ESTRATEGIA BRASILEÑA DE CIBERSEGURIDAD (E-Ciber)

2025

GOBIERNO DE BRASIL

BRASIL

JUNTO AL PUEBLO BRASILEÑO

E-Ciber

Presentación

El Gabinete de Seguridad Institucional de la Presidencia de la República (GSI/PR) presenta la nueva **Estrategia Nacional de Ciberseguridad (E-Ciber)**, reglamentada por el Decreto nº 12.573/2025, que orienta los esfuerzos destinados a elevar la seguridad y la resiliencia cibernéticas nacionales.

La estrategia fue elaborada con base en las propuestas del **Comité Nacional de Ciberseguridad (CNCiber)**, integrado por 25 miembros, de los cuales 16 son representantes gubernamentales y 9 de la sociedad civil.

Estructurada en cuatro ejes interconectados, la E-Ciber promueve:

1. Acciones para ampliar la protección y la concienciación de la ciudadanía y de la sociedad, mediante iniciativas de educación formal e informal para todas las edades;
2. El fortalecimiento de la seguridad y de la resiliencia de los servicios esenciales e infraestructuras críticas, apoyando la transformación digital en curso y mitigando riesgos;
3. La integración y cooperación entre organismos e instituciones, en Brasil y en el exterior; y
4. Medidas destinadas a garantizar la soberanía nacional y la gobernanza de la ciberseguridad.

Se trata de la segunda estrategia nacional de ciberseguridad de Brasil, que incorpora características de tercera generación, comparables a las de las naciones líderes en la materia, alineando al país con las prácticas más avanzadas a nivel mundial, en conformidad con estudios del Banco Interamericano de Desarrollo (BID).

La E-Ciber establece 40 acciones estratégicas, desglosadas en **Planes Nacionales de Ciberseguridad**, que serán periódicamente actualizados por el CNCiber. El documento representa un avance significativo en el ámbito de la ciberseguridad, en la resiliencia de los servicios esenciales e infraestructuras críticas y en la consolidación de la soberanía digital de Brasil.

Gabinete de Seguridad Institucional
Presidencia de la República

Confira el decreto 12.573/2025

RESUMEN

Estrategia Nacional de Ciberseguridad (E-Ciber) 2025

En 2023 fueron instituidos la Política Nacional de Ciberseguridad (PNCiber) y el Comité Nacional de Ciberseguridad (CNCiber), con la participación de representantes del gobierno, del sector académico, de la sociedad civil y del empresariado. El objetivo fue perfeccionar la ciberseguridad y la ciberresiliencia del país, así como promover la cooperación nacional e internacional en estos temas.

Corresponde al CNCiber la elaboración de la propuesta que fundamentó la presente estrategia, que busca delinear las mejores directrices para alcanzar los objetivos establecidos en la PNCiber. Para ello, el Comité definió un conjunto de prioridades orientadas a atender las necesidades más urgentes de Brasil en el ámbito de la ciberseguridad, garantizando una asignación más eficaz de los recursos en el corto y mediano plazos, dentro de un proceso gradual y evolutivo. Asimismo, compete al CNCiber la gestión de riesgos durante la implementación de toda esta política pública y, en consecuencia, de la E-Ciber. El Comité vislumbra la creación de un organismo para la gobernanza de la ciberseguridad nacional, que será responsable de coordinar las acciones y de establecer mecanismos de regulación, supervisión, coordinación y control en la materia, incluyendo la protección de los servicios esenciales y de las infraestructuras críticas, así como la gestión de cibercrisis relevantes.

