Comentarios a la Segunda Estrategia Nacional de Ciberseguridad

Resumen

Este documento contiene los aportes de los equipos interdisciplinarios de la Fundación Sadosky a la propuesta de Estrategia Nacional de Ciberseguridad presentada mediante la Resolución 1/2023 de la Secretaría de Gabinete de Ministros de la Jefatura de Gabinete de Ministros el 5 de enero de 2023.

Está dividido en comentarios generales a la Estrategia Nacional y comentarios sobre los objetivos. Nos enfocamos en nuestras áreas de especificidad, en particular sobre los aspectos técnicos de seguridad informática y de seguridad de la información, así como aspectos de seguridad pública.

Índice

Tabla de contenido

Sobre la Fundación Sadosky

La Fundación Sadosky es una organización público-privada dentro de la órbita del Ministerio de Ciencia, Tecnología e Innovación de la Nación, cuya misión es la articulación para la innovación productiva en el sector TIC. Cuenta con equipos interdisciplinarios con amplia experiencia en distintas áreas relacionadas con la Informática y está comprometida a contribuir con el desarrollo del país desde su especificidad temática.

La Fundación analizó el documento a la luz de experiencias internacionales, así como los antecedentes en el país en lo que hace a la elaboración de Estrategias Nacionales.

La propuesta de Estrategia Nacional de Ciberseguridad fue analizada por los equipos de Seguridad en TIC en colaboración con los equipos de Ciencias de Datos e Inteligencia Artificial, de Legales y del área de TIC para la Paz, la Justicia y las Instituciones Sólidas. En este análisis intervinieron investigadoras, investigadores y profesionales de la Informática, de las Ciencias de Datos y del Derecho, entre otros.

Sobre este documento

Este documento es el resultado del análisis de marcos internacionales de ciberseguridad en sus distintas aristas y de profesionales multidisciplinares antes mencionados, en conjunto con la Dirección Ejecutiva de la institución, y expertas y expertos convocados específicamente. La decisión ha sido centrarse en los aspectos en los que, a nuestro criterio, se impide el desarrollo de una política pública efectiva en materia de ciberseguridad.

Los aportes que a continuación se enumeran están relacionados con la Estrategia Nacional, desde su elaboración hasta los organismos asignados para su puesta en funcionamiento y el contenido de sus objetivos. Los comentarios apuntan a señalar debilidades y enfoques que pondrían en riesgo la eficacia de la estrategia y la orientación de la temática.

A su vez, hemos tratado de que nuestros aportes pongan en primer plano el ejercicio de derechos por parte de la ciudadanía, no solo en las declaraciones sino para las acciones. Aspectos como el uso del cifrado, la persecución penal a las personas que reportan vulnerabilidades o la protección de la privacidad en las investigaciones penales nos obligan a promover un enfoque que se centre en la prevención; expectativa que se diluye cuando se incluye en la definición de Ciberseguridad al delito, sin desconocer la necesidad, al mismo tiempo, de la capacitación en seguridad informática e informática forense para la investigación de delitos que usen o tengan como finalidad a las tecnologías para todos los operadores de la justicia y sus auxiliares.

Principales aportes

Resumimos aquí los principales comentarios:

1. Sugerimos realizar un diagnóstico en materia de ciberseguridad en base a un marco de referencia reconocido internacionalmente y la Estrategia Nacional de Ciberseguridad 2019.
2. Sugerimos establecer marcos de ciberseguridad para definir ámbitos de coordinación e incorporar seguridad de la información en los servicios al ciudadano desde el Estado, en todos sus servicios digitales. También, evaluar un mejor diseño institucional para la ejecución de las políticas públicas y de la Estrategia Nacional de ciberseguridad.
3. Proponemos adoptar, junto a los principios de ciberseguridad, los aspectos relativos a la protección de datos y privacidad.
4. Proponemos la adopción de un marco de medición para la planificación y las acciones.
5. Proponemos la creación de una institución que estudie, analice e investigue los distintos aspectos de la ciberseguridad para el asesoramiento en materia de capacitación, emisión de regulaciones, normativa, legislación y para colaborar con el Poder ejecutivo.
6. Sugerimos el fortalecimiento de las acciones de gestión ante incidentes. En particular, la asistencia y la generación de material que den soporte a la distinta normativa y permita la coordinación de acciones ante incidentes relevantes en general y ante aquellos que afecten a la protección de datos en particular.
7. Proponemos elaborar y desarrollar un marco de formación en ciberseguridad para identificar áreas de conocimientos faltantes y proponer planes de capacitación.
8. Sugerimos promover investigación en materia de ciberseguridad. Su despliegue, tanto en las administraciones públicas como en el sector privado, desde el diseño y por defecto en productos y servicios.
9. Proponemos una visión preventiva, teniendo como objeto de la prevención los incidentes de seguridad informática o ciberseguridad, y sugerimos eliminar la referencia al delito en la definición de ciberseguridad.
10. Proponemos incluir en la Estrategia Nacional, específicamente para prevenir incidentes, la definición de circuitos efectivos para reportar vulnerabilidades en organismos públicos y promover acciones similares para el sector privado.

