVERSIÓN**

  La ausencia de incentivos regulatorios puede desincentivar a las empresas a priorizar la transformación digital segura.

OBSTÁCULOS DEL SECTOR PÚBLICO Y ESTADO DE LA POLÍTICA PÚBLICA

- **ESTÁNDARES DE SEGURIDAD Y CAPACITACIÓN**

  La falta de estándares transversales de seguridad, que abarquen todas las áreas del sector público, es un obstáculo significativo. Esto se ve agravado por la carencia en capacitación y concientización del personal, ya que la seguridad de la información requiere un compromiso continuo y una cultura organizacional que priorice la protección de datos.

- **SOSTENIMIENTO DE LAS POLÍTICAS PÚBLICAS**

  Fue señalado como una dificultad, la de sostener políticas públicas en el tiempo, algo que resulta difícil inclusive en un escenario en el cual existen gobiernos del mismo signo político.

- **FALTA DE REGULACIÓN APROPIADA**

  Hay consenso sobre la falta de regulación apropiada, especialmente aquella orientada a asegurar cumplimiento (enforcement). Se menciona la necesidad de contar con auditorías, incentivos y penalidades. También se destaca la falta de debates legislativos de calidad y la falta de participación de los investigadores en esos procesos.

- **FALTA DE INVERSIÓN EN TECNOLOGÍA**

  La inversión general en tecnologías de la información y comunicación (TIC) es insuficiente. El presupuesto asignado a estos fines es limitado, lo que dificulta la adquisición de equipos y herramientas necesarias para adecuar los estándares de seguridad y protección de datos. También se identifica la necesidad de acompañamiento a empresas para la formación de agentes de seguridad.

d. Hechos y percepciones

Como fue señalado al principio del documento, las entrevistas y los cuestionarios de la etapa de diagnóstico buscaron capturar la variedad de perspectivas sobre ciberseguridad. De allí se desprendieron algunos hechos y determinadas percepciones que deberían ser tenidas en cuenta, al menos en algunas de sus aristas.

La mayor parte de las organizaciones, tanto públicas como privadas, no están implementando esfuerzos máximos respecto de la ciberseguridad.

- **Una porción considerable de los actores del ecosistema remarcaron que observan bajos niveles de coordinación entre los sectores público y privado.**

- **En todos los planos se mencionó que existen carencias significativas en la formación de especialistas en seguridad de la información.**

- **La expansión de trayectos formativos, y su diagnóstico y ejecución permanente, apareció como una cuestión fundamental para el ecosistema. Fomentar una mayor -y más profunda- oferta educativa luce como decisivo.**

- **El 70% de los actores consultados consideró que el Estado debería proporcionar mayor apoyo en esta materia.**

e. Recursos Humanos

Como se subrayó, la escasez de recursos humanos capacitados es una de las mayores dificultades en materia de ciberseguridad en Córdoba. Al mismo tiempo, la competencia laboral con otros mercados -tanto nacionales como internacionales- hace que sea difícil retener a los mejores talentos.

En ese punto, es importante comprender que los salarios promedio del área son más elevados que los de la media del sector tecnológico. De ahí se derivan dificultades adicionales para crear posiciones internas o inclusive retener esos talentos en organizaciones locales, sean éstas públicas o privadas.

Respecto de la oferta formativa, inclusive si existe una amplia batería de trayectos formativos en diferentes instituciones de la provincia, el abanico de posibilidades posee limitaciones. Uno de los mayores consensos señala que es vital ampliar la oferta formal con carreras de mayor especialización y fortalecer perfiles seguros en trayectos tecnológicos generales. De la misma manera, es coincidente la necesidad de introducir instancias experimentales en esas formaciones, ya que los conocimientos académicos requieren complementariedad con las prácticas en un área muy específica.

Lo que aparece como una debilidad, por una parte, es en realidad una gran oportunidad, por otra. En el debate multisectorial, el tema de la formación y la creación de trayectos es el que mayor interés suscita.

LA CONCLUSIÓN, EN ESTE PLANO, ES QUE **LA DISPONIBILIDAD DE TALENTO ESPECIALIZADO ES EL FACTOR PRINCIPAL PARA ALCANZAR DOS METAS** DE LO MÁS TRASCENDENTES PARA LA PROVINCIA:

EN PRIMER TÉRMINO, PARA MEJORAR LA ADOPCIÓN DE PRÁCTICAS DE CIBERSEGURIDAD QUE TENGAN COMO HORIZONTE LOS MEJORES ESTÁNDARES INTERNACIONALES;

EN SEGUNDO LUGAR, PARA AMPLIAR LA CAPACIDAD DEL SECTOR TECNOLÓGICO DE CÓRDOBA PARA EXPORTAR SERVICIOS ESPECIALIZADOS.

f. Exploración sobre el crecimiento del sector de Ciberseguridad

El diagnóstico tuvo un foco importante en la exploración de la posibilidad de instalar nuevas empresas en Córdoba o de que crezcan las que ya tienen operaciones. Las conclusiones de estos diálogos con actores relevantes tienen que ver con que solo podrán crearse nuevos puestos de trabajo para el sector tecnológico local si se desarrollan capacidades, es decir, trayectos formativos. La cantidad de egresados de alguna de las ofertas académicas y la naturaleza experimental de alguna clase de capacitación son el único factor esencial para la instalación de empresas o crecimiento del ecosistema.

Para pasar de ser egresado de un trayecto formativo en ciberseguridad a tener algún rol operacional hace falta llenar el gap con una formación experimental, no solo por la naturaleza de sus actividades sino por el carácter confidencial de las vulnerabilidades o problemas con lo que se encuentran los profesionales.

Si bien tiene rendimientos decrecientes, mayor inversión en trayectos debería generar mayor empleabilidad y capacidad de que se instale o desarrolle industria local. Y eso debería estar planteado en la hoja de ruta.

g. Evaluación del CSIRT Córdoba

La creación del CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) se destacó de manera positiva para generar conciencia sobre ciberseguridad en Córdoba. Además, el mecanismo multisectorial con el que se constituyó el CSIRT goza de amplia legitimidad y es observado como un acierto.

En relación a las iniciativas educativas y eventos generados por el CSIRT, estos fueron bien recibidos, aunque muchos de los encuestados señalaron que estas iniciativas deben ser más frecuentes y económicamente accesibles.

Aun así, se valoró al CSIRT como punto de encuentro, ya que algunos encuestados consideraron que sirvió como un nexo valioso entre diferentes actores del sector, facilitando la comunicación y el intercambio de información sobre incidentes y mejores prácticas.

Sin embargo, un número significativo de encuestados subrayó una **falta de articulación y proyección real en las acciones del CSIRT.** Se mencionó que las iniciativas parecen por momentos inactivas o espasmódicas. Diferentes actores del sector expresaron que el CSIRT no parece tema prioritario en la agenda política de la provincia y mencionaron la falta de recursos financieros y humanos para implementar políticas efectivas.

Entre las falencias también se mencionó que aún no se perciben resultados concretos o evidentes de las acciones del CSIRT, por lo que se sugirió establecer metas claras y acciones concretas para poder medir y dimensionar el impacto positivo del CSIRT.

- **UTILIZACIÓN DEL CSIRT POR PARTE DE LA COMUNIDAD Y CONFIANZA:**

Un factor crítico del éxito del CSIRT es la utilización de alguna de sus funciones por parte de la comunidad. En el caso de las vulnerabilidades que se producen en relación al Estado provincial, la situación es preocupante de cara al CSIRT.

Casi ninguna de las dependencias estatales u organismos descentralizados ha implementado políticas “estado del arte” frente a incidentes de seguridad, documentación y comunicación pública de los mismos. El Estado provincial no solamente no utiliza los servicios del CSIRT que creó y lidera, sino que, con este proceder, desalienta el uso por parte de la comunidad a la hora de recibir vulnerabilidades.

h. Hallazgos relevantes sobre prácticas de ciberseguridad

Si bien el diagnóstico no tiene pretensiones académicas, hay algunas cifras interesantes de observar. Debe tenerse en cuenta, además, que se trata de un grupo de líderes y que, por ello, los datos consignados no deben ser extrapolados a la totalidad de las entidades provinciales:

- 48% de los encuestados afirmó tener políticas documentadas, aunque muchos de ellos indicaron que éstas no son revisadas con regularidad o están desactualizadas.
- 60% indicó que sus políticas son revisadas anualmente o cada dos años.
- 25% señaló que sus políticas son revisadas con menor frecuencia o nunca.
- 38% de las organizaciones cuentan con un canal o método documentado para el reporte de vulnerabilidades por agentes externos.

Tabla 1: Hallazgos sobre prácticas de ciberseguridad

Sector	Políticas documentadas	Frecuencia de revisión	Estándares seguidos
Privado	Sí (en su mayoría documentadas)	Anualmente	Algunos siguen GDPR / ISO 27001
Público	Sí (pero no siempre actualizadas)	Con menor frecuencia/nunca	Algunos siguen ISO 27001
Académico	Sí (pero no siempre actualizadas)	Con menor frecuencia/nunca	Poca referencia a estándares

Fuente: entrevistas a líderes cordobeses.

