ESTRATEGIA NACIONAL de **CIBERSEGURIDAD del URUGUAY** 2024 - 2030

Uruguay Presidencia

agesic

CONTENIDOS

1

RESUMEN EJECUTIVO

Uruguay reafirma su compromiso con la ciberseguridad y la competitividad global a través de la Estrategia Nacional de Ciberseguridad (ENC) 2024-2030, cuya visión es que el país se destaque por tener un ciberespacio seguro, abierto, resiliente y confiable, que impulse el desarrollo sostenible y proteja los derechos y libertades de todas las personas.

Esta Estrategia involucra activamente sector público y privado, la academia, la sociedad civil y a todas las personas. En su elaboración participaron 49 instituciones públicas, 57 instituciones del sector privado, 12 instituciones del sector educativo, 6 organismos internacionales y 3 organizaciones de sociedad civil.

Esta Estrategia se desarrolla en respuesta al creciente desafío que representan las ciberamenazas, y se fundamenta en los siguientes principios rectores: un enfoque centrado en las personas, para proteger derechos y privacidad; una mirada holística que integra diversos sectores; la gestión proactiva de riesgos para adaptarse a un entorno digital en constante cambio; la articulación, la colaboración e inversión entre actores nacionales e internacionales; y el fortalecimiento de la resiliencia digital para asegurar la continuidad de operaciones en caso de ciberataques. La misma impulsará 24 líneas estructuradas en 8 pilares: Gobernanza; Marco normativo; Ciberdelitos; Ciberdefensa; Infraestructuras de información crítica; Cultura de ciberseguridad; Ecosistema e industria; y Política internacional.

Su implementación está sujeta a un proceso de seguimiento, monitoreo y evaluación a cargo del Comité de Gestión de la Estrategia Nacional de Ciberseguridad formalizado por la Ley 20.212 Artículo 83.

Su creación refuerza el marco de colaboración nacional e internacional conseguido para responder a ciberataques y apoyar la transformación digital del país.

2

INTRODUCCIÓN

La Estrategia Nacional de Ciberseguridad (ENC) de Uruguay establece un enfoque integral para enfrentar los crecientes desafíos del ciberespacio y proteger a las personas, organizaciones y las infraestructuras de información crítica del país.

Ante la creciente sofisticación de las ciberamenazas como el ransomware, los ataques a la cadena de suministro y la desinformación, que afectan a las personas y a la industria, se ponen en riesgo la seguridad, erosionando la confianza en las instituciones y generando pérdidas económicas significativas. La ciberseguridad se convirtió en una prioridad para poder hacer un uso seguro del potencial de la transformación digital y las tecnologías emergentes.

Fortalecer e impulsar la ciberseguridad es necesario para garantizar la estabilidad del país y apoyar el crecimiento económico. La ENC fomenta una cultura de ciberseguridad que empodere a las personas y organizaciones para el uso seguro de la tecnología, fortalece las capacidades nacionales mediante la inversión en educación y formación en ciberseguridad en todos los niveles, garantiza la protección de la información sensible y la continuidad de los servicios críticos. Asimismo, reconoce la naturaleza global de las ciberamenazas, por lo que fomenta la cooperación internacional para coordinar una respuesta efectiva y coherente ante estos desafíos.

La Estrategia es el resultado de un proceso participativo y multisectorial, que se fundamenta en los siguientes principios rectores: un enfoque centrado en las personas; una mirada holística; la gestión proactiva de riesgos; la articulación y colaboración entre actores nacionales e internacionales; y el fortalecimiento de la resiliencia digital. Además, se apoya en ocho pilares clave: Gobernanza; Marco normativo; Ciberdelitos; Ciberdefensa; Infraestructuras de información crítica; Cultura de ciberseguridad; Ecosistema e industria; y Política internacional; que presentan líneas de acción específicas para garantizar un ciberespacio seguro, abierto, resiliente y confiable.

Uruguay se ha posicionado en un lugar destacado en América en lo que respecta su madurez en ciberseguridad y desarrollo de capacidades, ocupando el tercer lugar encontrándose en el grupo de países con nivel en el Índice Global de Ciberseguridad (IGC) 2024. Esta Estrategia es fundamental para el progreso del país, y busca garantizar la seguridad de las infraestructuras de información crítica, proteger la privacidad de las personas y promover la innovación. Además, genera crecimiento económico al demandar profesionales calificados y posiciona al país como un referente global en ciberseguridad, impulsando el progreso, el bienestar, y garantizando la protección de los derechos fundamentales de las personas desde un abordaje ético.

3_

ESTADO ACTUAL DE LA CIBERSEGURIDAD, DESAFÍOS Y OPORTUNIDADES

Las Tecnologías de la Información y la Comunicación (TIC) revolucionaron la sociedad, impulsando el progreso y el desarrollo en todos los ámbitos. Su omnipresencia en la vida de las personas generó un sinfín de oportunidades, pero también ha expuesto nuevas vulnerabilidades.

Uruguay destaca por su alto índice de conectividad [1] y la creciente adopción de las TIC [2]. Esto trae como contrapartida una mayor exposición de las personas y de las organizaciones a ciberataques. La obsolescencia de muchos sistemas y la falta de conciencia generalizada sobre los riesgos de ciberseguridad agravan esta situación.

Garantizar la ciberseguridad nacional implica un desafío complejo que requiere la colaboración de todos los actores de la sociedad, por lo que es necesario adoptar un enfoque multidisciplinario. Solo a través de un esfuerzo conjunto podremos construir un ciberespacio seguro, abierto, resiliente y confiable, protegiendo los activos de información y garantizando el desarrollo sostenible del país.

3.1 Contexto internacional

El panorama global de la ciberseguridad se transformó radicalmente en las últimas décadas, evolucionando de incidentes aislados a una amenaza sistémica que desafía la estabilidad y la seguridad de naciones enteras. Estos incidentes aislados, aunque inicialmente limitados a organizaciones o individuos específicos, dejan secuelas profundas, erosionando la confianza en el uso de la tecnología y generan pérdidas económicas significativas. La interconexión cada vez mayor de sistemas y la proliferación de dispositivos inteligentes crearon un ciberespacio altamente vulnerable, donde los actores maliciosos encuentran un terreno fértil para llevar a cabo sus operaciones.

La complejidad de las ciberamenazas actuales se ve agravada por la diversidad de amenazas y de actores involucrados, así como su constante evolución. Las tácticas empleadas por estos actores son cada vez más sofisticadas, incluyendo el uso de inteligencia artificial, el aprendizaje automático y otras tecnologías avanzadas para evadir las defensas y maximizar el impacto de sus ataques. El auge de la desinformación no solo afecta la cohesión social, sino que también puede ser utilizado como herramienta de actores malintencionados para desestabilizar la gobernanza y erosionar la credibilidad institucional.

Las consecuencias de los ciberataques trascienden las fronteras nacionales, afectando la economía global e infraestructura crítica de la que dependen diferentes naciones. Asimismo, dichos ataques socavan la seguridad nacional y junto a ella la confianza de las personas que se sienten más vulnerables.

Ante este escenario, la ciberseguridad se convirtió en una prioridad estratégica para los países de todo el mundo. Sin embargo, la naturaleza transnacional de las ciberamenazas exige una respuesta coordinada a nivel internacional. La cooperación entre países es fundamental para compartir información sobre amenazas, desarrollar estándares comunes y fortalecer la capacidad de respuesta a incidentes de ciberseguridad.

En este contexto, se han establecido diversos foros y mecanismos de cooperación internacional, como el Grupo de Trabajo de Composición Abierta (GTCA o OEWG por sus siglas en inglés) sobre seguridad y utilización de la TIC de las Naciones Unidas [3], el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio (MFCS) del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), el cual busca aumentar la cooperación, transparencia, predictibilidad y la estabilidad entre los Estados en el uso del ciberespacio. Sin embargo, aún persisten desafíos significativos, como la falta de un marco normativo internacional unificado y las divergencias entre los intereses nacionales de los diferentes países y la red CSIRT Américas de la OEA/CICTE.

3.2 Contexto nacional

Desde la creación de la Dirección de Seguridad de la Información dentro de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic) y del Centro Nacional de Respuestas a Incidentes de Seguridad Informática (CERTuy), el país ha avanzado en la construcción de un ecosistema que privilegia la seguridad de la información en los entornos digitales y se enfoca, entre otros aspectos, en la concientización de la población, lo que se logró a través de distintas campañas dentro de la iniciativa Seguro Te Conectás [4].

Es así como desde el año 2009 a la fecha, se sancionaron normas legales y reglamentos que contribuyeron a generar un entorno más seguro, definiendo las competencias de Agesic y de otras entidades a cargo de llevar adelante las políticas de seguridad en el Estado, y promoviendo la colaboración con entidades privadas en sectores que por su criticidad ameritan un tratamiento especial.

Un hito de especial relevancia lo constituyó la creación del Marco de Ciberseguridad de Uruguay [5], que tuvo y tiene como principal objetivo el dar lineamientos y buenas prácticas para un abordaje integral de la ciberseguridad.

Por otra parte, las sucesivas Agendas Digitales (actualmente se encuentra vigente la Agenda Uruguay Digital 2025) [6] se constituyen en promotoras de la ciberseguridad a nivel del Estado. Además, y en línea con la profundización del trabajo en ciberseguridad que tiene el país, en 2019 el Banco Interamericano de Desarrollo (BID) aprobó para el país el primer programa sobre ciberseguridad en América Latina: “Fortalecimiento de la Ciberseguridad en Uruguay”.

El ámbito de la ciberseguridad tuvo un nuevo impulso en el año 2023 con la sanción de la Ley N° 20.212, que establece una nueva institucionalidad, genera nuevas competencias, y define legalmente la necesidad de construir este ecosistema a través de una Estrategia Nacional que cuente con la participación de diversos actores y visiones en la materia.

En lo que respecta al posicionamiento del país en relación con otros, actualmente, y de acuerdo con diversos indicadores internacionales, Uruguay tiene un nivel medio de madurez en ciberseguridad. En el Índice Global de Ciberseguridad de 2024 [7] , Uruguay se destaca entre los países que han priorizado la ciberseguridad como un componente esencial para la infraestructura digital del país, así como la protección de personas y organizaciones. En este índice, Uruguay se ubica en el nivel avanzando, con aspectos destacables en la implementación de medidas organizacionales, técnicas y de cooperación internacional, así como avances en el fortalecimiento del marco legal y el desarrollo de capacidades.