1 Panorama cibernético mundial

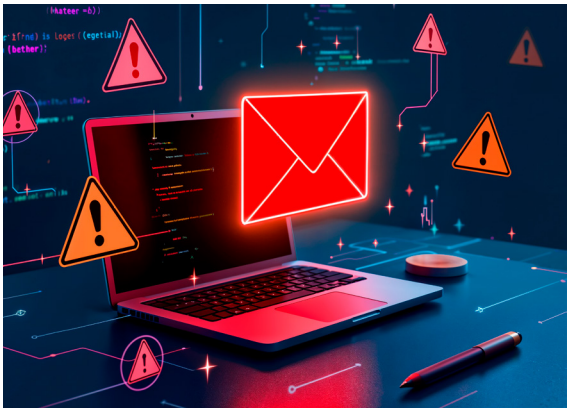
En enero de 2023, el Foro Económico Mundial (WEF) presentó su Informe de Riesgos Globales, en el que afirmó que "la tecnología exacerbará las desigualdades, mientras que los riesgos de ciberseguridad continuarán siendo una preocupación constante". El informe también señaló que el delito y la inseguridad cibernéticos pasaban a integrar la lista de los 10 principales riesgos globales más graves de la próxima década.

En enero de 2024, el WEF actualizó dicho informe, situando la ciberseguridad en el quinto lugar entre los mayores riesgos globales. También indicó que las pérdidas económicas mundiales derivadas de ciberincidentes podían estimarse en torno al 14% del Producto Interno Bruto (PIB) global, lo que, proyectado al PIB brasileño de 2024, corresponde a aproximadamente 1,5 billones de reales.

En la edición de 2025, el informe destacó la ciberespionaje y la ciberguerra como la quinta principal preocupación en un horizonte de dos años, percepción probablemente influenciada por el agravamiento de las tensiones económicas y políticas, así como por los conflictos militares contemporáneos.

A medida que el ciberespacio se consolida como la arena preferida para la criminalidad transnacional, así como para la competencia y fricción geopolíticas, sus usos ofensivos y defensivos ingresan en el cálculo estratégico de Estados y actores no estatales, con impactos directos en el orden internacional.

1.1 Amenazas



Las ciberamenazas tienen la capacidad de poner en riesgo a un gran número de individuos y organizaciones, incluídas aquellas que poseen u operan servicios esenciales e infraestructuras críticas, cuyo papel central en la sociedad conlleva un elevado grado de sensibilidad.

Problemas graves y socialmente relevantes —como el hambre o la dificultad de acceso a la electricidad o al saneamiento básico— se enfrentan mediante esfuerzos concentrados y priorización de inversiones. En el contexto de las ciberamenazas, sin embargo, existen oponentes motivados, con recursos y capacidades técnicas diversas, lo que exige acción y atención permanentes por parte del Estado.

Algunos de los principales tipos de amenazas contra los servicios esenciales e infraestructuras críticas son: *phishing*; ataques de denegación de servicio en gran escala; *ransomware*; filtraciones de informaciones privadas o institucionales; ciberespionaje; interrupción de servicios; y Amenazas Persistentes Avanzadas (APT).

Estas acciones maliciosas, perpetradas por actores estatales y no estatales, presentan distintos alcances, niveles de sofisticación y motivaciones. Pueden responder a intereses políticos, religiosos, militares, económicos, de inteligencia, de sabotaje o puramente criminales.

El avance de tecnologías emergentes, como la Inteligencia Artificial y la Computación Cuántica, tiende a tornar este escenario aún más desafiante, en la medida en que dichas innovaciones pueden ampliar las capacidades de los agentes maliciosos.

El desarrollo de capacidades cibernéticas ofensivas, dependiendo de su alcance, puede tener impactos comparables a los de ataques cinéticos y comprometer de manera decisiva los intereses nacionales.

1.2 Contexto nacional

En junio de 2022, la Lista de Alto Riesgo de la Administración Pública (LAR), elaborada por el Tribunal de Cuentas de la Unión (TCU), señaló que "en 2021, el 73,1% de los servicios públicos prestados por el gobierno federal ya eran totalmente digitales, lo que corresponde a 3.598 servicios". Si se incluyen también los servicios parcialmente digitalizados, el porcentaje asciende al 86,7%. El informe destacó que "estos números, por sí solos, muestran la magnitud de los riesgos y de los perjuicios que las fallas de seguridad y la indisponibilidad de servicios pueden ocasionar".