- Sector privado: tiende a tener más políticas documentadas.
- Sector público: aunque hay reconocimiento sobre la importancia de tener políticas, muchas no están documentadas o son ineficaces.

i. Conclusiones

Es posible identificar las necesidades para desarrollar políticas adaptadas a las realidades locales y orientadas a fortalecer la competitividad de Córdoba en seguridad de la información. Las **deficiencias y desafíos** se clasifican de la siguiente manera:

INFRAESTRUCTURA Y TECNOLOGÍA

La infraestructura de ciberseguridad de la provincia presenta deficiencias. Apenas un tercio de las organizaciones cuenta con certificaciones avanzadas y las inversiones en tecnología son insuficientes para cubrir las necesidades actuales.

RECURSOS HUMANOS

Es el factor fundamental, tanto para para el posible desarrollo del sector como para hacer frente a las dificultades mencionadas.

REGULACIÓN Y POLÍTICAS

La provincia carece de un marco normativo robusto y actualizado para la seguridad de la información. La falta de potestad sancionatoria impide que el sector público y el privado implementen prácticas de seguridad efectivas.

PROTECCIÓN DE DATOS PERSONALES

Aunque Argentina cuenta con una legislación en protección de datos personales que cuenta con algunas limitaciones, Córdoba no ha optado por adherir a estas normativas. En el universo de los encuestados, solo el 15% de las organizaciones cumple con estándares avanzados de protección de datos.

3. HOJA DE RUTA: RECOMENDACIONES PARA FORTALECER LA CIBERSEGURIDAD EN LA PROVINCIA DE CÓRDOBA

a. Consideraciones generales

La provincia de Córdoba enfrenta importantes desafíos en ciberseguridad, que requieren una intervención estratégica y coordinada. La Mesa Provincial de Ciberseguridad se propone el diseño concertado de una política pública con participación del sector privado y la academia. La misma tiene **cuatro objetivos primordiales:**

1. AUMENTAR LA PRODUCTIVIDAD Y EMPLEABILIDAD DEL SECTOR TECNOLÓGICO EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN Y SUS DIFERENTES ÁREAS DE INCUMBENCIA.

2. REFORZAR EL NIVEL GENERAL DE LA SEGURIDAD DIGITAL DE LA PROVINCIA DE CÓRDOBA.

3. MEJORAR LA RESILIENCIA INSTITUCIONAL Y LA PROTECCIÓN DE ENTIDADES PÚBLICAS Y PRIVADAS

4. INCREMENTAR LA CONCIENCIA CIUDADANA GENERAL EN LA MATERIA.

b. Propuesta institucional: Consejo Provincial de Políticas Digitales

El diagnóstico, la evaluación de los diferentes desafíos de la Mesa Provincial y los consensos que se han relevado con los interlocutores, además de las experiencias comparadas que se relevaron han inspirado la propuesta de un diseño institucional que contemple:

- Institución pública con participación del sector privado y la academia.
- Elaboración de políticas de ciberseguridad, inteligencia artificial y otros temas emergentes.

Los aspectos específicos del diseño institucional serán formulados de manera conjunta por las Mesas Provinciales de Ciberseguridad e Inteligencia Artificial atendiendo a los ejemplos y alternativas referidas en la sección ¨experiencias comparadas¨ de este estudio.

ESTRUCTURA

- Un organismo público enfocado a los dos temas principales de políticas digitales: ciberseguridad e Inteligencia Artificial.
- Un directorio multisectorial, con participación del sector privado y universidades.
- Fondos públicos, provenientes de inversiones e ingresos recursivos del ecosistema.
- El Consejo Provincial conduce la política pública, canaliza la inversión. No es de economía mixta.

c. Oportunidad

El diagnóstico da cuenta de limitaciones, obstáculos y desafíos estructurales que resultan insoslayables para una hoja de ruta del sector. Sin embargo, también ilustra acerca de una oportunidad singular en el ecosistema de ciberseguridad de la provincia, derivado del compromiso de un importante número de sus actores con el problema general:

CONSENSO ENTRE ACTORES DE DIFERENTES STAKEHOLDERS

Resulta positiva la coincidencia de los actores en un diagnóstico, más aún por el consenso sobre la situación acuciante respecto del crecimiento de delitos informáticos ya descrita en el diagnóstico.

PODER SANCIONATORIO DEL ESTADO

El consenso referido anteriormente se extiende a la necesidad de aumentar el poder sancionatorio del Estado en materia de seguridad y protección de datos. En la hoja de ruta se exploran oportunidades para materializar esta potestad, recaudar fondos y aumentar la creación de capacidades tanto en trayectos formativos como en proyectos de servicios experimentales.

EXTERNALIDADES DEL ECOSISTEMA PROVINCIAL

El ecosistema de Córdoba cuenta con individuos que, aún si tienen trabajo en organizaciones que forman parte de diferentes grupos de interés, están preocupados y son capaces de pensar las políticas públicas macro desde su lugar de origen. Estos actores desean participar en la resolución de problemas generales o en el desarrollo de diversas iniciativas, más allá de sus intereses individuales.

PERCEPCIONES POSITIVAS

La percepción positiva de la estructura multisectorial del CSIRT, creado en 2022, ofrece un antecedente que puede inspirar la hoja de ruta provincial.

d. Principios compartidos

Las acciones propuestas tendrán como hilo conductor una serie de proyectos con las siguientes características:

- Diseño y ejecución de la política pública con participación de todos los sectores, liderazgo del estado.
- Eficacia en la inversión pública inicial, con foco en la posibilidad de generar flujos recursivos de ingresos.
- Búsqueda de sustentabilidad y de impacto circular (flujos de fondo y recurrencia).
- Evaluaciones de impacto para orientar la profundización de la inversión sostenida.

e. Acciones propuestas

Los hallazgos del diagnóstico sugieren:

ACCIONES INMEDIATAS

Por un lado, aumentar la inversión en infraestructura de ciberseguridad; por el otro, establecer un marco normativo actualizado.

PROYECTOS A MEDIANO Y LARGO PLAZO

Generar programas de capacitación continua y campañas de concientización, así como asegurar la sostenibilidad de estas políticas en el tiempo.

f. Proyectos e impacto presupuestario

1. Fortalecimiento del CSIRT y su rol en la comunidad

Impacto presupuestario: requiere de una inversión pública marginal, por cuanto el Instituto Provincial ya dispondrá de actualización en infraestructura. Resta disponer de personal y capacidades de gestión para coordinación y management.

→ 1.1. Ampliar la participación del sector privado en el CSIRT

OBJETIVO

Involucrar más actores del sector privado para una respuesta coordinada a incidentes de ciberseguridad sin necesidad de modificar su estructura de gobernanza.

ESTRATEGIA

Invitar a empresas privadas y startups a formar parte del CSIRT, implementando comisiones de trabajo que permitan a cada sector expresar sus necesidades y colaborar en la seguridad conjunta.

→ 1.2. Crear un sistema de alertas y canalización de incidentes

OBJETIVO

Desarrollar un servicio de alertas que permita la rápida comunicación y respuesta a incidentes cibernéticos.

ESTRATEGIA

Establecer un sistema de alertas tempranas, manteniendo el anonimato de los incidentes reportados, con el fin de disipar el temor a la pérdida de reputación. Este sistema debe ser accesible tanto a instituciones públicas como privadas, y debe operar de acuerdo con altos estándares de privacidad y seguridad.

→ 1.3. Generar confianza a través de servicios

OBJETIVO

Crear un esquema de servicios de alertas avanzadas que permita generar ingresos y aumentar la confianza en el CSIRT.

ESTRATEGIA

Ofrecer servicios premium para aquellos actores que requieran apoyo técnico y personalizado en ciberseguridad. Los ingresos generados pueden ser reinvertidos en el desarrollo de nuevas capacidades y en la sostenibilidad del CSIRT.

2. Sensibilización, concientización ciudadana y empleos

→ 2.1 Impulsar programas de concientización ciudadana

OBJETIVO

Elevar el nivel de conciencia entre los ciudadanos y los actores locales.

ESTRATEGIA

Articular con actores de la comunidad que posean la inclusión digital en su agenda, poniendo a disposición de esos actores (agencias gubernamentales, sociedad civil, sistema financiero, etc) la información generada por el CSIRT y por sus miembros, así como por CSIRT Américas.

→ 2.2 Impulsar programas de empleo

3. Creación de capacidades y trayectos formativos

Impacto presupuestario: Se requieren algunas capacidades de coordinación y comunicación para ejecutar esta clase de programas con articulación de otros actores (ej: Cisco, ACC, Fundaciones, etc).

→ 3.1. Crear una comisión sobre trayectos formativos en ciberseguridad

OBJETIVO

Desarrollar un debate continuo acerca de la estrategia de formación en ciberseguridad que impulse el desarrollo de trayectos formales, que detecte oportunidades específicas en el desarrollo perfiles profesionales. El foco del debate de la comisión deberá incluir no solo la formación sino la retención de talentos en el ecosistema.