De acuerdo con el reporte sobre Ciberseguridad de 2020 [8] realizado por el BID y la OEA, Uruguay progresó en todas las dimensiones desde el 2016, cuando se realizó el primer reporte de Ciberseguridad [9] , y se encuentra liderando en cuatro de las cinco dimensiones a nivel de América Latina y el Caribe: Política y Estrategia de ciberseguridad; Cultura cibernética y sociedad; Educación, capacitación y habilidades en ciberseguridad; y Estándares, organizaciones y tecnologías. Asimismo, el país alcanza la máxima puntuación en temas referidos a la organización y coordinación de respuesta a incidentes; el desarrollo de la temática en el Estado y la confianza de las personas en el uso de servicios en línea, entre otros.

Uruguay realizó avances significativos en materia de ciberseguridad, posicionándose como un referente en la región. Sin embargo, la creciente sofisticación de las ciberamenazas, la escasez de profesionales especializados [10] y una institucionalidad

acorde para abordar la problemática actual, representan desafíos importantes. Los ciberataques pueden tener un impacto devastador en la economía nacional, afectando sectores críticos como el financiero, el sistema de salud o el energético; en el año 2023, el CERTuy atendió 4.968 incidentes, de los cuales el 1% fueron de severidad alta o muy alta [11]. Además, la recurrencia de ciberataques, incluso aquellos de menor impacto individual, tiene un efecto acumulativo que erosiona la confianza y debilita la capacidad de recuperación ante incidentes mayores.

3.3 ¿Por qué es necesaria una Estrategia Nacional de Ciberseguridad?

Ante la creciente sofisticación de las ciberamenazas y la acelerada transformación digital, resulta imperativo contar con una ENC que promueva un esfuerzo coordinado y multidisciplinario de todos los sectores. Esta Estrategia debe adoptar un enfoque integral, sólido y flexible, que permita adaptarse de manera ágil a un ciberespacio en constante evolución. Para construir un ciberespacio seguro, abierto, resiliente y confiable, es fundamental adoptar un enfoque integral que abarque todos los aspectos de la ciberseguridad. Una Estrategia Nacional debe promover la colaboración entre el sector público, el privado, la academia y la sociedad civil, fomentar la investigación y el desarrollo en ciberseguridad, y proteger los datos personales y la privacidad de las personas. Invertir en ciberseguridad es una inversión en el futuro del país. Una Estrategia Nacional sólida no solo protegerá los activos de información y garantizará la continuidad de los servicios críticos, sino que también estimulará el crecimiento económico, atraerá inversiones y fortalecerá la confianza de las personas en el ciberespacio. Al construir una ciberseguridad robusta, se crea un ambiente propicio para la innovación y el desarrollo.

3.4 Alineación con marcos normativos nacionales e internacionales

La Estrategia Nacional de Ciberseguridad contribuye al logro de los objetivos de la Agenda Uruguay Digital buscando garantizar un ciberespacio seguro, abierto, resiliente y confiable. Además, se encuentra en sinergia con diferentes políticas y Estrategias nacionales, y aporta al cumplimiento de tratados internacionales y compromisos país.

Se relaciona con la Política de Defensa Nacional, para garantizar una respuesta coordinada ante ciberamenazas que puedan afectar la seguridad nacional y con la Política Nacional de Gestión Integral del Riesgo de emergencias y desastres en Uruguay 2019-2030 para alinear esfuerzos ante un incidente que, por su magnitud y/o

afectación, genere una emergencia sistémica. Se vincula con la Estrategia Nacional de Inteligencia Artificial para permitir aprovechar las capacidades de esta tecnología en la mejora de la detección y respuesta ante incidentes, así como para desarrollar soluciones innovadoras en ciberseguridad.

Asimismo, busca apoyar el cumplimiento de los marcos asociados a los derechos de privacidad y de protección de datos personales y da soporte a la Estrategia Nacional de Datos aportando criterios y marcos de referencia. Actúa en sinergia con la Estrategia de Ciudadanía Digital la cual complementa la visión de promover la educación y la conciencia de la población en materia de ciberseguridad, empoderando a las personas para el uso seguro y responsable en el entorno digital.

Finalmente, considera los compromisos asumidos a nivel internacional y la necesidad de fortalecer la cooperación en materia de ciberseguridad con otros países.

4_

VISIÓN

La ENC de Uruguay visualiza un futuro donde el país se destaca por un ciberespacio seguro, abierto, resiliente y confiable, que impulse el desarrollo sostenible y proteja los derechos y libertades de todas las personas. Esta visión se materializa a través de una gobernanza sólida y colaborativa, un marco normativo robusto, la capacidad de combatir eficazmente el ciberdelito y la protección de las infraestructuras de información crítica.

Además, la Estrategia aspira a fomentar una cultura de ciberseguridad arraigada en la sociedad, donde todas las personas tengan la capacidad para utilizar la tecnología de manera segura y responsable. Se busca impulsar un ecosistema nacional de ciberseguridad vibrante, con una industria innovadora y competitiva, que posicione a Uruguay como un referente regional en la materia.

Finalmente, la visión incluye una participación activa y comprometida en el escenario internacional, promoviendo la cooperación y la adopción de normas para construir un ciberespacio seguro, abierto, resiliente y confiable para todos.

Esta visión guiará las acciones y políticas en ciberseguridad, asegurando un futuro digital próspero, resiliente, inclusivo y seguro para Uruguay, donde la tecnología sea una herramienta para el progreso y el bienestar de todas las personas, garantizando la protección de los derechos y libertades en el ciberespacio, y promoviendo la confianza y la prosperidad en la era digital.

5

PRINCIPIOS RECTORES

La ENC representa un compromiso de los actores del ecosistema de ciberseguridad para proteger al país, a las personas e instituciones en el ciberespacio.

Mediante una gestión proactiva y coordinada, se pretende fortalecer la resiliencia frente a los desafíos del entorno digital y construir un futuro seguro y confiable para todos. Es con este fin, que se desarrollan el conjunto de principios rectores en los que se funda la ENC. Cada pilar, así como sus líneas de acción deben velar por el respeto de estos. Abarcan al sector público y privado, la academia y la sociedad civil, y deben aplicarse según el contexto, los roles, las obligaciones y responsabilidades correspondientes de los actores según el ordenamiento jurídico.

5.1 Centrado en las personas

Es esencial garantizar a las personas, sin distinción, un nivel de ciberseguridad que les permita llevar a cabo, con confianza y seguridad, actividades personales, sociales y comunitarias en el ciberespacio. Por tanto, toda iniciativa deberá ser respetuosa de la diversidad y resaltar la importancia de los derechos humanos (como la libertad de expresión, el acceso a la información, la preservación de la privacidad y la protección de la propiedad) como base y marco de la ciberseguridad. Construyendo una sociedad digital inclusiva y segura, basada en los principios de equidad y justicia social, donde la tecnología, sea clave y contribuya en el desarrollo pleno de las personas en los diferentes ámbitos y roles sociales.

5.2 Enfoque holístico

La ciberseguridad comprende un conjunto de actores y elementos diversos, que resultan transversales a distintas ciencias y disciplinas. Su alcance trasciende la tecnología y deriva en estructuras complejas que requieren métodos y sistemas que faciliten su gobernanza. La toma de decisiones al respecto de la Estrategia a seguir en materia de ciberseguridad implica necesariamente la participación de las múltiples partes involucradas, lo que exige coordinación y acuerdos.

5.3 Proactividad en la gestión de riesgos

La ENC prioriza la adaptación continua en un ciberespacio que evoluciona constantemente. Esta evolución conlleva un aumento permanente en la sofisticación de las ciberamenazas, que se manifiestan en diversas formas y provienen de diferentes orígenes. Como respuesta se debe adoptar un enfoque proactivo y ágil que se centra en la identificación, evaluación y mitigación de los riesgos relacionados con la ciberseguridad, velando por la integridad, confidencialidad y disponibilidad de la información.

5.4 Articulación, colaboración e inversión

La ciberseguridad en Uruguay requiere un esfuerzo conjunto a nivel nacional e internacional. A nivel nacional, es esencial la articulación y colaboración entre todos los actores (personas, sociedad civil, academia, entidades públicas y privadas) para compartir información y recursos, fortaleciendo así la resiliencia digital. A nivel internacional, Uruguay debe participar activamente en foros multilaterales y regionales para apoyar el desarrollo de un ecosistema de ciberseguridad global. Además, es fundamental invertir en investigación, desarrollo e innovación, así como en la formación de profesionales en la materia.

5.5 Fortalecimiento de la resiliencia digital

La resiliencia digital es fundamental para cualquier transformación digital y para el desarrollo sostenible del país. La ENC se enfoca en fortalecerla en diferentes niveles: desde las personas, pasando por las grandes organizaciones, hasta el país en su conjunto. El objetivo es que todas las partes, sean conscientes de la importancia de la resiliencia digital y cuenten con las herramientas básicas para implementarla.

6_

PILARES

Los pilares de la ENC son componentes clave que conforman la base de un plan integral para proteger el ciberespacio del país. Estos pilares trabajan en conjunto para abordar los diversos desafíos y ciberamenazas, garantizando la ciberseguridad y resiliencia digital. A lo largo del documento, se desarrolla la visión de cada uno, así como el objetivo general, las líneas de acción y las acciones a implementar.

A continuación se presentan los ocho pilares de la Estrategia Nacional de Ciberseguridad:

1. GOBERNANZA

Establecer los mecanismos y políticas para la rectoría de la ciberseguridad a nivel nacional, y definir roles y responsabilidades de los diferentes actores involucrados.

2. MARCO NORMATIVO

Establecer un marco normativo claro, actualizado y articulado para una adecuada gobernanza de la ciberseguridad que permita prevenir, detectar y reaccionar frente a los incidentes de ciberseguridad, investigar y sancionar los ciberdelitos, así como proteger y facilitar el ejercicio de los derechos y las libertades de la ciudadanía en el ciberespacio; abarcando el conjunto de leyes, decretos, regulaciones y estándares que rigen la ciberseguridad en el país.

3. CIBERDELITOS

Desarrollar las capacidades para la prevención, detección, investigación y persecución de los delitos cometidos en el ciberespacio, así como la cooperación internacional y la concientización de la sociedad sobre los riesgos del ciberdelito.

4. CIBERDEFENSA

Fortalecer la ciberdefensa nacional mediante la consolidación de su ecosistema y el desarrollo de capacidades de respuesta de las Fuerzas Armadas (FF.AA.)

5. INFRAESTRUCTURAS DE INFORMACIÓN CRÍTICA

Proteger las infraestructuras de información crítica para el funcionamiento de los sistemas de información que soportan los servicios críticos de posibles ciberataques que puedan afectar su operación y causar graves consecuencias, con un fuerte énfasis en aquellos ataques que puedan ser sistémicos.