Comentarios generales a la Estrategia Nacional

a. **Sobre los principios rectores:**

- Las declaraciones enunciadas en los principios rectores deberían ser incorporadas en los planes de acción y, para que no queden como meros enunciados, su inclusión debería ser identificada y controlada.

b. **Sobre el marco organizativo de la Estrategia Nacional de ciberseguridad:**

- En el marco organizativo actual, el Comité Nacional está conformado por representantes de los ministerios designados por decretos del Poder ejecutivo, con la experiencia y formación que hace a cada funcionario. En este sentido, y debido a la amplia variedad y especificidad técnica que aborda la ciberseguridad actual, se considera imprescindible contar con la asesoría de especialistas en sus distintos campos. Esta asesoría debería institucionalizarse para que luego asista a los representantes del Comité Nacional y al Poder Ejecutivo en la toma de decisiones que consideren oportunas de acuerdo con las incumbencias de cada ministerio y la política que el Ejecutivo haya definido para sus áreas.

  En el mismo sentido, y para la coordinación estratégica en el despliegue de las políticas públicas, es necesario un liderazgo ejecutivo en la asignación de las funciones en materia de ciberseguridad, que no está presente en el actual esquema.

  El desarrollo y la implementación de la Estrategia Nacional debería ser liderada por un organismo con capacidades ejecutivas, recursos asignados a tal fin, personal con las capacidades administrativas, técnicas e infraestructura necesaria. Por su parte, el Comité Nacional debería oficiar de participante para la coordinación del despliegue de las políticas en lo que a cada ministerio le incumbe. Por otro lado, habrá actividades que cada ministerio deberá llevar adelante, por lo que la instancia interministerial es necesaria.

c. **Sobre aspectos prácticos y de forma de la estrategia:**

- Una estrategia es un documento que registra la forma de llevar adelante un objetivo prioritario. Se mencionan ocho objetivos con un conjunto de acciones generales, sin mencionar acciones concretas, ni plazos. No se mencionan instancias de planificación, por lo que se entiende que las actividades correspondientes a la planificación ya fueron realizadas. Se recomienda indicar plazos, documento con objetivos concretos (medibles) y recursos estimados y asignados para facilitar el seguimiento y control de su cumplimiento. Sería deseable contar con un informe de resultados con alguna fecha preestablecida y estimada.
- Por otro lado, para la definición de metas concretas y medibles es necesario la realización de un diagnóstico con la finalidad de evaluar el estado de situación actual y planificar un camino hacia los objetivos deseables. Para este diagnóstico podrían utilizarse referencias como los modelos de madurez en ciberseguridad de la Unión Internacional de Telecomunicaciones (ITU), o

el Modelo de la Universidad de Oxford, como así también la evaluación de cumplimiento de la Estrategia nacional 2019 para identificar metas cumplidas, desafíos no resueltos y/o lecciones aprendidas.

d. Sobre los procesos y requisitos de las TIC en general:

- Deberían identificarse aspectos como los planes de continuidad del negocio/TIC, análisis técnicos de factibilidad, la gestión de crisis, la ingeniería de requerimientos o la ingeniería de software en los proyectos del sector público que incluyan tecnologías de la información. Temas que sin ser estrictamente de seguridad son prerrequisitos para que las acciones de ciberseguridad sean efectivas. Es necesario que estos temas sean incorporados como requerimientos básicos e incorporarlos a las recomendaciones o normativas como tales.

e. Sobre aspectos básicos de la Ciberseguridad:

- Las tecnologías y servicios se diversifican de manera rápida, creciente e interactúan para dar lugar a la complejidad. Para su protección, es necesario contar con una institución técnica que pueda emitir recomendaciones basadas en evidencia y principios técnicos, tanto de las Ciencias de la Computación como de la Ingeniería en Sistemas de Información o Informática, principalmente. También que pueda intervenir en las recomendaciones, emitir dictámenes u opiniones en aspectos claves como: normativas, estándares y protocolos, con capacidades de investigación en seguridad, así como en la aplicación de nuevas tecnologías.