ESTRATEGIA

Crear una comisión especializada que reflexione acerca de las necesidades de formación y proponga trayectos formativos u otras estrategias de generación de capacidades en ciberseguridad, incluyendo diplomaturas, cursos técnicos, certificaciones para profesionales del sector, así como también acciones de menor formalización. Es imprescindible trabajar de manera conjunta con instituciones educativas locales y debe considerarse el financiamiento estratégico de dichos trayectos.

→ 3.2. Capacitación continua y reciclaje profesional

OBJETIVO

Mantener actualizados a los profesionales de TI y ciberseguridad en las nuevas tendencias y amenazas emergentes.

ESTRATEGIA

Ofrecer capacitaciones regulares y módulos de actualización que cubran temas como protección de datos, gestión de incidentes y análisis de malware. La capacitación continua debería convertirse en un requisito para los empleados en sectores críticos.

4. Proyectos de creación de capacidades y servicios best effort de ciberseguridad

Impacto presupuestario: se requiere de inversión semilla y se prevé la posibilidad de tornar autosustentable cada servicio aún con costos de coordinación y management.

En línea con la oportunidad descrita al inicio de este documento, se pretende crear una serie de servicios experimentales en ciberseguridad.

La característica diferencial de estos proyectos tiene su origen en la avidez por parte de actores “senior” del ecosistema para supervisar la ejecución de los mismos.

La propuesta de ofrecer servicios desde una política pública concertada no busca que los mismos compitan con el mercado. Por el contrario, el foco central de los proyectos que se enuncian a continuación es la creación de capacidades en áreas que producen un complemento con los trayectos formales, agregando la diferencia con la adquisición de experiencia profesional.

De manera colateral, se prevé un impacto de los proyectos en el ecosistema, ya que los servicios están destinados a ser consumidos por instituciones que no pueden acceder a los mismos en el mercado ni tampoco desarrollarlos internamente en sus estructuras.

La participación de estudiantes en proyectos tiene una característica central. El nivel de los servicios no tendrá las garantías que ofrecen los profesionales establecidos en el mercado, sino que será “de mejor esfuerzo”. Si bien en algunos casos se contempla el cobro de un monto por la provisión de los servicios, se propone que el mismo se devengue dependiendo de la satisfacción.

→ 4.1 Proyectos de creación de capacidades en forma de servicios “best effort”

- ***Phishing Ético***

ESTRATEGIA

El diseño de simulaciones de phishing mediante técnicas de Ingeniería Social para identificar usuarios propensos a ser engañados en las organizaciones. con el objetivo de entrenarlos y concientizarlos, evitando que se conviertan en el punto de entrada para incidentes reales.

- ***Intrusion Detection con Suricata***

ESTRATEGIA

El trabajo consiste en configurar la infraestructura existente en la organización con www.suricata.io. El servicio se limita a ID sin dejar en manos de un proyecto “de mejor esfuerzo” a otras tareas más complejas como la IP, intrusion prevention.

- ***Pen Testing***

ESTRATEGIA

Evaluar la efectividad de los sistemas de seguridad a través de simulaciones de ataques controladas mediante un programa de pruebas periódicas de penetración.
Si bien el pentesting tiene por objetivo detectar vulnerabilidades antes de que sean explotadas por atacantes, el proyecto propone ofrecérselo ainstituciones y empresas que no pueden adquirir este servicio en el mercado.
El proyecto tiene como resultado esperado un aumento de las capacidades de dichas empresas, al tiempo que se fortalecen las capacidades de los participantes y se genera mayor empleabilidad.

- ***App Sec con devsecops***

ESTRATEGIA

DevSecOps es la práctica de integrar las pruebas de seguridad en cada etapa del proceso de desarrollo de software. Incluye herramientas y procesos que fomentan la colaboración entre los desarrolladores, los especialistas en seguridad y los equipos de operaciones para crear un software que sea eficiente y seguro.

Debe destacarse que esta clase de servicios no se extienden a la totalidad del abanico de network security ni de app security.

→ 4.2. Proyecto sobre Indicadores de compromiso para startups

OBJETIVO

Desarrollar métricas que evalúen el compromiso y desempeño de startups en ciberseguridad con supervisión senior de CISOs.

ESTRATEGIA

Implementar un sistema de indicadores de compromiso que mida el impacto de las startups en la comunidad y en el desarrollo de prácticas seguras. Este sistema debería ser administrado por una entidad que colabore con el sector fintech para obtener información fiable y fomentar el rendimiento de las startups.

5. Desarrollo y actualización normativa en ciberseguridad

Impacto presupuestario: no se prevé impacto para el proyecto, más allá de las acciones de coordinación y management del Instituto.

→ 5.1. Crear un marco regulatorio de seguridad integral

OBJETIVO

Desarrollar y actualizar un marco regulador claro y específico en ciberseguridad que abarque tanto al sector público como al privado y que sea adecuado a las posibilidades del ecosistema provincial. Si bien se busca promover el cumplimiento de los estándares internacionales (ISO 27001, NIST), resulta fundamental mantener conciencia acerca de las limitaciones estructurales y posibilidades de los actores de la provincia.

ESTRATEGIA

Crear un comité de regulación compuesto por expertos en derecho digital, ciberseguridad y tecnología. Este comité debe definir las normas para en la región, adaptándolas a las necesidades locales y a los avances en amenazas cibernéticas.

→ 5.2. Evaluar la pertinencia y conveniencia de implementar auditorías y mecanismos de cumplimiento, así como las de introducir sanciones e incentivos económicos.

OBJETIVO

Evaluar la pertinencia de estas estrategias y la implementación de incentivos, sanciones o mecanismos de cumplimiento.

ESTRATEGIA

crear una comisión que mantenga en contacto a referentes de la materia con tomadores de decisiones de las organizaciones públicas y privadas a fin de explorar la posible eficacia de estas decisiones antes de implementarlas.

6. Ejecución de la potestad sancionatoria provincial

→ 6.1. Dotar al Consejo Provincial de Políticas Digitales de potestad sancionatoria en materia de ciberseguridad.

OBJETIVOS

- Alentar el cumplimiento de estándares de ciberseguridad y
- Recaudar fondos que permitan inyectar recursos a la creación de capacidades.

ESTRATEGIA

Crear una comisión en el marco del Consejo Provincial.

→ 6.2 Exploración de alternativas para adhesión al marco de Protección de Datos

OBJETIVO

Hacer cumplir el régimen de protección de datos personales.

ESTRATEGIA

Se puede delegar en la autoridad federal la potestad sancionatoria o crear una provincial. La Directora de la AAIP ha manifestado su disposición a tener reuniones con la Mesa Provincial a fines de disponer de las diferentes alternativas.

→ 6.3. Políticas de Protección de Datos en organismos públicos.

OBJETIVO

Elevar el nivel de Protección de Datos en el Estado.

ESTRATEGIA

Dictar, publicar y ejecutar una política de Protección de Datos en cada ministerio o secretaría, inspirada en el CIDI.

4. MAPA DE OPORTUNIDADES Y RECOMENDACIONES INTERNACIONALES APLICABLES A LA SEGURIDAD DE LA INFORMACIÓN EN LA PROVINCIA

a. Introducción

El presente documento procura funcionar como un insumo para los diagnósticos y hoja de ruta que se propondrá adoptar por la Mesa Provincial de Ciberseguridad de la Provincia de Córdoba. Se trata de una revisión exhaustiva del "estado del arte" en recomendaciones y buenas prácticas internacionales y políticas públicas de inteligencia artificial.

La información aquí presentada pretende relevar los problemas, conocimientos o dilemas que existen a nivel global e internacional sobre políticas públicas de seguridad de la información. El objetivo, luego de listar y ponderar las principales recomendaciones emitidas por organismos internacionales, expertos y organizaciones líderes en cada uno de estos temas es el de servir como apoyo para la Mesa Provincial resaltando aspectos claves que pueden ser aplicados para orientar el desarrollo de políticas provinciales.

Las fuentes ofrecen un conjunto de recomendaciones para fortalecer la ciberseguridad y la protección de datos, especialmente en el contexto del rápido desarrollo de la inteligencia artificial (IA).

b. Acerca del desarrollo de CSIRTs

Es materia de Centros de Respuesta a Incidentes de Seguridad Informática debe tenerse en cuenta que Córdoba cuenta con un CSIRT oficial[10] establecido y que el mismo conforma la red de CSIRT Américas.

10 El CSIRT Córdoba cuenta con un mecanismo de gobernanza multisectorial: https://csirtcordoba.ar/

Algunos consejos vertidos en la Guía Práctica para CSIRTs[11] de CSIRT Américas, pueden ser de utilidad para el actual estadío de evolución de esta institución.