6. CULTURA DE LA CIBERSEGURIDAD

Promover la adopción de buenas prácticas y comportamientos seguros en el uso de las tecnologías de la información y la comunicación por parte de las personas, empresas e instituciones. Asimismo, busca fomentar la educación y concientización sobre los riesgos en el ciberespacio y las medidas de prevención.

7. ECOSISTEMA E INDUSTRIA

Impulsar el desarrollo de un ecosistema nacional de ciberseguridad sólido y competitivo, que incluya a empresas, profesionales, investigadores, emprendedores y sociedad civil capaces de desarrollar soluciones innovadoras y servicios de calidad en esta área de forma de contribuir a una industria fuerte y vibrante.

8. POLÍTICA INTERNACIONAL

Establecer los lineamientos para la participación y cooperación con otros países y organismos multilaterales en materia de ciberseguridad, así como fortalecer la posición de Uruguay en el escenario global y para la promoción de un ciberespacio seguro, abierto, resiliente y confiable a nivel mundial.

1. Gobernanza

La ciberseguridad es un desafío global que requiere una respuesta coordinada y efectiva a nivel nacional. Una gobernanza sólida en este ámbito es esencial para proteger la infraestructura de información crítica, la economía y la privacidad de las personas. Alinear a todos los actores involucrados (personas, sociedad civil, academia, entidades públicas y privadas), permite al país desarrollar una postura de ciberseguridad robusta y resiliente.

Objetivo general

Establecer una institucionalidad con capacidades de rectoría y operativas. Definir las directrices y protocolos para que el ecosistema nacional de ciberseguridad funcione de forma cohesiva y eficiente para proteger los intereses nacionales e impulsar el desarrollo seguro y confiable del ciberespacio uruguayo.

Línea 1.1 Fortalecer la estructura de gobernanza nacional

Al establecer una estructura de gobernanza clara y eficiente, se fortalece la ciberseguridad, y se garantiza una respuesta coordinada y efectiva ante las ciberamenazas, fomentando asimismo la cultura de ciberseguridad a nivel nacional.

Acciones

a. Analizar la institucionalidad actual y alternativas para la coordinación, supervisión y ejecución de las políticas nacionales en materia de ciberseguridad.

b. Definir un modelo de gobernanza multinivel que permita establecer una estructura clara y eficiente que distribuya responsabilidades entre los niveles estratégicos (qué hacer), tácticos (cómo hacer) y operativos (hacer), que podrá ser enfocada por sector, asegurando una gobernanza integral y colaborativa.

c. Desarrollar mecanismos de coordinación para el modelo establecido y diseñar directrices, protocolos y procedimientos para facilitar la comunicación, el intercambio de información y la colaboración entre los diferentes actores involucrados en la ciberseguridad a nivel nacional.

Línea 1.2 Ciberseguridad como objetivo de gestión en las organizaciones vinculadas a servicios o sectores críticos del país

Incorporar a la ciberseguridad como un objetivo de gestión en el gobierno corporativo de las organizaciones vinculadas a servicios o sectores críticos del país, generando el compromiso institucional en su implementación y otorgamiento de recursos. Permitirá velar por la prevención, mitigación y manejo de crisis, que redundará en la resiliencia digital del país, siendo pilar de una economía digital sostenible.

Acciones

a. Desarrollar un conjunto de objetivos de gestión en ciberseguridad aplicable a todas las organizaciones vinculadas a servicios o sectores críticos del país.

b. Identificar las organizaciones vinculadas a servicios o sectores críticos del país, evaluando la naturaleza de sus activos de información, su vulnerabilidad, el impacto potencial de un incidente y el contexto en el que operan, y sus interconexiones y dependencias.

c. Establecer la obligatoriedad de implementar estos objetivos de gestión, al tiempo que se promueve la adopción voluntaria por parte de otras organizaciones.

Línea 1.3 Participación del sector privado, la academia y la sociedad civil

Promover la participación activa del sector privado, la academia y la sociedad civil es fundamental para garantizar la efectividad de las medidas de ciberseguridad y para fomentar una cultura de ciberseguridad en toda la sociedad.

Acciones

a. Crear mecanismos de consulta y participación para involucrar a las empresas, organizaciones de la sociedad civil y la academia en el desarrollo e implementación de la Estrategia Nacional de Ciberseguridad.

b. Fomentar la creación de asociaciones público-privadas para abordar los desafíos comunes en materia de ciberseguridad.

Línea 1.4 Fortalecer la comunicación en ciberseguridad

Una comunicación efectiva es clave para la ciberseguridad, esto incluye desde fomentar una cultura de seguridad hasta gestionar incidentes de manera clara y transparente.

Acciones

a. Definir y coordinar un plan de comunicación integral alineado a los objetivos de la presente Estrategia, la concientización, la prevención y respuesta ante ciberamenazas.

b. Crear un programa de vocería para la adecuada comunicación ante incidentes de ciberseguridad destinado a quienes toman decisiones en las entidades públicas.

c. Capacitar en ciberseguridad a los equipos de comunicación sobre cómo abordar el manejo de incidentes a través de herramientas de comunicación.

d. Generar espacios de intercambio con los medios de comunicación.

2. Marco normativo

Una meta fundamental de esta Estrategia es fortalecer el marco legal y regulatorio en materia de ciberseguridad, velando porque éste sea sólido, integrado, actualizado y exhaustivo. Para responder adecuadamente al avance digital, Uruguay requiere diversas adecuaciones en este ámbito, a distintos niveles.

Objetivo general

Desarrollar un marco normativo integrado, coherente y adaptable, que garantice la protección de los sistemas de información, datos y privacidad de las personas, promoviendo la confianza y la resiliencia digital a nivel nacional.

Línea 2.1 Consolidar un marco normativo integral

Se busca establecer un conjunto de leyes, normas, estándares y regulaciones que sirvan como base sólida para toda la actividad relacionada con la ciberseguridad en el país. Se trata de crear un marco legal coherente y completo, que abarque todos los aspectos de la ciberseguridad y contemple la protección de los derechos de las personas, con especial énfasis en la protección de datos personales, sin olvidar cuestiones esenciales como la seguridad de las infraestructuras de información crítica. Al tener un marco legal sólido, se garantiza un entorno más seguro y confiable para todos los actores involucrados.

Acciones

a. Adoptar el Marco de Ciberseguridad de Uruguay adecuado para los sectores y servicios críticos del país contemplando la cadena de suministro, y generar su respectiva regulación cuando corresponda.

b. Asegurar que el marco normativo nacional vele por la ciberseguridad a nivel supraterritorial en concordancia con los estándares y las obligaciones asumidas por el país a nivel internacional.

c. Desarrollar un marco legal que fomente la colaboración entre el sector público y privado para el fortalecimiento de la ciberseguridad nacional.

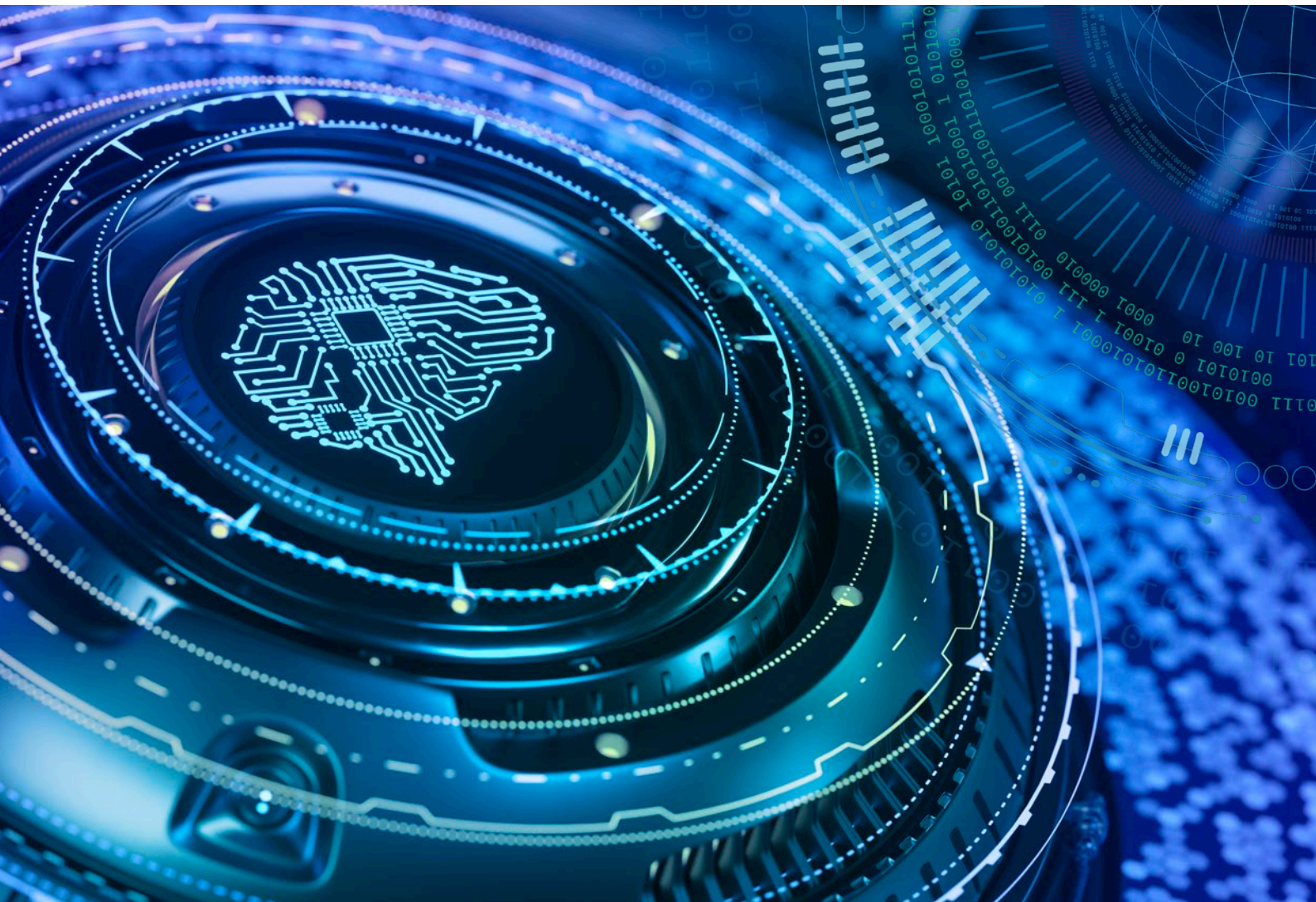
Línea 2.2 Certificación y conformidad

Promover que las organizaciones públicas y privadas, así como los sistemas y procesos relacionados con la ciberseguridad, cumplan con los estándares y requisitos establecidos en el Marco de Ciberseguridad de Uruguay.