  No se puede esperar que el asesoramiento o la asistencia técnica segmentada por temas y ad-hoc sea un práctica que perdure en el tiempo cuando aspectos como la seguridad o la soberanía nacional están en juego, ni temáticas que hacen a los derechos fundamentales como la libertad de expresión o la privacidad, o conflictos geopolíticos. Debería poder establecerse una institución para orientar y promover las mejores capacidades para el país en los distintos campos y disponibles cuando sea necesario.

  Aplicaciones de las TIC como IoT (internet de las cosas), nube, IA (inteligencia artificial o machine learning) y 5G, entre otras, tienen sus aspectos específicos en materia de seguridad que deberán ser contempladas al momento de emitir alguna recomendación o regulación, así como establecer requisitos en sus despliegues en el país.

  Por otro lado, las exigencias derivadas de la legislación vigente en materia de protección de datos (Ley 25326 y Ley 27699) y el proyecto de actualización de la ley vigente implican, en el estado actual de las tecnologías, la necesidad de una institución técnica que pueda orientar en su cumplimiento, en sus aspectos relacionados con los servicios y productos digitales, las plataformas y los intereses de los habitantes de este país y del Estado.

  En el mismo sentido, la evaluación o informes de ciberamenazas requieren un seguimiento y análisis, a nivel local, para emitir las recomendaciones oportunas y específicas a nuestro país, tanto para la población en general como para las autoridades y sus decisiones estratégicas.

Cualquier normativa o recomendación en términos de requisitos técnicos para completar el ciclo de vida debería ser auditada y su cumplimiento certificado para un aseguramiento del sistema, por lo que contar con una institución técnica con tales capacidades es imprescindible.

- El fortalecimiento del CERT coordinador nacional debería ser la prioridad para la asistencia técnica sobre seguridad informática y aspectos relacionados con el sector público. Como así también debería brindarse atención a los incidentes de los denominados “data breach” (incidentes de ciberseguridad que involucra datos personales) basado en los estándares internacionales, por ejemplo, los de la comunidad FIRST, en el asesoramiento a la comunidad de atención, brindar información en línea y asistencia para la creación de más equipos de respuesta a incidentes que atiendan distintos sectores.

f. Sobre marcos de formación en ciberseguridad:

- En materia de capacitación se considera necesario contar con un marco de referencia en materia de ciberseguridad que dé cuenta de las habilidades, capacidades y conocimientos necesarios para abordar sus distintas áreas y tareas.
- Analizar, comparar y establecer un marco de referencia de requisitos básicos en materia de seguridad de la información, como en ciberseguridad, para que haya un entendimiento de las actividades y acciones más relevantes y promover capacitaciones y planes de formación para cubrir las necesidades de mayor importancia. De esta manera, se podría evaluar mejor el riesgo de no abordar temas complejos y críticos, como seguridad desde el diseño y por defecto en software o proyectos de TI, algoritmos criptográficos, metodologías y herramientas de gestión de riesgos, riesgos de la biometría, gestión de crisis, etc.
- El Estado debe promover la formación en ciberseguridad y privacidad para que los requisitos de la legislación en protección de datos se incorporen como controles técnicos en conjunto con los de seguridad, en la formación y educación de todos los niveles educativos.
- Según los ámbitos de aplicación, ya sea para el diseño, implementación o en cuanto a características deseables de un servicio, las recomendaciones en materia de ciberseguridad deben contemplar aspectos de usabilidad, accesibilidad, interoperabilidad, o de otras disciplinas aplicables. Así como aspectos que hacen a la psicología de las personas en materia de concientización, por lo que es necesaria la incorporación de recomendaciones y análisis en materia de diversidad de capacidades y de género en la formación de las personas.

g. **Sobre aspectos sociales y de gobernanza de la ciberseguridad:**

- Los servicios digitales inseguros generan múltiples incidentes que afectan a las personas en su vida económica, política y social. Se encuentran en peligro aspectos de la libertad de expresión, la intimidad y afectaciones patrimoniales, como mínimo.