ASEGURAR LA CONTINUIDAD DE UN CSIRT:

En la sección de asegurar la continuidad se hacen recomendaciones sobre:

- Servicios: "*Hay coincidencia en que en que un factor que puede contribuir al éxito de un CSIRT es ¨comenzar en pequeño; construir a partir de un plan sencillo, con acciones o servicios concretos, y realizar evaluaciones periódicas que permitan conocer los avances y, si fuera el caso, proponer cambios"*.
- Talento Humano: "*es recomendable iniciar con el personal mínimo necesario para operar los servicios mencionados"*. Según la ENISA[12], el número promedio de personal trabajando en un equipo pequeño es de 3 a 7.
- Rol en la sociedad: Se plantea que un CSIRT no solamente se debe enfocar en responder a incidentes cibernéticos cuando una institución lo requiere, sino que un CSIRT juega un rol fundamental en la coordinación de ciberseguridad en eventos de impacto social y económico de un país, razón por la que deberá desarrollar confianza más allá de los decretos y acuerdos existentes. Es por medio de la confianza y la generación de valor que un CSIRT puede ubicarse del lado del afectado y ayudarlo, y no en su contra.
- Sostenibilidad del Modelo de Negocio: Una buena práctica al momento de crear un CSIRT es formarlo como un modelo de negocio ajustado a las oportunidades y limitaciones cambiantes, teniendo presente que no necesariamente va a generar rentabilidad monetaria, pero sí será un diferenciador al contribuir a tener sistemas más seguros, mayor confianza de la ciudadanía y minimización de impactos de gravedad ante incidentes cibernéticos. La propia guía aporta un CANVA para asistir al desarrollo de una propuesta de valor para los CSIRTs.
- El CSIRT del futuro: La guía propone un listado de 14 roles que los CSIRTs deben cumplir en el futuro.

11 Guía Práctica de CSIRT Américas, 2023: https://shares.csirtamericas.org/s/AqfMc7XYBmcRpZM/download/GuiaCSIRT%202023%20ESP%20V6.pdf

12 Red Europea de CSIRTs:https://www.enisa.europa.eu/topics/eu-incident-responseand-cyber-crisis-management

Por otra parte, la guía diseñada por el Banco Mundial[13] para países en desarrollo ofrece a los responsables de las políticas de los países en desarrollo un marco para establecer y mejorar los equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés).

Entre las recomendaciones prácticas que ofrece se incluyen las estimaciones de costos y la dotación de personal que se requiere para montar un CSIRT. Aborda el tema clave de la importancia de la cooperación internacional y la utilización de herramientas de código abierto para maximizar la eficiencia y minimizar los costos.

El documento del Banco Mundial tiene por objeto fomentar la inversión en los CSIRT, demostrando su importante rentabilidad de la inversión en comparación con las importantes pérdidas económicas causadas por los incidentes de ciberseguridad.

SOBRE PRECIOS Y COSTOS

El precio de establecer y mantener un CSIRT varía mucho según el tamaño y el nivel de ingresos de un país, así como el diseño, el contexto y las funciones del CSIRT. Por lo general, los costos del CSIRT se pueden dividir en dos categorías:

GASTOS DE CAPITAL (CAPEX)

Son las inversiones iniciales necesarias para establecer el CSIRT, como una evaluación previa, compras de software y hardware (servidores, conmutadores, cortafuegos, computadoras portátiles, impresoras, copias de seguridad, etc.), contratación de consultores para la capacitación y mejora de las habilidades del personal y financiamiento de activos fijos, como la compra de una oficina.

GASTOS OPERATIVOS (OPEX)

Cubren los costos continuos del CSIRT, como el salario del personal, las licencias de software, la capacitación, las cuotas de membresía, el mantenimiento de la oficina, las comunicaciones y los eventos.

13 Guia del Banco Mundial para CSIRTs en países en desarrollo, 2024. https://documents1.worldbank.org/curated/en/099060824112023473/pdf/P177852158c0330d51 a71613967bd98edc4.pdf

La Figura 6 del documento fuente proporciona una estimación amplia de los costos asociados con la creación de un CSIRT nacional con tres ofertas de servicios diferentes. Los costos estimados proporcionados se basan en un modelo operativo muy austero, por lo que los costos reales podrían ser más altos.

Figure 6. Illustrative structures and estimated costs for national CSIRTs at different maturity levels

	Minimal service offering[7]	Average service offering	Key factors
Staff	5-6	12-20	30-50
Structure	• 1 x Manager • 2-3 x Incident Handlers • 1-2 x Multifunctional Roles (Communications; IT support; Project Management, Policy Analysis)	• 1 x Manager • 1 x Deputy Manager • 8 x Incident Handlers • 1-3 x Analysts • 1-3 x IT support • 1-3 x Communications & Liaison	• 1 x Director • 1 x Deputy Director • 3-4 x Unit Managers • 12-14 x Incident Handlers • 3-6 x Analysts • 3-6 x IT support • 3-6 x Communications & Liaison • 3-6 x Admin & Support
Initial investments (capex)	$500,000 - 700,000 +	$700,000 - 1.5 million +	$1.5 - 3 million +
Annual operating costs (opex)	Up to $500,000	$500,000 - 1 million +	$1 - 2 million +

Source: World Bank

A su vez, existe una sección con estrategias para reducir los costos de los CSIRT. Se destaca una perspectiva sobre el error común que se comete en países de bajos ingresos: concentrarse solo en el CAPEX e ignorar la necesidad de financiar el OPEX, en particular cuando se agota la financiación inicial de la asistencia internacional para el desarrollo.

La inversión inicial en la creación de un CSIRT es una decisión financiera inteligente porque puede producir importantes retornos económicos en comparación con los costos proyectados de los incidentes de ciberseguridad, que pueden alcanzar hasta el 3% del PIB.

La figura 3 tiene ejemplos de posibles modelos de fondeo para CSIRTs.

Table 3. Examples of potential funding models for CSIRTs

Funding mechanism	Benefits	Risks	Key factors	Example
Earmarked government budget	Can be more stable and enable long-term planning, if government support is guaranteed. Can be necessary in the first stages of CSIRT establishment when the value proposition still needs to be demonstrated.	Can provide less incentives for the CSIRT to evolve and effectively respond to a wider membership base. In some cases, can be more dependent on changes in political leadership or governmental restructuration.	This model requires long-term governmental support and is likely to be successful in politically stable countries where cybersecurity is recognized as a policy priority (e.g., through a dedicated cybersecurity agency)	In Ghana, the national CSIRT is hosted within the national Cyber Security Authority and benefits from an earmarked
Membership fees	Can provide more incentives to closely align CSIRT service offering and activities with the needs of the membership base. Can be more flexible and allow for progressive growth in case members decide to allocate more resources to the CSIRT.	Can be more difficult to implement in the first stages of CSIRT establishment, as the value proposition may still be unclear to potential members. Can be less stable and limit long-term financial planning, particularly if funding is dependent upon one or two key members.	This model requires strong engagement from the private sector and is likely to be successful where co-operation mechanisms (including between competitors within a sector) are already in place.	The Nordic Financial CERT brings together financial institutions from five Nordic countries in Europe.
Hybrid or blended	Can provide more flexibility for budget allocation and growth. Can limit dependency on members and political leadership.	Can lead to conflicts of interests or confusion among stakeholders. In some cases, can compete with services that could be offered by the private sector.	This model requires a clear delineation of services offered freely and services offered for a fee (e.g., SOC services).	
Public-Private Partnerships (PPPs)	Can facilitate and accelerate knowledge transfer and skills development. Can reduce the need for initial public funding. Can enable the implementation of private sector good practices.	Can lead to conflicts of interests or confusion among stakeholders. Can result in difficult situations if sensitive, national security information is involved. Can result in partner lock-in or be subject to geopolitical constraints if the PPP involves a foreign company.	TTo be successful, PPPs for CSIRTs require well-designed articles of incorporation and / or Service Level Agreements (SLAs). Establishing trust between the retained company and the stakeholders is also key.	The national CSIRT of Togo (see Box 2).

Source: World Bank

c. Análisis integral sobre capacidades de ciberseguridad: el Modelo de Madurez de Oxford sobre Capacidades

El Modelo de Madurez de Capacidades de Ciberseguridad[14] (CMM) proporciona un marco integral para evaluar y mejorar la capacidad de ciberseguridad de un país. Al identificar las fortalezas y debilidades en cada dimensión, factor y aspecto, los países pueden desarrollar estrategias específicas para fortalecer su postura de ciberseguridad.

PROPÓSITO DEL CMM:

- Revisar la capacidad de ciberseguridad de un país.
- Ayudar a los países a identificar fortalezas y debilidades en su capacidad de ciberseguridad.
- Proporcionar una hoja de ruta para mejorar la capacidad de ciberseguridad.

ESTRUCTURA DEL CMM:

- Dimensiones: abarcan la amplitud de la capacidad nacional de ciberseguridad. Las cinco dimensiones son:

  ➢ Desarrollo de políticas y estrategias de ciberseguridad.
  ➢ Fomento de una cultura de ciberseguridad responsable en la sociedad.
  ➢ Desarrollo de conocimientos y capacidades de ciberseguridad.
  ➢ Creación de marcos legales y regulatorios eficaces.
  ➢ Control de riesgos mediante normas y tecnologías.

Cada Dimensión se compone de varios factores que describen lo que significa poseer capacidad de ciberseguridad. Estos Factores se miden en términos de Etapas de madurez, que van desde la etapa inicial hasta la etapa dinámica. La mayoría de los factores se dividen en aspectos para facilitar la comprensión y la medición.