Acciones

a. Crear un esquema formal de acreditación y certificación que permita a las empresas acreditadas certificar el cumplimiento de otras organizaciones, y para estas demostrar su adhesión a las mejores prácticas y controles de ciberseguridad definidos por el Marco de Ciberseguridad de Uruguay. Esta certificación servirá como un sello de calidad y confianza, tanto para las propias organizaciones como para sus clientes, socios y la sociedad en general.

b. Implementar mecanismos de evaluación y auditoría para verificar de manera independiente y objetiva el cumplimiento de los requisitos normativos en materia de ciberseguridad, que permitan identificar posibles brechas o debilidades, así como promover la mejora continua en la gestión de riesgos de ciberseguridad.



3. Ciberdelitos

La constante evolución del ciberdelito representa cada vez más una amenaza para los derechos y la seguridad de las personas, así como la estabilidad de las naciones y las sociedades en la era digital. La prevención y el combate efectivo de los ciberdelitos son fundamentales para salvaguardar los activos de información críticos, la privacidad de las personas y la integridad de las instituciones. El combate de los ciberdelitos de manera proactiva y colaborativa es esencial para la prosperidad y seguridad del país, así como la defensa de la soberanía.

Objetivo general

La lucha proactiva y coordinada contra el ciberdelito requiere fortalecer las capacidades técnicas y operativas, mejorar la infraestructura de soporte y establecer mecanismos de monitoreo y seguimiento. Además, busca actuar eficazmente en la recepción de denuncias, procesamiento y condena referidos a este tipo de delitos.

Línea 3.1 Desarrollar las capacidades relativas al combate de los ciberdelitos

Desarrollar la capacidad de Uruguay para prevenir, investigar y perseguir los ciberdelitos con un enfoque integral que involucre la cooperación internacional, tanto privada como pública, el desarrollo de habilidades especializadas, la colaboración interinstitucional y la formación de profesionales en el ámbito de la ciberseguridad.

Acciones

a. Adherir al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), realizando las adecuaciones normativas y protocolares pertinentes que permitan dar cabal cumplimiento.

b. Definir y establecer la forma de colaboración activa entre todos los organismos gubernamentales, autoridades locales, el sector privado y organizaciones internacionales para intercambiar información y recursos en la lucha contra el ciberdelito.

c. Fomentar el desarrollo de carreras de especialización vinculadas a la temática.

Línea 3.2 Fortalecer las infraestructuras de soporte al combate de los ciberdelitos

Dotar de las herramientas y protocolos adecuados que permitan soportar las actividades de combate de los ciberdelitos, velando por la trazabilidad y transparencia.

Acciones

a. Desarrollar capacidades nacionales de forensia digital, que incluya el análisis de la creación de uno o más laboratorios de referencia, alineados con los estándares internacionales, para brindar apoyo a todos los sectores del país en la investigación y análisis de evidencia.

b. Generar capacidades para la investigación y gestión de la evidencia digital en todo el ecosistema específico (Policía, Fiscalía, Poder Judicial), basando los protocolos en estándares internacionales.

c. Facilitar el acceso de las personas a un mecanismo ágil que permita realizar la denuncia de estos delitos.

Línea 3.3 Monitoreo y seguimiento del ciberdelito

La recopilación y análisis de datos relevantes permitirá obtener una visión integral de la situación de los ciberdelitos en el país, al proporcionar información crucial para el diseño e implementación de medidas efectivas en la lucha contra este fenómeno.

Acciones

a. Incorporar, dentro del observatorio de delitos del Ministerio de Interior, los datos referentes a los delitos relacionados con TIC (ciberdelitos, delitos informáticos).

b. Trabajar en la consolidación de todas las fuentes de datos vinculados a delitos relacionados con TIC.

c. Publicar datos abiertos, vinculados a esta temática, en el observatorio.

4. Ciberdefensa

El país deberá estar preparado para responder ante un evento sistémico, como consecuencia de un ciberataque.

Deberán preverse y gestionarse escenarios de incidentes masivos, que afecten las operaciones del país y las personas, en las cuales los recursos en ciberseguridad sean puestos a prueba con una carga y demanda inusual.

Objetivo general

Desarrollar una ciberdefensa nacional basada en la prevención, la detección temprana, la respuesta coordinada, la resiliencia digital, la capacitación y entrenamiento de los actores relevantes y la promoción de una cultura de ciberseguridad en las FF.AA.

Línea 4.1 Consolidar el ecosistema de ciberdefensa nacional

Consolidar la ciberdefensa nacional mediante la identificación y fortalecimiento de las capacidades institucionales para prevenir, detectar y responder a incidentes de ciberseguridad que puedan poner en riesgo la seguridad nacional, la integridad territorial y el bienestar de la población.

Acciones

a. Identificar los organismos que trabajan en la prevención y monitoreo de eventos que anticipen una emergencia sistémica, y las instituciones públicas y privadas que desempeñan un rol en la respuesta a incidentes de ciberseguridad que puedan desencadenar tales emergencias.

b. Establecer los protocolos para la coordinación entre los organismos vinculados a ciberdefensa, para responder eficazmente a incidentes de ciberseguridad que puedan causar interrupciones significativas en infraestructuras críticas. Estos se articularán con la estructura y el marco de gobernanza de ciberseguridad nacional definido en la Línea 1.1 de esta Estrategia.

Línea 4.2 Fortalecer las capacidades de respuesta en ciberdefensa

Es clave para la ciberdefensa del país lograr consolidar una estructura que permita articular las iniciativas en materia de ciberdefensa y ciberseguridad dentro de las Fuerzas Armadas de cara a la protección de la Defensa Nacional, en línea con lo establecido en la Política de Defensa Nacional.

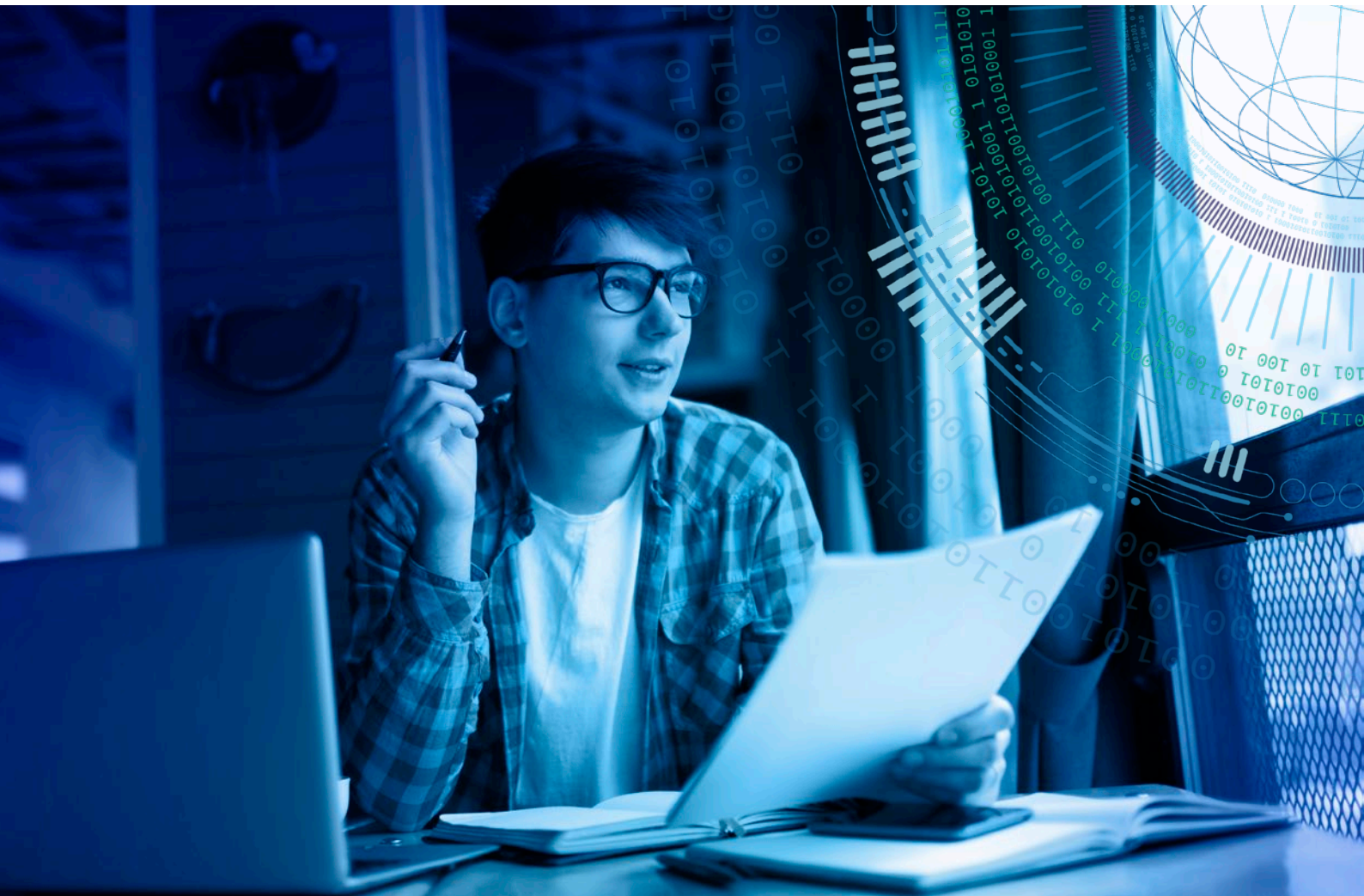
Acciones

a. Analizar las estructuras y mecanismos de ejecución a través de un Comando Conjunto de Ciberdefensa, el cual será definido y operado bajo la órbita del Ministerio de Defensa y las Fuerzas Armadas (FF.AA.)

b. Fortalecer el D-CSIRT mediante la ampliación de su personal para la conformación de equipos técnicos y la adquisición de tecnologías adecuadas.

c. Capacitar y entrenar al personal en la respuesta a incidentes de ciberseguridad para todas las FF.AA. de acuerdo con su perfil y necesidades.

d. Fomentar la colaboración interinstitucional y el intercambio de información con otras entidades de seguridad nacional, especialmente en los niveles operativos de ejecución.



5. Infraestructuras de Información Crítica (IIC)

La protección de las infraestructuras de información crítica es vital, ya que su compromiso podría tener consecuencias devastadoras en la estabilidad del país, mediante la afectación de sus servicios críticos. Para ello, es necesario identificarlas, mejorar sus sistemas de monitoreo y detección, así como gestionar sus incidentes, tanto a nivel organizacional como sectorial, y su resiliencia digital.