  En este sentido, promover una cultura de ciberseguridad implica la incorporación de los principios de seguridad y privacidad desde el diseño y por defecto en productos y servicios digitales en un sentido práctico y utilitarista; pero también es necesario fomentar un desarrollo o cambio cultural para que inversores, accionistas y tomadores de decisiones de distintas industrias entiendan las consecuencias de los problemas de seguridad, las responsabilidades y sus alcances.

  Promover la cultura de ciberseguridad, entonces, requiere un conjunto de acciones que tiendan a producir cambios en las conductas humanas, a lo largo del tiempo, en distintos segmentos educativos y socioculturales. Por este motivo, son necesarias acciones y producciones en el ámbito de la investigación científica, desarrollos, normas, políticas públicas y recomendaciones basadas en evidencias, en los distintos campos de las ciencias como de la tecnología aplicada.

  En la misma línea de ideas, es necesario divulgar y concientizar sobre las acciones que se deben adoptar desde las máximas autoridades de los organismos públicos, las empresas y organizaciones de todo tipo en materia de ciberseguridad. Independientemente de la industria, se debe sensibilizar sobre los procesos de gestión de los riesgos de tecnología y seguridad de la información, la asignación de recursos, promover cultura y liderazgo para que las acciones se lleven adelante, controlando y gestionando. Estas acciones corresponden al ámbito que se denomina gobierno o gobernanza de la ciberseguridad

Comentarios sobre los objetivos de la Estrategia Nacional de Ciberseguridad

a. Seguridad y privacidad.

- En virtud del ciclo de vida de los sistemas de información o, desde otro punto de vista, de los servicios y productos digitales cabe mencionar que la seguridad desde el diseño y por defecto debería estar acompañada por el principio de privacidad, también desde el diseño. En esta materia, los marcos de referencia en ciberseguridad se han actualizado en los últimos años y en ellos se incorpora el abordaje de la seguridad en conjunto con la privacidad.

Tres ejemplos:

1) La reciente versión del estándar internacional mundialmente reconocido y tomado de referencia por Argentina desde 2005. ISO/IEC 27001:2022 se denomina “Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos”.
2) El estándar internacional que se utiliza como referencias en materia de controles de seguridad informática es de la Serie 800 de NIST (Instituto Nacional de Estándares y Tecnologías) la publicación 800-53 rev. 5 que se denomina “Controles de seguridad y privacidad para sistemas de información y organizaciones”.
3) Contenidos sobre sobre las habilidades y capacidades en ciberseguridad del Marco de referencia europeo.

En este sentido, se recomienda incorporar contenidos de protección de la privacidad y datos personales en los objetivos de la Estrategia Nacional de Ciberseguridad; en particular, en la formación y elaboración de normativa

b. La coordinación y gestión de incidentes de ciberseguridad y el delito.

- La gestión de incidentes es la base técnica sobre la que los países han desarrollado su visión estratégica de la ciberseguridad porque lo esencial ante un incidente es brindar asistencia, como así también intercambiar la información de incidentes y vulnerabilidades para evitar nuevas ocurrencias.

  Asimismo, teniendo en cuenta que en los catálogos básicos de servicios de los equipos de respuesta ante incidentes (CERT/CSIRT/ERI, etc.), la asistencia ante incidentes es solo uno de los servicios reactivos, existen también servicios preventivos y de gestión de la calidad de la seguridad de la información. En este sentido es importante fortalecer el CERT Nacional para que asista a su comunidad en modalidad 7x24x365 con los canales de comunicación adecuados, así como se deberían promover la creación de CSIRT sectoriales por industria, academia en las provincias, municipios y en los distintos poderes del Estado. Estos equipos con capacidades técnicas luego podrían asistir en la prevención de incidentes, así como ante la eventual investigación de un delito en el caso que corresponda.

El objetivo 3, en este sentido, debería ser específico en el objeto de las acciones enunciadas en materia de ciberseguridad, debiendo indicarse: “Fortalecimiento de capacidades en prevención, detección y respuesta ante incidentes de seguridad informática”, ya que como está expresado en el texto actual, el objeto de las acciones de prevención, detección y respuesta se aplicarían al uso del ciberespacio con fines ilícitos e indebidos.