14 Modelo de Madurez de capacidades de ciberseguridad de Oxford, 2021: https://gcscc.ox.ac.uk/the-cmm

Fuente: Modelo de Madurez de capacidades de ciberseguridad de Oxford

- Etapas de madurez: definen el grado de progreso de un país en relación con un determinado Factor o Aspecto de la capacidad de ciberseguridad. Las cinco etapas son:
  - ➢ Inicial: Primeros pasos en el desarrollo de la capacidad.
  - ➢ Formativa: Se están estableciendo procesos y estructuras básicas.
  - ➢ Establecida: Se han implementado procesos y estructuras sólidas
  - ➢ Estratégica: La capacidad se gestiona de forma estratégica y proactiva.
  - ➢ Dinámica: La capacidad es robusta y se adapta constantemente a las nuevas amenazas.

Cada Etapa se caracteriza por un conjunto de Indicadores que un país debe cumplir para alcanzarla.

- Indicadores: representan los componentes básicos del CMM. Describen las acciones, pasos o elementos que indican un nivel específico de madurez. *"Para haber alcanzado con éxito una etapa de madurez, un país tendrá que convencerse de que puede evidenciar cada uno de los Indicadores"*

La mayoría de los Indicadores son binarios: el país puede demostrar que cumple con los criterios del indicador o no puede proporcionar dicha evidencia.

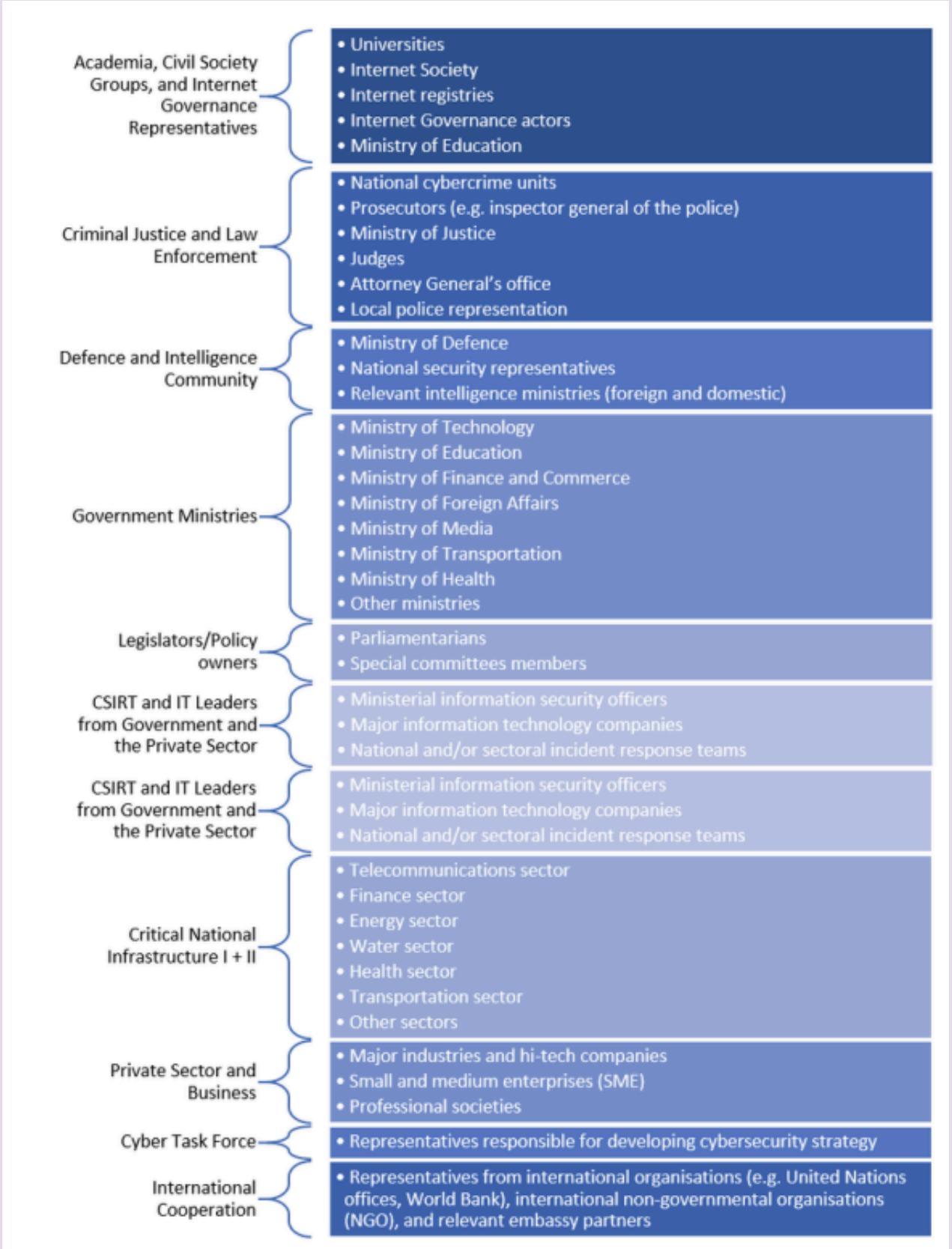
El CMM es un modelo en constante desarrollo y evolución. Esto implica que se actualiza y mejora con el tiempo para reflejar las nuevas tendencias y desafíos en el panorama de la ciberseguridad.

El modelo de madurez CMM analiza diferentes actores del ecosistema de ciberseguridad de un país y evalúa dimensiones en cada uno de ellos. Los actores son:

- Academia, sociedad civil y representantes de gobernanza de internet.
- Cortes de justicia y policías abocados al ciberdelito.
- Comunidad de defensa e inteligencia.
- Ministerios de gobierno.
- Legisladores y desarrolladores de política pública.
- Líderes técnicos y de CSIRTs.
- Infraestructura crítica.
- Sector privado.
- Cyber task force.
- Cooperación Internacional.

El gráfico que describe el proceso de revisión[15] del CMM destaca las diferentes dimensiones en las que evalúa a los actores antes descriptos:

15 Proceso de revisión del Modelo de Madurez de Oxford: https://gcscc.ox.ac.uk/cmmreview-process


Academia, Civil Society Groups, and Internet Governance Representatives
• Universities
• Internet Society
• Internet registries
• Internet Governance actors
• Ministry of Education
Criminal Justice and Law Enforcement
• National cybercrime units
• Prosecutors (e.g. inspector general of the police)
• Ministry of Justice
• Judges
• Attorney General's office
• Local police representation
Defence and Intelligence Community
• Ministry of Defence
• National security representatives
• Relevant intelligence ministries (foreign and domestic)
Government Ministries
• Ministry of Technology
• Ministry of Education
• Ministry of Finance and Commerce
• Ministry of Foreign Affairs
• Ministry of Media
• Ministry of Transportation
• Ministry of Health
• Other ministries
Legislators/Policy owners
• Parliamentarians
• Special committees members
CSIRT and IT Leaders from Government and the Private Sector
• Ministerial information security officers
• Major information technology companies
• National and/or sectoral incident response teams
CSIRT and IT Leaders from Government and the Private Sector
• Ministerial information security officers
• Major information technology companies
• National and/or sectoral incident response teams
Critical National Infrastructure I + II
• Telecommunications sector
• Finance sector
• Energy sector
• Water sector
• Health sector
• Transportation sector
• Other sectors
Private Sector and Business
• Major industries and hi-tech companies
• Small and medium enterprises (SME)
• Professional societies
Cyber Task Force
• Representatives responsible for developing cybersecurity strategy
International Cooperation
• Representatives from international organisations (e.g. United Nations offices, World Bank), international non-governmental organisations (NGO), and relevant embassy partners

d. Córdoba Cybersecurity Conference 2024: Recomendaciones de política pública y Protección de Datos Personales

La conferencia de Ciberseguridad celebrada en Junio de 2024 en la Universidad Empresarial Siglo XXI co-organizada por el CSIRT Córdoba[16] arrojó un documento con recomendaciones sobre políticas públicas.

El mismo, ya ha sido oportunamente citado en el diagnóstico principal y en la hoja de ruta específicamente en materia de actualización del régimen de Protección de Datos Personales y con referencia específica al CSIRT.

Sin embargo, resulta pertinente destacar otras recomendaciones generales que se destacan en el siguiente resumen:

IDENTIFICACIÓN DE RIESGOS

Se identificaron los siguientes riesgos prioritarios desde las perspectivas privadas, estatales y de los ciudadanos:

- Protección de Datos Personales: La falta de políticas robustas para proteger los datos personales de los ciudadanos.
- Regulación de Amenazas Emergentes: Ausencia de legislación específica para abordar amenazas cibernéticas emergentes que no están contempladas en el código penal o contravencional actual.
- Coordinación y Respuesta: Necesidad de fortalecer las capacidades del CSIRT existente y ampliar sus funciones para realizar acciones concretas y efectivas.