Objetivo general

Fortalecer la seguridad y resiliencia digital de las infraestructuras de información crítica del país, mediante la identificación, protección, detección, respuesta y recuperación ante incidentes de ciberseguridad, trabajando con los coreguladores para garantizar la continuidad de los servicios críticos.

Línea 5.1 Definir, identificar y clasificar las IIC

Para poder proteger las IIC se deben establecer criterios claros para determinar qué constituye una IIC, identificar los activos de información críticos dentro de estas infraestructuras y desarrollar una clasificación que permita priorizar y gestionar los riesgos de manera efectiva.

Acciones

a. Identificar, bajo criterios claros, las IIC del país, junto con los actores involucrados en su gestión y administración.

b. Analizar las interconexiones y dependencias entre IIC que permita evaluar el alcance e impacto de un potencial incidente de ciberseguridad.

c. Fomentar junto a los coreguladores la coordinación y cooperación entre los actores involucrados en la gestión de las IIC, promoviendo la colaboración entre el sector público, el sector privado, la academia y la sociedad civil para fortalecer la ciberseguridad.

Línea 5.2 Proteger las IIC

Velar por la seguridad de las IIC mediante la implementación de medidas de prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad.

Acciones

a. Incrementar y fortalecer las capacidades de monitoreo y detección de incidentes en las IIC, esto implica desarrollar capacidades para identificar y responder de manera efectiva a incidentes de ciberseguridad, incluyendo la implementación de sistemas de monitoreo y la creación de equipos especializados en ciberseguridad, impulsando un abordaje sectorial bajo la coordinación del CERTuy.

b. Promover la cultura de la ciberseguridad y la formación en todos los niveles, concientizando y capacitando a los diferentes actores involucrados en la gestión de las IIC sobre la importancia de contar con una infraestructura de TI robusta y segura.

c. Fortalecer los mecanismos de financiamiento para garantizar la implementación de: infraestructuras de TI robustas y seguras por diseño, la remediación de vulnerabilidades relevantes, así como otras medidas de ciberseguridad en las IIC.

d. Contar con fondos de contingencia que permitan abordar emergencias sistémicas en ciberseguridad.

e. Identificar las necesidades de las IIC respecto de la criptografía poscuántica y desarrollar un plan de transición.

Línea 5.3 Fortalecer la resiliencia digital de las IIC

El país deberá contar con infraestructuras de la información crítica que sean robustas y resilientes, preparadas para resistir y recuperarse de incidentes de ciberseguridad, bajo una perspectiva de gestión integral de riesgos. Para ello es necesario asegurar la continuidad de las operaciones de las IIC frente a incidentes o emergencias sistémicas, mediante el desarrollo de planes de recuperación, la adopción de estándares y auditorías, y la promoción de la cultura de ciberseguridad.

Acciones

a. Desarrollar e implementar planes de recuperación ante desastres para las IIC, que permitan la continuidad de las operaciones en caso de incidentes o emergencias sistémicas, garantizando la disponibilidad de los servicios críticos.

b. Establecer ejercicios de simulación que pongan a prueba la resiliencia digital, y que permitan fortalecer la coordinación y cooperación de los actores involucrados en la gestión de las IIC.

c. Establecer alianzas estratégicas con organizaciones (públicas y/o privadas, nacionales o extranjeras), que puedan asistir al país ante incidentes de severidad muy alta o emergencias sistémicas.

d. Desarrollar una nueva infraestructura de clave pública nacional, alineada con los estándares internacionales y resistente a las amenazas de la tecnología cuántica, a través de la colaboración público-privada y la adopción de algoritmos criptográficos poscuánticos.

Línea 5.4 Fortalecer el ecosistema de equipos de monitoreo y respuesta

La capacidad de monitoreo y respuesta, ante incidentes de ciberseguridad, debe ser elevada. Para ello, resulta fundamental reforzar los equipos de monitoreo y respuestas que actualmente existen en los sectores públicos, privados y la academia, así como promover la creación de nuevos equipos cuando corresponda.

Acciones

a. Desarrollo de estándares y guías para CSIRT y SOC, en línea con las mejores prácticas internacionales y, en particular, aquellas promovidas por la red CSIRT Américas de la OEA/CICTE. Esto proporcionará un marco común para la operación de los CSIRT y SOC, asegurando la calidad y eficiencia de sus servicios.

b. Trabajar junto con los coreguladores para establecer obligaciones legales y reglamentarias claras e implementar incentivos y sanciones. Definir las responsabilidades de los diferentes actores y establecer mecanismos para garantizar el cumplimiento de las normas.

c. Generar y establecer una serie de ejercicios anuales específicos para los equipos de monitoreo y respuesta.

6. Cultura de ciberseguridad

Es fundamental generar una cultura en ciberseguridad para promover la higiene digital como norma, así como impulsar las capacitaciones adecuadas para el desarrollo y formación de las personas en esta área.

Objetivo general

Fomentar una cultura de ciberseguridad integral en Uruguay, adaptando la comunicación y la educación a las audiencias, teniendo en consideración la diversidad de la población y, por ende, sus necesidades y prioridades diferenciadas, para fortalecer las capacidades humanas mediante la concientización y la educación. Empoderar a las personas para utilizar las tecnologías de manera segura y responsable protegiendo sus derechos y libertades en el ciberespacio.

Línea 6.1 Concientizar a las personas para el uso seguro de la tecnología

En particular, se vuelve sustancial generar en las personas una cultura de la ciberseguridad desde la más temprana edad con el fin de protegerlas.

Acciones

a. Implementar campañas masivas y focalizadas de concientización en ciberseguridad dirigidas a toda la población, contemplando su adecuación para personas mayores e infancias y otras poblaciones vulnerables. Estas campañas deben considerar temas relevantes (como la violencia en línea), con el objetivo de promover una cultura de ciberseguridad que brinde a las personas las habilidades y los conocimientos necesarios para usar las tecnologías de forma segura. En particular, se deberá desarrollar la Campaña nacional educativa en ciberseguridad prevista en el artículo 9 de la Ley N° 20.327.

b. Promover el uso de identificaciones digitales fuertes y firmas digitales como herramientas fundamentales para proteger la identidad en línea y realizar transacciones seguras. Universalizar el acceso de identificaciones seguras fortalecidas por autenticadores biométricos, certificados digitales u otras, bajo el concepto de autenticación continua, respetando la protección de datos personales, facilitando el uso transfronterizo.

c. Desarrollar un programa de voluntariado para organizaciones, sociedad civil y academia, que colaboren en el fomento de la cultura de ciberseguridad en la sociedad.

Línea 6.2 Desarrollar y fortalecer las capacidades

Lograr captar y retener dentro de una organización el capital humano especializado en ciberseguridad es uno de los desafíos más apremiantes en la actualidad. Esto es fundamental para proteger los activos de información de una organización, salvaguardar la información sensible y garantizar la continuidad de las operaciones en un entorno de ciberamenazas en constante evolución. Cerrar la brecha existente en este campo requerirá un esfuerzo sostenido y la implementación de estrategias a largo plazo. Invertir en el desarrollo y retención de talento en ciberseguridad, de diversos perfiles y talentos, no solo fortalece la resiliencia digital de una organización frente a las ciberamenazas, sino que también representa una inversión estratégica para el futuro.

Acciones

a. Ampliar la oferta de actualización profesional en ciberseguridad para maestros, docentes de los subsistemas de Administración Nacional de Educación Pública (Anep) y educadores, incentivando su realización.

b. Incluir la temática de ciberseguridad de manera obligatoria en los planes de estudio de formación docente.

c. Buscar los mecanismos para expandir significativamente la oferta educativa en ciberseguridad a todos los niveles de formación, desde programas de formación técnica hasta grados y postgrados universitarios; incentivando la formación continua de profesionales.

d. Trabajar en la actualización de los programas y planes de estudio de las carreras técnicas y profesionales, para que se incluyan aspectos de ciberseguridad asociados a su línea de estudio (derecho, diplomacia, salud, comunicación, administración, entre otros).

e. Establecer la obligatoriedad del abordaje de la temática de ciberseguridad establecida en los tramos 2 y 5 del Programa de Educación Básica Integrada (EBI).

f. Promover la generación de redes de apoyo para el desarrollo de capacidades en grupos con situación de desigualdad y vulnerabilidad.

g. Crear un programa de desarrollo de capacidades, a través de la oferta educativa, que permita fortalecer las habilidades y capacidades en el sector público.

Línea 6.3 Prevención y respuesta para las personas

Lograr que las personas estén prevenidas y contar con mecanismos que les permitan reportar y dar atención de manera integral a los incidentes o problemas que los afectan en el ciberespacio es una tarea fundamental para lograr la confianza de la sociedad en los ambientes digitales.

Acciones

a. Creación de un equipo de respuesta con foco en la protección de las personas en línea. Este equipo multidisciplinario se encargará de prevenir, detectar y responder a incidentes que afecten a las personas en línea, brindando asistencia técnica, y generando las alianzas y articulaciones necesarias para una respuesta oportuna.

b. Registrar las incidencias para generar datos que guíen la toma de decisiones y mejoren las campañas de concientización.

c. En colaboración con plataformas digitales y medios de comunicación, evaluar procedimientos de monitoreo y respuesta para identificar y neutralizar desinformación y narrativas maliciosas en tiempo real.

7. Ecosistema e industria de la ciberseguridad

Crear un entorno propicio para el desarrollo de la ciberseguridad en el país, a nivel público y privado, generando sinergias que permitan posicionar a Uruguay como proveedor de servicios y productos seguros.

Objetivo general

Fortalecer el ecosistema nacional de ciberseguridad, promoviendo la innovación, la cooperación público-privada y la adopción de mejores prácticas internacionales, con el objetivo de posicionar a Uruguay como un referente regional en servicios de ciberseguridad y fomentar el desarrollo económico sostenible.

Línea 7.1 Posicionar la industria de ciberseguridad nacional

Desarrollar una industria de ciberseguridad nacional sólida es una inversión estratégica que impulsa el crecimiento económico a largo plazo. Esto se traducirá en mayores exportaciones de servicios, una industria de software más competitiva y segura, y una generación significativa de empleo.

Acciones

a. Mejorar y fortalecer mecanismos que permitan promover la colaboración entre el sector público, el privado, la academia y la sociedad civil, con el fin de mejorar la industria de ciberseguridad.

b. Promover y unificar los esfuerzos para la investigación, desarrollo e innovación (I+D+i) en ciberseguridad, en particular sobre las tecnologías emergentes (como la inteligencia artificial y la computación cuántica), y la suplantación de identidad.

c. Crear un catálogo de productos y servicios de ciberseguridad provistos en el país.