La LAR de 2024 registró un incremento del 56% en el número de ciberincidentes que afectaron a la Administración Pública Federal, lo que "genera preocupación respecto de la capacidad de las organizaciones públicas para proteger sus datos (estratégicos y personales) y mantener la prestación de servicios a la sociedad brasileña". Asimismo, resaltó que la ciberseguridad, la autodeterminación y la capacidad de explotar económica, estratégica y tecnológicamente sus datos personales y críticos constituyen las tres dimensiones fundamentales de la soberanía digital.

Por otra parte, las evaluaciones de la madurez brasileña en ciberseguridad, realizadas en 2020 y 2023 con base en el Modelo de Madurez en Ciberseguridad de la Universidad de Oxford, muestran que Brasil se ubica por debajo del punto medio de la escala ("Establecido") en todos los criterios. Aunque hubo una ligera mejora en un 50% de los ítems, el país se mantuvo igual en un 29% y retrocedió en un 21%, pasando de un promedio del 40% en 2020 al 44% en 2023. Este nivel resulta insuficiente frente al grado de exposición digital de la sociedad brasileña.

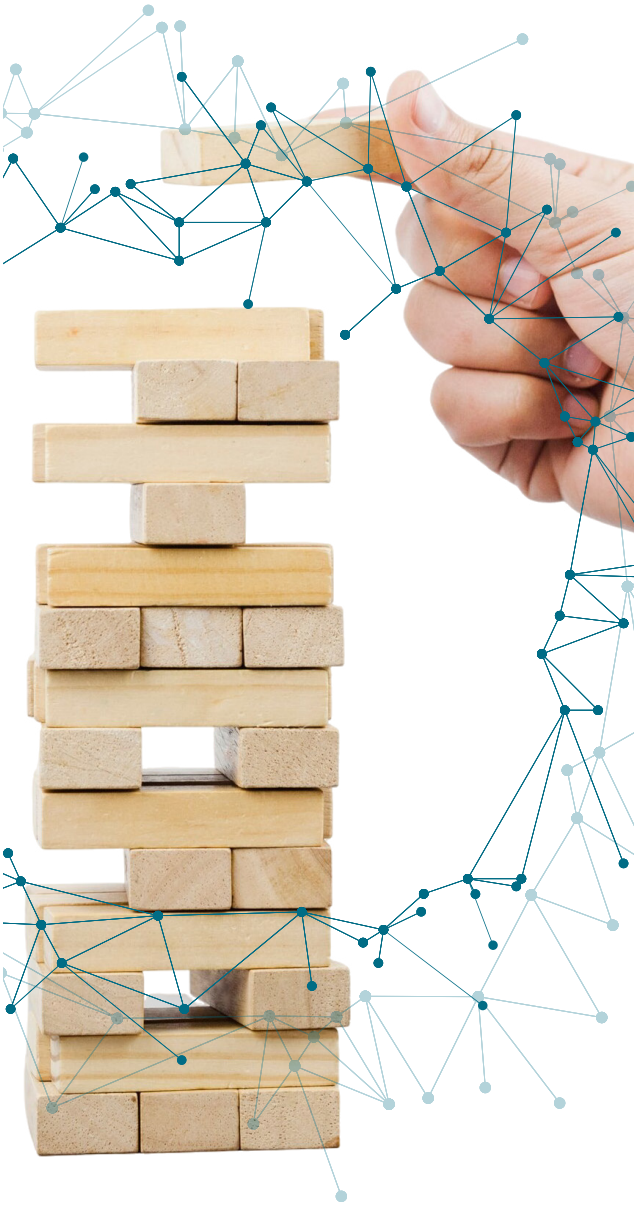
Para una sociedad que busca mejorar la calidad de vida a través de la evolución tecnológica, estas cifras constituyen una señal de alerta, evidenciando la urgencia de invertir en la materia y de adoptar una estructura normativa y regulatoria consistente. Los ciberincidentes impactan severamente los derechos humanos, el ejercicio de la ciudadanía, la economía y el desarrollo sostenible.