16 Cordoba Cybersecurity Conference 2024: https://contenidos.21.edu.ar/microsites/cordoba-security-conference-2024/programa.html

SUGERENCIAS DE POLÍTICAS PÚBLICAS

- Desarrollo de una Estrategia Integral de Protección de Datos:

  ➢ Ley de Protección de Datos Personales: Adaptar y actualizar la legislación existente para alinearse con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.
  ➢ Autoridad de Protección de Datos: Crear una autoridad independiente encargada de supervisar y hacer cumplir las leyes de protección de datos, similar a la Agencia Española de Protección de Datos (AEPD)

- Legislación para Amenazas Emergentes:

  ➢ Marco Legal para internet de las cosas (IoT) y Dispositivos Conectados: Desarrollar regulaciones específicas para la seguridad de dispositivos IoT, inspirándose en la legislación de ciberseguridad con marcos internacionales como la de California
  ➢ Ciberseguridad en Infraestructuras Críticas: Implementar normativas que obliguen a las infraestructuras críticas a seguir estándares de ciberseguridad, tomando como referencia el NIST Cybersecurity Framework de Estados Unidos.
  ➢ Actualización del Código Penal: Incluir delitos cibernéticos específicos que sean aplicados a diferentes modalidades que han quedado obsoletas o que todavía se aplican por analogía dentro del código penal a fin de cubrir las amenazas actuales no contempladas.

- Fortalecimiento y Ampliación del CSIRT:

  ➢ Recursos y Capacitación: Asignar más recursos al CSIRT y proporcionar capacitación continua a sus miembros para enfrentar las amenazas más avanzadas.
  ➢ Colaboración Público-Privada y Academia: Fomentar la colaboración entre el CSIRT, empresas privadas y academia para compartir información, mejores prácticas en ciberseguridad y necesidades que permitan generar nuevos entrenamientos, capacidades para contrarrestar flagelos que sufren el sector empresarial, sector público y en especial los usuarios de servicios provistos por estos.
  ➢ Proyectos de Respuesta Rápida: Implementar proyectos de respuesta rápida y simulacros de ciber incidentes para evaluar y mejorar la capacidad de respuesta del CSIRT.

- Estándares Internacionales:

  ➢ Adopción de Normas ISO/IEC 27001: Promover la adopción de la norma ISO/IEC 27001 para la gestión de la seguridad de la información en organizaciones públicas y privadas.
  ➢ Participación en Foros Internacionales: Incentivar la participación activa en foros y consorcios internacionales de ciberseguridad, como la Organización de Estados Americanos (OEA) y el Foro Global de Expertos en Ciberseguridad (GFCE).
  ➢ Intercambio de Información: Establecer acuerdos bilaterales y multilaterales para el intercambio de información y colaboración en investigaciones cibernéticas transnacionales.

- Plan de Acción a Largo Plazo con seguimiento y actualización:

  ➢ Desarrollar un plan de acción a largo plazo con metas y objetivos claros para cada una de las áreas mencionadas que involucren a todos los stakeholders, ya sea público, privado, academia y organizaciones sin fines de lucro.
  ➢ Monitoreo y Evaluación: Implementar mecanismos de monitoreo y evaluación para medir el progreso y ajustar las políticas según sea necesario.
  ➢ Informe Anual: Publicar un informe anual sobre el estado de la ciberseguridad en Córdoba, detallando los avances y desafíos en base al trabajo entre las partes involucradas.

e. Recomendaciones en materia de protección de datos personales

La citada Córdoba Cybersecurity Conference propuso una estrategia provincial para promover la sanción de una Ley Nacional de Protección de Datos, dado que Córdoba no puede sancionar leyes de protección de datos de fondo.

El documento fue elaborado por profesionales asistentes al Córdoba Cybersecurity Conference realizado en el mes de junio de 2024 en las instalaciones de la Universidad Siglo 21 en la ciudad de Córdoba, Argentina.

El mismo propone adoptar un enfoque estratégico para influir en la política nacional y promover la implementación de una ley de protección de datos alineada con el Reglamento Europeo, GDPR. A continuación, se detallan las acciones:

1. Desarrollo de una Política Regional Sólida

- Implementación de Políticas Locales: Aunque no pueda legislar a nivel nacional, Córdoba puede implementar políticas y normativas locales que sigan los principios del GDPR. Esto servirá como un modelo de referencia para otras provincias y el gobierno nacional.
- Establecimiento de un Consejo Asesor de Ciberseguridad: Crear un consejo compuesto por expertos en ciberseguridad, representantes del sector privado, la academia y la sociedad civil para asesorar al gobierno en la implementación de políticas de protección de datos.

2. Colaboración con Otras Provincias

- Formación de una Coalición Interprovincial: Unir fuerzas con otras provincias para formar una coalición que apoye la necesidad de una ley nacional de protección de datos. Esto aumentará la presión sobre el gobierno nacional.
- Intercambio de Buenas Prácticas: Compartir experiencias y buenas prácticas en la implementación de políticas locales de protección de datos con otras provincias.

3. Lobbying y Advocacia

- Presentación de Propuestas al Congreso Nacional: Trabajar con legisladores nacionales para presentar propuestas de ley basadas en los principios del GDPR. Proveer estudios de caso y datos que demuestren la efectividad de estas políticas a nivel local.
- Campañas de Concientización: Realizar campañas de concientización a nivel nacional para educar a la ciudadanía sobre la importancia de una ley de protección de datos.
- Utilizar medios de comunicación, redes sociales y eventos públicos para difundir el mensaje.

4. Alianzas con el Sector Privado y la Academia

- Colaboración con Empresas Tecnológicas: Asociarse con empresas tecnológicas y organizaciones del sector privado que ya estén alineadas con el GDPR para apoyar y financiar iniciativas de protección de datos.
- Proyectos de Investigación: Promover y financiar proyectos de investigación en universidades y centros de estudios sobre los beneficios y la implementación de una ley de protección de datos.

5. Participación en Foros Nacionales e Internacionales

- Participación en Foros Nacionales: Ser un miembro activo en foros nacionales sobre ciberseguridad y protección de datos, presentando la postura de Córdoba y promoviendo la necesidad de una legislación nacional.
- Interacción con Organismos Internacionales: Colaborar con organismos internacionales como la Unión Europea, la OEA y el Foro Global de Expertos en Ciberseguridad (GFCE) para obtener apoyo y orientación en la implementación de políticas de protección de datos.

6. Creación de Informes y Recomendaciones

- Informe Anual de Ciberseguridad: Publicar un informe anual sobre el estado de la ciberseguridad y la protección de datos en Córdoba, destacando los beneficios de seguir los estándares del GDPR y cómo estas políticas podrían aplicarse a nivel nacional.
- Recomendaciones Formales: Enviar recomendaciones formales al gobierno nacional y a los legisladores sobre la necesidad y los beneficios de una ley de protección de datos.

7. Programas Piloto

- Implementación de Programas Piloto: Iniciar programas piloto de protección de datos en Córdoba que puedan servir como estudios de caso para una posible implementación a nivel nacional.
- Evaluación y Ajustes: Evaluar los resultados de estos programas piloto y ajustarlas

f. Otras recomendaciones sobre Protección de Datos en el marco IA

Un documento de Accesnow[17] propone y una guía de la Dirección de Protección de Datos[18] de Argentina coinciden en algunos postulados.

PRIORIZAR LA LEGISLACIÓN DE PROTECCIÓN DE DATOS:

- Contar con una ley integral: Es fundamental tener una ley de protección de datos personales sólida y actualizada que establezca principios claros para la recopilación, el uso, el almacenamiento y la transferencia de datos, especialmente en el contexto de la IA.
- Autoridad de protección de datos independiente: Esta ley debe establecer una autoridad de protección de datos independiente con la autoridad y los recursos para supervisar y hacer cumplir las normas de protección de datos.

IMPLEMENTAR EL PRINCIPIO DE "SEGURIDAD DESDE EL DISEÑO"

- Integrar la seguridad en todas las etapas: Los sistemas de IA deben diseñarse y desarrollarse teniendo en cuenta la seguridad desde el principio, y no como una idea de último momento.
- Evaluaciones de impacto en la privacidad y seguridad: Se deben llevar a cabo evaluaciones de impacto en la privacidad y seguridad de los datos en las primeras etapas del desarrollo de la IA para identificar y mitigar los riesgos potenciales.

FOMENTAR LA TRANSPARENCIA Y LA RENDICIÓN DE CUENTAS

- Explicabilidad de los sistemas de IA: Los sistemas de IA, especialmente aquellos que toman decisiones automatizadas, deben ser transparentes y explicables. Los usuarios deben poder comprender cómo los sistemas llegan a sus conclusiones y qué datos se utilizan en el proceso.
- Auditorías de los sistemas de IA: Se deben establecer mecanismos para auditar y supervisar los sistemas de IA de forma regular para garantizar que funcionen según lo previsto y que cumplan con las normas de seguridad y protección de datos.