Línea 7.2 Impulsar una industria de TI segura

Una industria local dinámica, capaz de ofrecer soluciones de alta calidad, es fundamental para proteger los intereses nacionales y para impulsar la innovación en el sector. Asimismo, es esencial que la industria del software y servicios a nivel nacional adopten las mejores prácticas internacionales en materia de ciberseguridad, teniendo

como objetivo que sus productos y servicios sean seguros por diseño y contribuyan a elevar el nivel de la ciberseguridad del país.

Acciones

a. Establecer e impulsar los pasos necesarios para que la academia y la industria revaloricen la enseñanza y adopción de la seguridad por diseño.

b. Analizar la viabilidad de crear un ecosistema de incentivos fiscales y financieros para impulsar el desarrollo de la industria nacional de ciberseguridad, y la ciberseguridad en toda la industria de TI (servicios de TI, el desarrollo de software seguro, el cumplimiento de estándares establecidos y la adopción de buenas prácticas en el sector).

c. Generar e impulsar los pasos necesarios para el desarrollo de una industria nacional de TI segura y resiliente, basada en la seguridad por diseño.

d. Establecer los lineamientos para la compra de servicios y software seguro en todos los sectores críticos del país.

Línea 7.3 Mejorar la ciberseguridad de las MiPymes

En Uruguay la gran mayoría de las empresas son MiPymes [12] y por lo general, son un sector bastante desprotegido en lo que a ciberseguridad se refiere. Como base del desarrollo sostenible del país, es crítico lograr que las mismas tengan un nivel de ciberseguridad acorde a la evolución digital del país, por lo que es necesario impulsar e incrementar acciones enfocadas específicamente en este sector.

Acciones

a. Analizar los estudios de campo sobre las MiPymes y en base a ellos evaluar la elaboración estrategias de sensibilización y protección ante los principales riesgos de ciberseguridad a los que están expuestos.

b. Estudiar mecanismos para el desarrollo de programas de acceso a servicios y herramientas de ciberseguridad con foco en las MiPymes.

Línea 7.4 Evolucionar el ecosistema de firma e identificación digital para fortalecer el gobierno digital

Impulsar el uso de la firma y la identificación digital a nivel nacional y promover el reconocimiento y uso a nivel regional e internacional. Desarrollar ecosistemas de Autoridades de Competencia involucrando a la ciudadanía, la industria, el Estado y la academia.

Acciones

a. Incentivar, facilitar y mejorar el uso de la firma y la identificación digital en el ecosistema.

b. Avanzar en el reconocimiento internacional de la identificación y firma digital desarrollando casos de uso específicos con impacto en la ciudadanía.

c. Desarrollar el ecosistema de credenciales verificables y sellos de competencia a nivel nacional.

d. Elaborar un programa de acceso a herramientas y recursos.

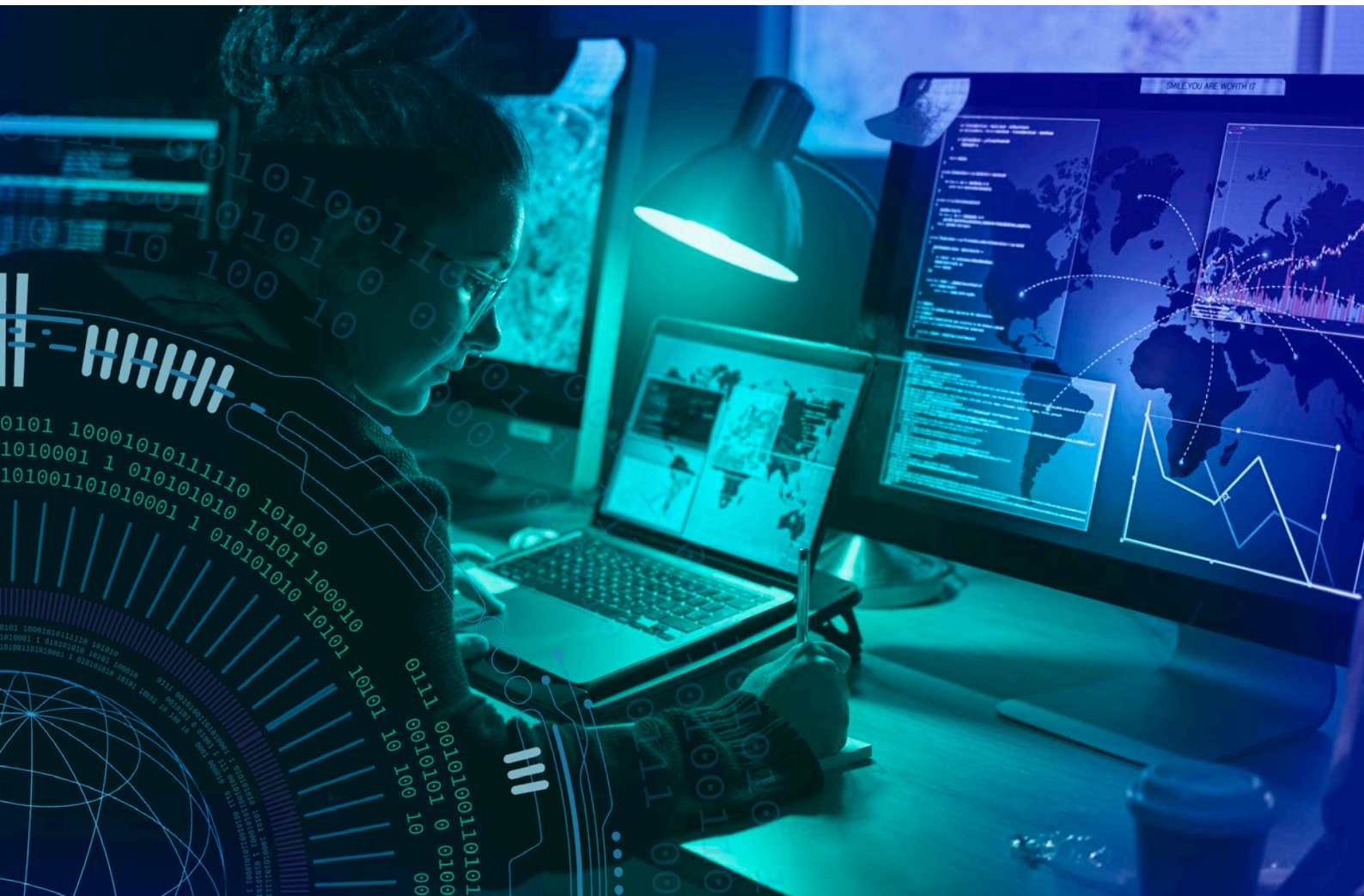
8. Política internacional

Las ciberamenazas no tienen fronteras. La cooperación, a través de la promoción de alianzas, acuerdos y tratados de ciberseguridad a nivel regional e internacional es crucial para abordar amenazas y para establecer normas y estándares comunes que promuevan un ciberespacio más seguro a nivel global. La colaboración regional e internacional permite una respuesta más efectiva y coherente ante ciberamenazas transnacionales.

En su accionar a nivel internacional, Uruguay trabajará para promover un ciberespacio seguro, abierto, resiliente y confiable, basado en el respeto a los principios de la Carta de las Naciones Unidas y el Derecho Internacional, incluyendo el Derecho Internacional de los Derechos Humanos y el Derecho Internacional Humanitario.

Objetivo general

Fortalecer la posición de Uruguay como actor proactivo y confiable en la gobernanza del ciberespacio a nivel regional e internacional, promoviendo la cooperación bilateral y multilateral, y la adopción de normas y estándares internacionales para mejorar el desarrollo de las capacidades y de la industria de ciberseguridad nacional.



Línea 8.1 Desarrollar las capacidades nacionales para un abordaje internacional de la ciberseguridad

El acelerado crecimiento de iniciativas y espacios multilaterales y regionales en los que se aborda la temática de la ciberseguridad requiere de una mayor formación y dedicación dentro de las diferentes instituciones con competencia en la materia. En particular el Ministerio de Relaciones Exteriores, en tanto órgano encargado de la política exterior del Uruguay, deberá desarrollar las siguientes acciones.

Acciones

a. Establecer y formar un equipo diplomático a cargo de gestionar los temas vinculados a la ciberseguridad del país, en coordinación con Agesic.

b. Coordinar con las instituciones nacionales competentes la Política Exterior del Uruguay para el ciberespacio.

c. Implementar un mecanismo formal de transferencia de conocimiento que permita que las lecciones aprendidas, mejores prácticas y avances obtenidos en espacios multilaterales sean compartidos de manera efectiva por las instituciones nacionales competentes en la Política Exterior del Uruguay para el ciberespacio.

Línea 8.2 Incrementar la presencia y participación de Uruguay en espacios regionales e internacionales

El intercambio y participación regional e internacional, tanto a nivel técnico como político, es vital para un adecuado abordaje de las medidas de ciberseguridad a nivel nacional. En tal sentido, resulta fundamental la participación en los espacios promovidos por los organismos, foros y grupos de trabajo multilaterales, que puedan resultar pertinentes de acuerdo con los intereses del país.

Acciones

a. Reforzar la participación de Uruguay en los espacios regionales e internacionales relevantes en materia de ciberseguridad, a través de la conformación de delegaciones interinstitucionales que potencien el intercambio sustantivo en la materia, de acuerdo con los intereses nacionales.

b. Fomentar la cooperación en materia de ciberseguridad.

c. Evaluar la adhesión del país a la normativa y estándares internacionales en concordancia con los principios de la Política Exterior para el ciberespacio.

7

PROCESO DE IMPLEMENTACIÓN Y SEGUIMIENTO

El proceso de implementación y seguimiento de la Estrategia Nacional de Ciberseguridad asegura el cumplimiento de sus objetivos, facilita el monitoreo, la rendición de cuentas y orienta el presupuesto y la inversión de recursos en función de los compromisos asumidos.

Este proceso se llevará adelante con el apoyo del Comité de Gestión de la ENC tal como lo establece el artículo 83 de la Ley N° 20.212.

7.1 Plan de acción

Se elaborará un plan de acción que detalle las acciones para implementar las líneas de acción propuestas en cada uno de los ocho pilares y defina responsabilidades de liderazgo y apoyo.

7.2 Monitoreo y evaluación

La implementación de la ENC es un proceso continuo y dinámico que requiere un monitoreo constante y una evaluación rigurosa para garantizar su efectividad y adaptabilidad a un entorno en constante evolución.