El enunciado actual de la propuesta es que las acciones de la ciberseguridad deben basarse en la prevención y para identificar un uso con fines ilícitos o indebidos del ciberespacio. En este sentido, en el análisis del texto del Objetivo 3 de la propuesta de Estrategia, se indica “Fortalecer las capacidades de prevención, detección y respuesta frente al uso del ciberespacio con fines ilícitos o indebidos”, es decir, requiere que debe llegarse a la intención del uso del ciberespacio para evaluar la ilicitud o la acción indebida de un comportamiento humano. El campo de estudio ya se pasa al contexto de las acciones en el campo del derecho, por la definición que se adopta en el glosario de ciberseguridad, se inclina hacia el derecho penal. En esta línea, en la seguridad de la información, como disciplina, están las herramientas que también abarcan evitar errores humanos o fallas en la gestión como objetivos, que permiten prevenir abusos del “ciberespacio”, incluyendo implícitamente esos objetivos.

> “Ciberseguridad: conjunto de políticas, estrategias y acciones orientadas a elevar los niveles de seguridad de las personas físicas y jurídicas frente a incidentes y delitos que utilicen como medio y/o fin un dispositivo informático.”

Una estrategia de ciberseguridad debe priorizar el aseguramiento de procesos y tecnología para procurar mejorar la seguridad de servicios y productos digitales, su desarrollo, implementación, mantenimiento y mitigación de los riesgos primero. También capacitar y educar a desarrolladores, a tomadores de decisiones y demás actores involucrados en la industrias de las tecnologías, y otras industrias que utilizan tecnologías, coordinar y asistir para resolver vulnerabilidades técnicas, accionar ante incidentes para contener consecuencias negativas. Además, analizar y compartir información de amenazas y concientizar sobre usos responsables, por mencionar algunas acciones centrales, con la finalidad de construir un entorno más seguro. Como consecuencia del conjunto de estas acciones se minimizan los incidentes y se aprende de ellos para evitarlos desde su análisis.

Por otro lado, que algunos incidentes se evalúen como delito debería estar analizado en el “Plan de gestión de incidentes de cada organización”, para una mejor resolución en términos de la investigación de delitos. La ciberseguridad debe estar basada en la prevención de incidentes y la colaboración en la investigación del delito, como una acción más, así como la ciberseguridad está relacionada en la cultura de la protección de datos personales y privacidad. Incluir en la definición de ciberseguridad al delito, deviene en una visión desde el derecho penal que no es necesaria ni contribuye a la creación de una visión preventiva y sustentable hacia el futuro. Sin mencionar los debates por el uso del cifrado en la investigación del delito.

El delito es una conducta específica disvaliosa establecida en un código y la última barrera de la sociedad para sancionar a las personas que transgreden ese código. Deberían identificarse e institucionalizarse las acciones de ciberseguridad para colaborar con la prevención e investigación de tales conductas, pero no convertir al delito como objeto de la ciberseguridad por definición, ya que existe como riesgo utilizar como herramientas de ciberseguridad, instrumentos del derecho penal, cuando el campo de conocimiento que hace el mayor aporte en la prevención viene de los principios y aplicación de la seguridad de la información y la seguridad informática.

Entre otros argumentos también se puede mencionar que, en la Carta de Derechos Digitales europea, el derecho a la ciberseguridad se encuentra bajo el título de Derechos de Libertad, capítulo VI y está enunciado como:

> Derecho a la ciberseguridad.
>
> 1. Conforme al ordenamiento jurídico, toda persona tiene derecho a que los sistemas digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o le presten servicios, posean las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información tratada y la disponibilidad de los servicios prestados.
>
> 2. Los poderes públicos, de conformidad con la regulación europea y nacional, velarán para que las garantías expresadas en el número anterior sean satisfechas por todos los sistemas de información, ya sean de titularidad pública o privada, proporcionalmente a los riesgos a los que estén expuestos. A tal efecto podrán contar con la colaboración de la sociedad civil. 3. Los poderes públicos promoverán la sensibilización y formación en materia de ciberseguridad de toda la sociedad e impulsarán mecanismos de certificación.

Así también y en un sentido la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital formula en su Capítulo V: seguridad, protección y empoderamiento:

> *Un entorno digital protegido y seguro*
>
> 16. Toda persona debería tener acceso a tecnologías, productos y servicios digitales diseñados para estar protegidos, ser seguros y proteger la privacidad, lo que se traduce en altos niveles de confidencialidad, integridad, disponibilidad y autenticidad de la información tratada.