17 Guia especial de Accessnow para una Ley de Inteligencia Artificial, 2024: https://www.accessnow.org/wp-content/uploads/2024/08/Guia-Esencial-Para-Ley-DeInteligencia-Artificial.pdf

18 Guia de la agencia AAIP para uso responsable de la Inteligencia Artificial, 2024: https://www.argentina.gob.ar/noticias/guia-de-la-aaip-para-usar-la-inteligencia-artificial-demanera-responsable

5. COMPARACIÓN DE ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD DE AMÉRICA LATINA Y EL CARIBE

a. Análisis de Estrategias Nacionales de Ciberseguridad

15 países[19] de la región de América Latina y el Caribe poseen Estrategias Nacionales de Ciberseguridad. Resulta de utilidad comparar los elementos en común como sus diferencias y los demás elementos salientes.

Las 15 Estrategias Nacionales de Ciberseguridad se abocan de los siguientes temas:

- Fortalecimiento de capacidades.
- Ciberseguridad en la educación.
- Ciencia.
- Competitividad,
- Concientización.
- Medidas de protección.
- Cooperación.

Paradójicamente, en ninguno de los 15 ejemplos recolectados se hace referencia ni a Inteligencia de Estado, ni a Inteligencia Artificial para la vigilancia.

A continuación, se presenta una comparación de las estrategias de ciberseguridad de los Argentina, Chile y Colombia: destacando los puntos clave:

19 Estrategias Nacionales de Ciberseguridad de 15 países de la región, 2024: https://www.segurilatam.com/ciberilatam/estas-son-las-estrategias-nacionales-deciberseguridad-de-los-paises-latinoamericanos_20240514.html

1) ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE ARGENTINA[20]

- Enfoque: Argentina aborda la ciberseguridad a través de Estrategias Nacionales de Ciberseguridad, elaborando una primera versión en 2019. La segunda versión está en proceso de consulta pública.
- Objetivo principal: Proteger el ciberespacio argentino y responder a los desafíos de las nuevas tecnologías.
- Implementación: La Secretaría de Innovación Pública tiene la responsabilidad de implementar la Estrategia Nacional de Ciberseguridad aprobada por el Comité de Ciberseguridad.
- Participación: Se destaca la importancia de la participación de la ciudadanía, los sectores público y privado, la academia y la sociedad civil.

2) ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE CHILE[21]

- Enfoque: Chile cuenta con una ley específica sobre ciberseguridad que establece la Agencia Nacional de Ciberseguridad (ANCI).

  -Rol de la ANCI:

  - ➢ Protección de los intereses nacionales en el ciberespacio.
  - ➢ Coordinación interinstitucional en ciberseguridad.
  - ➢ Supervisión del sector público en ciberseguridad.

  Principios rectores: Control de daños, seguridad en el ciberespacio, respuesta responsable, racionalidad, seguridad y privacidad por defecto y desde el diseño.

- Obligaciones de ciberseguridad: Se aplican tanto a instituciones públicas como privadas y abarcan:
  - ➢ Implementación de sistemas de gestión de seguridad de la información.
  - ➢ Planes de continuidad operacional.
  - ➢ Programas de capacitación.

20 Estrategia Nacional de Ciberseguridad de Argentina, 2023: https://www.boletinoficial.gob.ar/detalleAviso/primera/279103/20230105

21 Estrategia Nacional de Ciberseguridad de Chile, 2024: https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/01/2475674.pdf

- Organismos de apoyo:
  - ➢ Consejo Multisectorial sobre Ciberseguridad: Asesora a la ANCI en la revisión de la situación de ciberseguridad del país, el análisis de amenazas y la propuesta de medidas.
  - ➢ Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional): Responde a ciberataques e incidentes de ciberseguridad de alto impacto.
  - ➢ CSIRT de la Defensa Nacional: Protege las redes y sistemas del Ministerio de Defensa Nacional y los servicios esenciales para la defensa nacional.

- Sanciones: Se aplican a las instituciones que no cumplan con las obligaciones de ciberseguridad.

3) ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE COLOMBIA[22]

- Enfoque: La estrategia de seguridad digital se integra a la Política de Gobierno Digital.
- Sujetos obligados: Las entidades señaladas en el Decreto 1078 de 2015 (DUR-TIC), que regula el sector de Tecnologías de la Información y las Comunicaciones.
- Lineamientos generales:
  - ➢ Adopción de medidas técnicas, administrativas y de talento humano para integrar la seguridad digital al plan de seguridad y privacidad de la información.
  - ➢ Mitigación de riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.
  - ➢ Adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) y la guía de gestión de riesgos de seguridad de la información.
- Estrategia de seguridad digital:
  - ➢ Integración de principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital.
  - ➢ Inclusión en el Plan de Seguridad y Privacidad de la Información, que a su vez se integra al Plan de Acción.
  - ➢ Análisis y tratamiento de riesgos de seguridad digital e implementación de controles.

22 Estrategia Nacional de Ciberseguridad de Colombia, 2021: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

- ➢ Establecimiento de roles y responsabilidades en seguridad digital.
- ➢ Promoción de una cultura de seguridad digital y de la información mediante actividades de difusión, capacitación y concientización.
- ➢ Inclusión de todas las tecnologías de la información y las comunicaciones utilizadas por la organización.

- Gestión de incidentes de seguridad digital:
  - ➢ Implementación de mecanismos para la prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje.
  - ➢ Notificación de incidentes al CSIRT de Gobierno.

4) PUNTOS DE DIVERGENCIA ENTRE LAS ESTRATEGIAS

Si bien las tres estrategias buscan un enfoque integral para abordar los desafíos del ciberespacio y destacan la colaboración entre el sector público y privado como un elemento fundamental, tienen elementos de diferencia sustancial.

Argentina se enfoca en la elaboración de Estrategias Nacionales de Ciberseguridad mientras que Chile opta por una ley específica que crea una agencia nacional. Colombia integra la seguridad digital a su Política de Gobierno Digital.

Chile establece un marco legal más completo que Argentina y Colombia, incluyendo la definición de principios rectores, la creación de organismos de apoyo, la imposición de obligaciones y la aplicación de sanciones.

Estrategia Nacional de Ciberseguridad de Brasil

Brasil posee una estrategia de ciberseguridad que data de 2020 y merece actualización. Sin embargo, por lo completo de su enfoque, se la destaca de manera separada:

- **Diagnóstico de vulnerabilidades cibernéticas:**
  - ➢ Falta de legislación adecuada sobre delitos cibernéticos: El 54% de los ataques cibernéticos reportados en Brasil se originan dentro del país. Brasil también es uno de los principales anfitriones de sitios de phishing.

- ➢ Bajo nivel de madurez en seguridad cibernética: Esto se refleja en la falta de conciencia, habilidades y conocimiento en ciberseguridad por parte de una gran cantidad de brasileños conectados al mundo digital.
- ➢ Falta de inversión en seguridad cibernética: Más de la mitad de las empresas encuestadas en un estudio destinan hasta el 2% de sus ingresos anuales a la seguridad de la información, mientras que el 34,5% destina menos del 1%.
- ➢ Falta de planes de contingencia: En 2019, el 44,2% de las empresas encuestadas en un estudio no contaban con un plan de contingencia para ciberseguridad ni presupuesto para atender una posible crisis.
- ➢ Dependencia de proveedores externos: Las empresas brasileñas, especialmente las consideradas como infraestructuras críticas, dependen en gran medida de la tecnología, lo que las hace vulnerables a los ataques a la cadena de suministro.
- ➢ Déficit de profesionales cualificados en ciberseguridad: Hay una escasez de profesionales especializados en ciberseguridad en Brasil. El 82% de los empleadores reportan una falta de habilidades en ciberseguridad en sus empleados.

- **Acciones estratégicas:** Buscan fortalecer la seguridad cibernética del gobierno brasileño, abordando diversas áreas, desde la contratación de servicios hasta la gestión de la cadena de suministro.
  - ➢ Incluir requisitos de seguridad cibernética en las contrataciones de bienes y servicios: Esta medida busca asegurar que los proveedores del gobierno cumplan con los estándares mínimos de seguridad cibernética, mejorando la protección general del sector público.
  - ➢ Perfeccionar y fomentar el uso de dispositivos de comunicación segura del gobierno: Al utilizar dispositivos de comunicación segura, se busca proteger la información sensible del gobierno y prevenir la interceptación o el acceso no autorizado.
  - ➢ Actualizar los sistemas informáticos y de comunicación de los órganos públicos: Es fundamental mantener los sistemas actualizados con las últimas medidas de seguridad para prevenir vulnerabilidades que puedan ser explotadas por atacantes.
  - ➢ Mantener copias de seguridad actualizadas y segregadas: Contar con copias de seguridad actualizadas y almacenadas en un lugar seguro permite al gobierno recuperar la información en caso de un ataque o incidente cibernético.