El objetivo estratégico de monitoreo y evaluación de la ENC del Uruguay es establecer un marco de supervisión que permita medir el progreso, identificar áreas de mejora para asegurar que la Estrategia cumpla con sus objetivos y metas y se adapte a la evolución de las amenazas. Se enfoca en la recopilación de datos, la evaluación periódica de desempeño y el análisis de tendencias para asegurar que la Estrategia se mantenga relevante y eficaz.

El proceso de definición de monitoreo y evaluación comenzará con un taller inicial dirigido a los representantes clave de cada objetivo. El fin principal es definir los mecanismos de monitoreo y evaluación partiendo de la siguiente propuesta:

- Definir y establecer indicadores clave de desempeño (KPI por su sigla en inglés) que reflejen los objetivos y metas de la Estrategia, lo que facilitará la medición y evaluación de su impacto.
- Se implementará una herramienta de monitoreo público a través de la cual los responsables de liderar cada una de las acciones informarán semestralmente sobre sus avances.
- Se difundirán los logros alcanzados regularmente a todas las partes interesadas.

7.3 Período de vigencia de la Estrategia

El período de vigencia de la Estrategia es 2024-2030 y tendrá una revisión de medio término.

8_

ANEXOS

8.1 Anexo I - Ciberseguridad en Uruguay, datos e indicadores

8.1.1 Datos estadísticos

Incidentes de seguridad informática – CERTuy
Ciberseguridad en las empresas uruguayas – Datasec y Grupo Radar

Índices internacionales sobre madurez en ciberseguridad

Reporte de ciberseguridad 2020 – OEA y BID
Reporte de ciberseguridad 2016 – OEA y BID
Índice Global de Ciberseguridad – ITU
Índice Nacional de Ciberseguridad– Estonia

8.1.2 Estudios de la ciberseguridad en Uruguay

Caracterización de la demanda de formación en ciberseguridad
Formación en ciberseguridad
Informe Ciberseguridad: empresas y sector público 2021
Informe 2020: Ciberseguridad en Uruguay

8.2 Anexo II - Normativa vigente

A continuación, se listan las leyes y decretos que sustentan la ciberseguridad en el país, y aquellas que tienen una vinculación estrecha con la temática. Asimismo, se incluyen estatutos, planes, políticas y demás definiciones que marcan el curso de las temáticas en materia de ciberseguridad.

8.2.1 Seguridad de la información y ciberseguridad

Consejo Asesor Honorario de Seguridad de la Información (CAHSI)
Ley N° 18.172 Art. 119 - Ley N° 20.212 Art. 84

Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)
Ley N° 18.362 Art. 73

Creación de la Dirección de Seguridad de la Información - Ley N° 18.719 Art. 149

Obligaciones de entidades públicas y privadas vinculadas a servicios o sectores críticos del país. - Ley N° 20.212 Art. 78

Competencias de Agesic ante incumplimientos de obligaciones. - Ley N° 20.212 Art. 79

Registro Nacional de Incidentes de Ciberseguridad. - Ley N° 20.212 Art. 80

Compras estatales y ciberseguridad. - Ley N° 20.212 Art. 81

Comité de Gestión de la Estrategia Nacional de Ciberseguridad. - Ley N° 20.212 Art. 83

Obligaciones vinculadas a seguridad de la información en la Administración Central
Decreto N° 66/025 - Decreto N° 92/014

Agenda Uruguay Digital (AUD) 2025

8.2.2 Ciberdelitos

Falsificación de documento electrónico. - Ley N° 18.600 Art. 4

Divulgación de imágenes íntimas. - Ley N° 19.580 Art. 92

Grooming - Código penal Art 277 bis

Regulación para la prevención y represión de la ciberdelincuencia. - Ley N° 20.327

Unidad de Cibercrimen de la Dirección de Investigaciones de la Policía Nacional
Ley N° 19.996 Art. 107

Convenio de Cooperación Iberoamericano en Materia de Ciberdelincuencia
Ley N° 20.004

8.2.3 Ciberseguridad en el contexto de la defensa nacional

Política Militar de Defensa. - Decreto N° 129/016

Decreto Reservado N° 44/018

Política de Defensa Nacional 2020-2025 - Decreto N° 371/020

8.2.4 Identificación electrónica

Documento y firma electrónicos
Ley N° 18.600 - Decreto N° 276/013 - Decreto N° 71/025

8.2.5 Protección de datos personales

Protección de datos personales
Ley N° 18.331 - Decreto N° 414/009 - Decreto N° 64/020

8.2.6 Ciberseguridad en el contexto educativo

Programa de educación básica integrada 2023 (EBI)
Se contempla la formación en Ciberseguridad en el componente Técnico-Tecnológico tramo 2 (primer y segundo año) y tramo 5 (séptimo y octavo año).

Oferta educativa en ciberseguridad
Oferta educativa disponible en carreras terciarias, certificaciones y posgrados.

8.2.7 Ciberseguridad en el contexto de una emergencia nacional

Política Nacional de Gestión Integral del Riesgo de emergencias y desastres en Uruguay 2019-2030 - Decreto N° 66/020,

8.3 Anexo III - Glosario

8.3.1 Glosario de términos de ciberseguridad

Seguro te Conectás
Marco de Ciberseguridad de Uruguay

8.3.2 Glosario de términos para la Estrategia Nacional de Ciberseguridad

» ***Activos de información***
Datos o información que tienen valor para una organización.

» ***Activos de información críticos***
Activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios críticos.

» ***Cadena de suministro***
Conjunto de recursos y procesos vinculados entre múltiples niveles de organizaciones, cada uno de los cuales es un adquirente, que comienza con la obtención de productos y servicios y se extiende a lo largo de su ciclo de vida. [13]

» ***Ciberataque***
Cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, denegar, degradar o destruir los recursos del sistema de información o la información misma. [13]

» ***Ciberdefensa***
Capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia. [14]

» ***Ciberdelincuencia***
Se entiende cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación. [15]

» ***Ciberdelito***
Toda acción antijurídica y culpable a través de vías informáticas que tiene como objetivo causar perjuicio de cualquier tipo por medios electrónicos y redes de internet en “delitos computacionales”, de acuerdo con los tipos penales encuadrados en el código penal y leyes especiales. Decreto N° 84/019, de 25 de marzo de 2019, Art. 100

» ***Ciberespacio***
La red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, computadoras, sistemas de información, sistemas de control industrial, redes y procesadores y controladores integrados. [13]

» ***Ciberseguridad***
Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

» ***CSIRT - Equipo de respuesta a incidentes de seguridad informática***
Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de ciberseguridad.

» ***Cultura de ciberseguridad***
Conjunto de valores, comportamientos y prácticas adoptadas por una persona u organización con el objetivo de proteger la integridad, confidencialidad y disponibilidad de la información en el ciberespacio.

» ***Ecosistema de autoridades de competencia***
Es el conjunto de entidades y actores responsables de regular, supervisar y promover la competencia en el ámbito de los servicios de confianza basados en el uso de certificados digitales en una Infraestructura de Claves Pública (PKI por sus siglas en inglés) reconocida por normativa nacional. Estos servicios incluyen la firma electrónica avanzada, el sello electrónico, el sellado de tiempo, la autenticación de sitios web y la preservación de documentos electrónicos.

» ***Ecosistema nacional de ciberseguridad***
Se compone de todos los actores, organizaciones, infraestructuras, procesos y tecnologías que contribuyen a la ciberseguridad del país. Esto incluye, organizaciones del sector privado y público, academia y sociedad civil.

» ***Emergencia sistémica***
Se refiere a una serie de incidentes que tienen el potencial de causar una interrupción significativa o un daño generalizado a infraestructuras críticas, infraestructuras de información crítica, servicios críticos, o a la estabilidad económica y social del país. Esto puede ser el resultado de ciberataques a gran escala, fallos tecnológicos masivos, o la explotación de vulnerabilidades críticas que afectan a múltiples sectores interconectados.

» ***Higiene digital***
Conjunto de prácticas para mantener segura la información en Internet.

» ***Incidente de ciberseguridad***
Uno o múltiples eventos de ciberseguridad relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones.

- ***Infraestructuras de información crítica (IIC)***
  Sistemas de información que soportan los servicios críticos y cuya afectación tendría un impacto debilitante en la seguridad de la información de los servicios críticos.

- ***Infraestructura de TI***
  Incluye una amplia gama de elementos, tanto físicos como virtuales:

  - ***Hardware:*** Servidores, computadoras, dispositivos de almacenamiento, dispositivos de red (routers, switches), impresoras, etc.
  - ***Software:*** Sistemas operativos, aplicaciones empresariales, software de gestión de bases de datos, software de seguridad, etc.
  - ***Red:*** Conexiones de red, ancho de banda, firewall, etc. que permiten la comunicación entre los diferentes componentes.
  - ***Instalaciones:*** Centros de datos, salas de servidores, sistemas de refrigeración, etc.
  - ***Servicios:*** Servicios de TI como soporte técnico, administración de sistemas, consultoría, etc.

- ***IoT***
  Internet de las cosas (IoT por su siglas en inglés).
  Dispositivos de IoT refiere a todos los aparatos (lámparas, heladeras, routers, monitores, relojes, etc.) que se conectan a internet.

- ***Ransomware***
  Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella.

- ***Resiliencia***
  La capacidad de prepararse y adaptarse a condiciones cambiantes y, resistir y recuperarse rápidamente de las perturbaciones. La resiliencia incluye la capacidad de resistir y recuperarse de ataques deliberados, accidentes o amenazas o incidentes naturales. [13]

- ***Riesgo***
  Potencial que una amenaza dada explote vulnerabilidades de un activo o grupo de activos, ocasionando un daño.

» ***Sectores críticos***
Salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agroindustria, industria, servicios públicos, banca y servicios financieros, defensa, y otros sectores de interés que oportunamente determine el Poder Ejecutivo, con el asesoramiento de Agesic.

» ***Seguridad de la información***
Preservación de la confidencialidad, integridad y disponibilidad de la información. Puede involucrar otras propiedades tales como: autenticidad, responsabilidad sobre acciones y decisiones, no repudio y confiabilidad.

» ***Seguridad por diseño***
Del inglés "Security by Design" (SbD), es un enfoque proactivo para el desarrollo de sistemas y productos que busca integrar la seguridad desde las etapas iniciales del proceso de diseño.

» ***Servicios críticos***
Servicios fundamentales para la operación del gobierno y la economía del país, pertenecientes a los sectores críticos, cualquier otro servicio que afecte a más del 30% (treinta por ciento) de la población, y otros servicios de interés que oportunamente determine el Poder Ejecutivo, con el asesoramiento de Agesic.