Por los motivos expuestos se sugiere eliminar de la definición de ciberseguridad la referencia al delito como objeto. Adicionalmente, implicaría orientar la disciplina en el contexto nacional, como ya se mencionó, al despliegue en términos conceptuales sobre las conductas tipificadas en el código penal para cualquier área o en la formación que requiera implementar “ciberseguridad”.

c. Coordinación de atención a vulnerabilidades técnicas.

- Así como la asistencia ante incidentes es una de las actividades principales de los CERT o CSIRT nacionales, entre las prácticas recomendadas está la coordinación para la atención y resolución de vulnerabilidades (es un servicio preventivo básico de los CSIRT), por lo que deberían priorizarse las acciones en este sentido como parte de la prevención de incidentes. Las acciones en este sentido son una recomendación por parte de todos los estándares en seguridad de la información y también lo son por parte de organismos internacionales como la OCDE y la ONU y fueron adoptadas en la legislación de la Unión Europea en la Directiva NIS2 y también en la Orden Ejecutiva para mejorar la ciberseguridad de EEUU en 2021.

  Se sugiere incluir como acción dentro de la prevención de incidentes, la planificación y puesta en funcionamiento de circuitos efectivos para el tratamiento y coordinación de vulnerabilidades en el Sector público y promover acciones con similar objetivo para el sector público de otras jurisdicciones y para el sector privado.

Buenos Aires, 16 de febrero de 2023.

Referencias y antecedentes

Normativa Argentina relacionada.

Resolución 1/2023 de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros. Llamado a consulta pública de la Estrategia Nacional de ciberseguridad. Asignación de impulso a la Secretaría de innovación.

https://www.boletinoficial.gob.ar/detalleAviso/primera/279103/20230105

Decreto 577/2017 - Creación del Comité Nacional de ciberseguridad (CNC)

http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm

Decreto 480/2019 - Ampliación, cambio de dependencia del CNC

http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/325052/norma.htm

Resolución 819/2019 de la Secretaría de Gobierno de Modernización- Estrategia Nacional de Ciberseguridad 2019.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/323594/norma.htm

Resolución 141/2019 JGM - Desígnase la presidencia del Comité de Ciberseguridad Nacional en el Secretaría de Gabinete de Modernización. Res. 149/2019 JGM

https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-141-2019-323038/texto

Resolución 1523/2019 Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros. Definición de infraestructuras críticas y glosario.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/328599/norma.htm

Modelo de madurez en materia de ciberseguridad para naciones.

Índice global de ciberseguridad de ITU.

https://www.itu.int/es/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/New_Reference_Model_GCIv4_V2_.pdf

Modelo de Madurez en ciberseguridad de la Escuela Martin Oxford de la Universidad de Oxford.

https://www.oxfordmartin.ox.ac.uk/cyber-security/

Descripción del modelo: https://www.oxfordmartin.ox.ac.uk/cyber-security/

Referencias al estándar ISO/IEC 27001 de seguridad de la información en la normativa Argentina.

Disposición ONTI 6/2005 - Apruébase la "Política de Seguridad de la Información Modelo".

http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/108672/norma.htm

Disposición ONTI 3/2013 - Apruébase la “Política de Seguridad de la Información Modelo”.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219163/norma.htm

Disposición ONTI 1/2015 - Aprobación de la “Política de Seguridad de la Información Modelo”

http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Decisión Administrativa 641/2021 - Requisitos mínimos de seguridad de la información para el Sector público.

https://ww.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-641-2021-351345

Sobre Derechos digitales en Europa.

Carta de Derechos digitales europea:

https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Declaración sobre los Derechos y Principios Digitales para la Década Digital

https://www.amic.media/media/files/file_352_3194.PDF

Leyes y proyecto en materia de Protección de datos personales de Argentina.

Ley 25326. Ley de Protección de datos

http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Ley 27699. Adhesión al Convenio 108+. Protección de datos personales.

https://www.boletinoficial.gob.ar/detalleAviso/primera/276783/20221130

Proyecto de actualización de la Ley 25326.

https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_datos_personales_aaip.pdf

Algunas acciones a nivel nacional en Latinoamérica sobre ciberseguridad

Colombia.

Cada CONPES establece objetivos y plazos en materia de seguridad digital a nivel Nacional. Que se ha evolucionado y adecuado a lo largo de los años.

1) CONPES-3854 - https://www.cancilleria.gov.co/sites/default/files/planeacion_estrategica/conpes_3854_-_seguridad_digital.pdf (2017) Política Nacional de Seguridad Digital.