- ➢ Establecer requisitos de seguridad para el uso de "endpoints" en las organizaciones públicas: Los endpoints, como smartphones, laptops o tablets, son puntos de acceso vulnerables para los atacantes. Es importante establecer requisitos de seguridad específicos para su uso en las organizaciones públicas.
- ➢ Establecer requisitos de seguridad para el uso de "endpoints" en las organizaciones públicas: Los endpoints, como smartphones, laptops o tablets, son puntos de acceso vulnerables para los atacantes. Es importante establecer requisitos de seguridad específicos para su uso en las organizaciones públicas.
- ➢ Incluir requisitos de seguridad en la gestión de la cadena de suministro: Los ataques a la cadena de suministro son una amenaza creciente. Incluir requisitos de seguridad en la gestión de la cadena de suministro ayuda a mitigar este riesgo.
- ➢ Incluir requisitos de seguridad en los procesos de desestatización de servicios esenciales: Al transferir servicios esenciales al sector privado, es crucial garantizar que se mantengan los niveles de seguridad cibernética necesarios.
- ➢ Monitorear la implementación de los requisitos mínimos de seguridad por parte de los proveedores: Es importante supervisar a los proveedores para asegurar que cumplen con los requisitos de seguridad establecidos en los contratos.

- **Acciones para mejorar la legislación en ciberseguridad**

La E-Ciber reconoce la necesidad de un marco legal sólido para la seguridad cibernética en Brasil. Las fuentes indican que la legislación actual es insuficiente para abordar los desafíos que presenta el panorama digital en constante evolución. Por lo tanto, la E-Ciber propone una serie de acciones para mejorar la legislación sobre seguridad cibernética en Brasil.

Estas acciones incluyen:

- ➢ Revisar y actualizar los marcos normativos existentes para abordar las nuevas tecnologías y los nuevos tipos de amenazas cibernéticas. Esto incluye la revisión de instrumentos como el Marco Civil da Internet (Ley No. 12.965 de 2014) y la Ley General de Protección de Datos Personales (LGPD) (Ley No. 13.709 de 2018).
- ➢ Abordar nuevas temáticas en la legislación: La legislación debe abordar nuevas temáticas, como las tecnologías emergentes, el trabajo remoto y los delitos cibernéticos. Se deben incluir nuevas tipificaciones de delitos cibernéticos en el Código Penal (DecretoLey No. 2.848 de 1940).

- ➢ Elaborar un anteproyecto de ley sobre seguridad cibernética: Se debe elaborar un anteproyecto de ley que establezca directrices generales para la seguridad cibernética en Brasil. Esta ley debe ser abarcativa e incluir a todos los actores relevantes, incluyendo los poderes de la Unión, los estados, el Distrito Federal, los municipios, el sector privado y la sociedad en general.
- ➢ Crear mecanismos para la participación de la iniciativa privada y la academia en la elaboración de normativas: Se debe fomentar la participación del sector privado y la academia en la elaboración de leyes y normas sobre seguridad cibernética. Esto asegurará que la legislación sea relevante para las necesidades del país y que se base en las mejores prácticas. La E-Ciber reconoce que la seguridad cibernética es un tema de seguridad nacional que requiere un enfoque holístico y multisectorial. Una legislación sólida es fundamental para establecer un marco legal claro que guíe las acciones de todos los actores relevantes y fortalezca la resiliencia cibernética del país.

- **Cooperación Internacional en la Estrategia Brasileña:**

La E-Ciber enfatiza la importancia de la cooperación internacional en ciberseguridad para Brasil. Reconoce que, en el panorama digital actual, las amenazas cibernéticas trascienden las fronteras nacionales y que ningún país puede afrontarlas de manera efectiva por sí solo.

Para fortalecer la seguridad cibernética de Brasil en el ámbito internacional, la E-Ciber propone las siguientes acciones estratégicas:

- ➢ Ampliar la cooperación con otros países de forma transparente: Se busca colaborar con la mayor cantidad de países posible en materia de ciberseguridad, reforzando la posición de Brasil en la búsqueda de la paz y la seguridad internacional.
- ➢ Estimular las discusiones sobre ciberseguridad en organismos internacionales: Se debe promover el debate sobre ciberseguridad en los organismos, foros y grupos internacionales de los que Brasil es miembro.
  Fortalecer la relación con países de América Latina: Se reconoce la importancia de una mayor integración con los países de la región en materia de ciberseguridad.
- ➢ Promover eventos y ejercicios internacionales: La realización de eventos y ejercicios internacionales sobre ciberseguridad permitirá compartir experiencias y mejores prácticas con otros países.

- Ampliar los acuerdos de cooperación: Se deben buscar y ampliar los acuerdos de cooperación en ciberseguridad con otros países.
- Utilizar mecanismos internacionales de combate a los delitos cibernéticos: Se deben aprovechar los mecanismos internacionales existentes para combatir los delitos cibernéticos que trascienden las fronteras nacionales.
- Participar en la creación de normas para tecnologías emergentes: Brasil debe participar activamente en la elaboración de normas de seguridad para tecnologías emergentes, como las redes 5G, la inteligencia artificial y la Internet de las Cosas.
- Identificar nuevas oportunidades comerciales: Se deben explorar las oportunidades comerciales en el ámbito de la ciberseguridad, como la exportación de tecnologías y servicios.

6. RESUMEN

El trabajo de la Mesa Provincial de Ciberseguridad con participación multisectorial produjo diagnósticos y una hoja de ruta para la política pública provincial.

El mismo arroja la **recomendación principal** de **crear un Instituto Provincial de políticas digitales**, es decir, un organismo público con participación del sector privado y de la academia en su liderazgo y en el que se contemplen la Seguridad de la Información conjuntamente con otros temas emergentes, por caso, la Inteligencia Artificial.

Otro elemento importante a considerar es la **necesidad de ejecutar los proyectos** que se han detectado y desarrollado en la hoja de ruta en cualquier escenario institucional, con Instituto Provincial o con otro diseño. Asimismo, se destaca como relevante la **necesidad de adherir al reciente Plan Nacional.**

7. BIBLIOGRAFÍA

-World Economic Forum. (2024). Global Risk Report. Recuperado de https://assets.weforum.org/editor/responsive_large_webp_6D5m57mKtQKA7ugUygfOOd7u6XyQkOLom4zuae4Xb7A.webp

- Pallero, M. (s.f.). Relevamiento de Ciberincidentes a bases de datos críticas de Argentina. Recuperado de https://time.graphics/es/line/630567

- NCSI. (s.f.).Ranking comparativo de NCSI. Recuperado de https://ncsi.ega.ee/compare/

-Unión Internacional de Telecomunicaciones. (2021). Índice Mundial de Ciberseguridad. Recuperado de https://www.itu.int/dms_pub/itud/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

- Universidad Siglo 21 (2024).Cordoba Cybersecurity Conference 2024, coorganizada por la UE SXXI y el CSIRT Córdoba. Recuperado de https://21.edu.ar/identidad21/gobierno-y-ciberseguridad-la-urgencia-depoliticas-publicas-y-gestion-de-incidentes

- CSIRT Córdoba. (s.f.). El CSIRT Córdoba cuenta con un mecanismo de gobernanza multisectorial. Recuperado de https://csirtcordoba.ar/

- CSIRT Americas. (2023). Guía Práctica de CSIRT Américas. Recuperado de https://shares.csirtamericas.org/s/AqfMc7XYBmcRpZM/download/GuiaCSIRT%202023%20ESP%20V6.pdf

- ENISA. (s.f.). Red Europea de CSIRTs. Recuperado de https://www.enisa.europa.eu/topics/eu-incident-response-and-cybercrisis-management

- Banco Mundial. (2024). Guía del Banco Mundial para CSIRTs en países en desarrollo. Recuperado de https://documents1.worldbank.org/curated/en/099060824112023473/pdf/P177852158c0330d51a71613967bd98edc4.pdf

- Oxford Cyber Security Capacity Centre. (2021). Modelo de Madurez de capacidades de ciberseguridad de Oxford. Recuperado de https://gcscc.ox.ac.uk/the-cmm

- Oxford Cyber Security Capacity Centre. (2021). Proceso de revisión del Modelo de Madurez de Oxford. Recuperado de https://gcscc.ox.ac.uk/cmm-review-process

- Access Now. (2024). Guía especial de Accessnow para una Ley de Inteligencia Artificial. Recuperado de https://www.accessnow.org/wpcontent/uploads/2024/08/Guia-Esencial-Para-Ley-De-InteligenciaArtificial.pdf

- Agencia Argentina de Acceso a la Información Pública. (2024). Guía de la agencia AAIP para uso responsable de la Inteligencia Artificial. Recuperado de https://www.argentina.gob.ar/noticias/guia-de-la-aaippara-usar-la-inteligencia-artificial-de-manera-responsable

- SeguriLatam. (2024). Estrategias Nacionales de Ciberseguridad de 15 países de la región. Recuperado de https://www.segurilatam.com/ciberilatam/estas-son-las-estrategiasnacionales-de-ciberseguridad-de-los-paiseslatinoamericanos_20240514.html

- Boletín Oficial de la República Argentina. (2023). Estrategia Nacional de Ciberseguridad de Argentina. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/279103/20230105

- Diario Oficial de la República de Chile. (2024). Estrategia Nacional de Ciberseguridad de Chile. Recuperado de https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/0 1/2475674.pdf

- Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia. (2021). Estrategia Nacional de Ciberseguridad de Colombia. Recuperado de https://gobiernodigital.mintic.gov.co/692/articles162625_recurso_2.pdf