» ***Sistema de información***
Conjunto interconectado de recursos de información bajo el mismo control de gestión directo que comparte una funcionalidad común (hardware, software, activos de información, comunicaciones y personas, entre otros).

» ***Sistema informático***
Los ordenadores y redes de comunicación electrónica, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

» ***SOC - Centro de Operaciones de Ciberseguridad***
Security Operations Center (SOC) es un equipo de profesionales de ciberseguridad que supervisa toda la infraestructura tecnológica de una organización o conjunto de organizaciones, las 24 horas del día, los 7 días de la semana, para detectar eventos de ciberseguridad en tiempo real y abordarlos de la forma más rápida y eficaz posible.

8.3.3 Glosario de acrónimos

ABPU - Asociación de Bancos Privados del Uruguay

AGESIC - Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento

AIN - Auditoría Interna de la Nación

AMEPP - Agencia de Monitoreo y Evaluación de Políticas Públicas

ANCAP - Administración Nacional de Combustibles, Alcohol y Portland

ANDEBU - Asociación Nacional de Editores de Periódicos del Uruguay

ANII - Agencia Nacional de Investigación e Innovación

ANP - Administración Nacional de Puertos

ANTEL - Administración Nacional de Telecomunicaciones

ASSE - Administración de Servicios de Salud del Estado

BBVA - Banco Bilbao Vizcaya Argentaria

BCU - Banco Central del Uruguay

BID - Banco Interamericano de Desarrollo

BPS - Banco de Previsión Social

BROU - Banco República Oriental del Uruguay

CCE - Confederación de Cámaras Empresariales

CGE - Comité de Gestión de la Estrategia Nacional de Ciberseguridad

CGN - Contaduría General de la Nación

CSIRT - Computer Incident Response Team

CTM - Comisión Técnica Mixta de Salto Grande

CUTI - Cámara Uruguaya de Tecnologías de la Información

D-CSIRT - CSIRT del Ministerio de Defensa Nacional

DGI - Dirección General Impositiva

DNA - Dirección Nacional de Aduanas

DINACIA - Dirección Nacional de Aviación Civil e Infraestructura Aeronáutica

DINATEL - Dirección Nacional de Telecomunicaciones

DIPN - Dirección de Investigaciones de la Policía Nacional

DNIC - Dirección Nacional de Identificación Civil

DNSFFAA - Dirección Nacional de Sanidad de las Fuerzas Armadas

ENC - Estrategia Nacional de Ciberseguridad

ESMADE - Estado Mayor de la Defensa

FAU - Fuerza Aérea Uruguaya

FGN - Fiscalía General de la Nación

I+D+I - Investigación, Desarrollo e innovación

IAU - Instituto Antártico Uruguayo

IM - Intendencia de Montevideo

IMES - Instituto Militar de Estudios Superiores

INDDHH - Institución Nacional de Derechos Humanos y Defensoría del Pueblo

IOT - Internet of Things (Internet de las cosas)

KPI - Key Performance Indicator (indicador clave de desempeño)

MDN - Ministerio de Defensa Nacional

MEC - Ministerio de Educación y Cultura

MGAP - Ministerio de Ganadería, Agricultura y Pesca

MI - Ministerio del Interior

MIEM - Ministerio de Industria, Energía y Minería

MRREE - Ministerio de Relaciones Exteriores

OEA - Organización de Estados Americanos

PNUD - Programa de las Naciones Unidas para el Desarrollo

SIEE - Secretaría de Inteligencia Estratégica del Estado

SINAE - Sistema Nacional de Emergencias

SOC - Security Operations Center

TI - Tecnologías de la Información

TIC - Tecnologías de la Información y las Comunicaciones

UAIP - Unidad de Acceso a la Información Pública

UDE - Universidad de la Empresa

UDELAR - Universidad de la República

UM - Universidad de Montevideo

URCDP - Unidad Reguladora y de Control de Datos Personales

URSEC - Unidad Reguladora de Servicios de Comunicación

UTE - Administración Nacional de Usinas y Trasmisiones Eléctricas

UTEC - Universidad Tecnológica - Uruguay

UTU - Universidad del Trabajo del Uruguay

8.4 Anexo IV - Proceso de cocreación

La ENC se construye mediante un proceso de cocreación inclusivo y participativo. Este enfoque garantiza que la Estrategia responda a las necesidades y realidades específicas del país, al involucrar a una amplia gama de actores claves.

El proceso de cocreación se inició con la elaboración de un primer borrador a cargo del Consejo Asesor Honorario de Seguridad de la Información (CAHSI). Este documento se construyó a partir de charlas formativas impartidas por LAC4 y luego fue enriquecido a través de mesas de trabajo que involucraron a diversos actores, como organismos públicos, sector privado, academia y sociedad civil. A través de estas instancias se recopilaron aportes que permitieron ajustar y mejorar la propuesta inicial. El resultado de este proceso colaborativo fue puesto en consulta pública a través de la Plataforma de Participación Ciudadana Digital de Agesic. Finalizada esta instancia, se generó la versión final de la Estrategia Nacional de Ciberseguridad de Uruguay.

Fases del proceso

En función de los objetivos planteados para la ENC, se estructura su desarrollo a través de un proceso de cocreación de seis etapas.

Etapa 1. **Definiciones estratégicas**

SETIEMBRE 2023 A MARZO 2024

- Estudio de Estrategias nacionales de ciberseguridad de otros países.
- Definición de principios rectores.
- Elaboración de propuesta borrador ENC.
- Diseño de propuesta del proceso participativo.
- Validación de la dirección de Agesic de las propuestas de borrador ENC y el proceso de creación.
- Plan de comunicación.
- Plan de trabajo y cronograma.

Etapa 2 **Lanzamiento del proceso de cocreación**

ABRIL A MAYO 2024

- Revisión del borrador de la ENC por parte del Comité de Gestión de la Estrategia Nacional de Ciberseguridad dispuesto por la Ley N° 20.212
- Lanzamiento del proceso de cocreación de la Estrategia Nacional de Ciberseguridad.

Etapa 3 **Aportes y análisis de viabilidad**

JUNIO A AGOSTO 2024

- Recepción de aportes por parte de las personas expertas, las mesas multiactor y los organismos internacionales.
- Análisis de viabilidad y priorización con Comité de Gestión de la Estrategia Nacional de Ciberseguridad.
- Elaboración de versión para consulta pública ENC.

Etapa 4 **Consulta pública**

SETIEMBRE 2024

- Publicación de versión de la ENC para consulta pública.
- Consulta pública en la Plataforma de Participación Ciudadana Digital.
- Sistematización de aportes de la consulta pública y respuesta.
- Diseño de la Estrategia de comunicación y difusión.
- Elaboración de la versión final.

Etapa 5 **Aprobación**

SETIEMBRE A OCTUBRE 2024

- Presentación y aprobación de la versión final a Consejo Asesor Honorario de Seguridad de la Información (CAHSI) y Comité de Gestión de la Estrategia Nacional de Ciberseguridad.

Etapa 6 **Presentación y difusión**

OCTUBRE A DICIEMBRE 2024

- Publicación y presentación de la ENC.
- Implementación de la Estrategia de comunicación y difusión.
- Inicio del proceso de seguimiento, monitoreo y evaluación.

8.4.1 Participantes

En el proceso se realizaron 10 mesas de trabajo y el documento resultante fue puesto en consulta pública. En dichas instancias participaron más de 300 personas de diversas organizaciones públicas y privadas, así como la sociedad civil y la academia.

Sector industria: Atos Uruguay, CUTI, Datasec, Deloitte, Equifax, Endovas, EY Uruguay, Fortinet, GeneXus Consulting, Getnet Uruguay, Globant, Grant Thornton, HG, ISACA, ISBEL, ITC, LIDECO, Matriz, Microsoft, PLEXO, QoxIT, SeCIU, Security Advisor, Sonda, Teledata, Tilo, Tilsor, Urudata, VaFirma, VCR, Willinn.

Sector legal: Dentons, Ferrere.

Sector educativo: Ceibal, CLAEH, Holberton School, ORT, UCU, UDE, UDELAR (Facultad de Derecho, Facultad de ingeniería), UM, UNIT, UTEC, UTU.

Sector público: Ancap, ANII, ANP, ASSE, BPS, Correo Uruguayo, FGN, Ibirapitá, IM, INDDHH, MDN (Armada Nacional, FAU, Ejército Nacional, Esmade, Dinacia, DNSFFAA, IAU, Imes), MEC, MEF (DNA, AIN, CGN, DGI), MI (DIPN, DNIC), Miem (DGS, Dinatel), MGAP, MRREE, Parlamento, Poder Judicial, Presidencia de la República (Agesic, AMEPP, DGS, SIEE), UAIP, URCDP, URSEC, Uruguay XXI, UTE.

Sector financiero y sistema de pagos: Abitab, ABPU, Santander, Scotiabank, Brou, Bamboo Paymen, BBVA, BCU, Total Net, Patria Investments, Prex, Galileo Latam.

Sector telecomunicaciones: ANDEBU, ANTEL, Claro, Flow, Montecable, Movistar, SpaceX, Telecom, Telefónica.

Sociedad civil: Data Uruguay (Datysoc), ISOC, OWASP.

Organismos internacionales, extranjeros: BID, CSIRT Chile, CTM Salto Grande, LACNIC, OEA, PNUD.

9 REFERENCIAS

[1] Asociación Global del Ecosistema Móvil (GSMA), «Índice de Conectividad Móvil,»

[2] Resultados del Índice de Desarrollo de las TIC (ITU), 2024

[3] Naciones Unidas, «OEWG on security of and in the use of ICT.

[4] Agesic, «Seguro Te Conectás.

[5] Agesic, «Marco de Ciberseguridad de Uruguay,»

[6] Agesic, «Agenda Uruguay Digital,»

[7] ITU, «Indice Global de Ciberseguridad,» 2024.

[8] OEA, BID, «Reporte Ciberseguridad 2020. Riesgos, avances y el camino a seguir en America Latina y el Caribe,» 2020.

[9] OEA, BID, «Reporte de Ciberseguridad,» 2016.

[10] Agesic, «Informe sobre ciberseguridad en Uruguay,» 2020.

[11] CERTuy, «Estadisticas de incidentes de seguridad informática,»

[12] ANDE, «Monitor MiPymes,»

[13] NIST, «Glosario,»

[14] *Convenio Iberoamericano de cooperaicón sobre Investigación, Asegurameiento y Otención de Prueba en materia de Ciberdelincuencia,* 2014.

[15] M. Pecoy Taque, Ciberdelitos y cibrecriminalidad, Montevideo: La Ley Uruguay, 2024.

Uruguay
Presidencia

agesic

gub.uy/agesic