2) CONPES-3995 - 2020. POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL https://www.csirtasobancaria.com/publicaciones/conpes-3995-politica-nacional-de-confianza-y-seguridad-digital
3) CONPES 4022 - 2022

   https://www.dnp.gov.co/Paginas/Asi-fortalecio-Colombia-su-ecosistema-digital-en-cuatro-anos.aspx

Críticas a las CONPES de la organización Karisma. 2016

https://web.karisma.org.co/que-es-el-conpes-de-seguridad-digital-y-por-que-esta-mal/

Uruguay:

Adaptó y adoptó el Marco de ciberseguridad de NIST como marco nacional de ciberseguridad, luego de un diagnóstico. Incluye auditorías y autoevaluación.

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

Chile:

Decreto del MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA- Subsecretaría del Interior- ESTABLECE OBLIGACIÓN DE REPORTAR INCIDENTES DE CIBERSEGURIDAD. 2022, septiembre.

https://www.diariooficial.interior.gob.cl/publicaciones/2022/12/02/43416/01/2226218.pdf

Proyecto de Ley Marco de Ciberseguridad en tratamiento legislativo.

https://www.trendtic.cl/2023/01/chile-proyectos-de-ley-sobre-ciberseguridad-y-proteccion-de-datos-personales-toman-velocidad-en-el-congreso/

Brasil:

Decreto 2020. Estrategia Nacional de ciberseguridad.

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm

Decreto 2018. Política Nacional de Seguridad de la Información.

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm

República Dominicana:

El Centro Nacional de Ciberseguridad, Decreto presidencial: aborda aspectos básicos prioritarios. Ya tienen un Centro Nacional de Ciberseguridad.

https://cncs.gob.do/wp-content/uploads/2022/12/Decreto-685-22.pdf

Referencias internacionales sobre estrategias nacionales de ciberseguridad

Herramienta de evaluación de estrategias nacionales de ciberseguridad. ENISA (Agencia Europea de Ciberseguridad)

https://www.enisa.europa.eu/news/enisa-news/enisa-launches-the-cybersecurity-strategies-evaluation-tool/

Marco de evaluación de capacidades en ciberseguridad de ENISA

https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-es.pdf

Cybersecurity Culture guidelines: Behavioral Aspects of cybersecurity, december 2018. ENISA

https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

Referencia para analizar estrategias nacionales de ciberseguridad. Si bien el sitio está en construcción, se encuentran listados los Framework recomendados para la elaboración de Estrategias Nacionales de ciberseguridad.

https://nationalcyberstrategies.org/part-1-advocating-for-a-national-cybersecurity-strategy/

Mapa interactivo de las Estrategias Nacionales Europeas de los distintos países.

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Estándares internacionales en Seguridad de la Información

ISO/CEI 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.

https://www.iso.org/standard/82875.html

NIST SP 800-53 rev. 5 Controles de seguridad y privacidad para sistemas de información y organizaciones

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Sobre los servicios básicos de un CERT/CSIRT

CSIRT al pie del cañón. https://www.first.org/newsroom/releases/FIRST-Press-Release-20201118.pdf

Coordinación y divulgación de vulnerabilidades.

OECD - Policy Framework on Digital Security- Cybersecurity for Prosperity. 4.1 - Tratamiento de las vulnerabilidades.

https://read.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en#page31

Resolución de las Naciones Unidas - Septuagésimo tercer período de sesiones- Tema 96 del programa. Resolución aprobada por la Asamblea General el 5 de diciembre de 2018 [sobre la base del informe de la Primera Comisión (A/73/505)] 73/27. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

https://digitallibrary.un.org/record/1655670/files/A_RES_73_27-ES.pdf

NIS2 - Directiva europea de ciberseguridad.

La Directiva (UE) 2022/2555, conocida como NIS2, establece principalmente obligaciones de ciberseguridad para los Estados miembros y medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación.

https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2023/Enero/Noticia-2023-01-09-Publicada-la-Directiva-NIS2-relativa-a-medidas-de-ciberseguridad.html

Orden ejecutiva - Mejorando la ciberseguridad - Mayo 2021

Executive Order on Improving the Nation's Cybersecurity

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Colaboradores

Colaboraron en este documento:

Matías Cavanagh

Victoria Dumas

Juan Heguiabehere

Laura Marés

Marcela Pallero

Fernando Schapachnik

Gustavo Sibilla