El Informe del Índice Global de Ciberseguridad 2024 de la Unión Internacional de Telecomunicaciones (UIT) reconoció los esfuerzos de Brasil con la aprobación de la PNCiber, la creación del CNCiber y la ratificación de la Convención de Budapest sobre ciberdelincuencia, entre otras medidas. El país fue ubicado en el grupo de naciones modelo en evolución en las áreas de medidas legales, técnicas, organizacionales, de concienciación, capacitación y cooperación internacional. Aunque el índice no mide la implementación práctica de capacidades, estos hitos reflejan un avance en la madurez del Estado brasileño en el tema.

1.3 Desafíos

En el contexto de las ciberamenazas, las organizaciones necesitan medios para identificar, proteger, responder y recuperarse de los incidentes. La prevención y la respuesta adecuadas demandarán conciencia situacional, cooperación y coordinación, preferentemente organizadas bajo una estructura centralizada de comando y control.

El principal desafío que enfrenta la sociedad brasileña en materia de ciberseguridad es establecer una coordinación nacional de las acciones existentes —o previstas— por distintos actores públicos y privados, abarcando todos los poderes y niveles de la Federación. Esta coordinación debe equilibrar los riesgos y necesidades más urgentes, buscando sinergia en el uso de los recursos humanos y materiales disponibles, de manera de garantizar la continuidad y aceleración del proceso de transformación digital que vive el país.



Asimismo, debe aprovechar las oportunidades que ofrecen las tecnologías emergentes, como el uso de herramientas de inteligencia artificial y aprendizaje automático para analizar, identificar y responder a los ataques cibernéticos.

Otro desafío relevante es la escasez de datos e indicadores nacionales consistentes y periódicos, que permitan diagnosticar y acompañar la evolución del contexto y del escenario de ciberseguridad, de forma adecuada a las características y necesidades del país.

Finalmente, se requiere una mayor concienciación entre los gestores públicos y privados respecto de los riesgos y amenazas del ciberespacio. La ciberseguridad debe ser entendida como un factor de estabilidad de las sociedades modernas, una inversión estratégica que garantiza el buen funcionamiento de todos los sectores de la economía y la continuidad de los negocios, minimizando el riesgo de incidentes o interrupciones de servicios esenciales.

La E-Ciber aborda estas y otras cuestiones críticas, orientando las acciones que Brasil debe seguir para volverse más seguro y resiliente frente a las amenazas presentes y futuras, al tiempo que asegura los beneficios de la tecnología y la inserción del país en la creciente cadena global de valor asociada a la ciberseguridad.

1.4 Evolución de E-Ciber

Esta estrategia consiste en la segunda versión del documento brasileño sobre este tema. En línea con los resultados del Informe del Índice Global de Ciberseguridad 2024 de la Unión Internacional de Telecomunicaciones, la evolución de la madurez nacional se puede inferir del análisis de algunos puntos, como los reflejados en la siguiente tabla, que presenta un resumen comparativo de este E-Ciber con su predecesor.

TEMA	E-Ciber 2020	E-Ciber 2025	DESCRIPCIÓN DE LA EVALUACIÓN
Gobernanza	Propuesta de gobernanza centralizada.	Gobernanza integrada a la soberanía nacional como uno de los cuatro ejes temáticos	La nueva estrategia propone el desarrollo de mecanismos de regulación, inspección, coordinación y control.
Desarrollo Tecnológico Nacional	Enfoque genérico en la industria de la ciberseguridad.	Incentivo específico a tecnologías y soluciones nacionales, reducción de la dependencia tecnológica.	Fortalece la independencia de Brasil y disminuye la dependencia de tecnologías extranjeras.
Inclusión y diversidad	No mencionada.	Inclusión de grupos subrepresentados (niños, adolescentes, ancianos y neurodivergentes).	La nueva estrategia fomenta la protección de los grupos vulnerables.
Madurez cibernética	Evaluación esporádica.	Objetivo claro de alcanzar el nivel "Establecido" en todos los requisitos de madurez.	La mejora trae un monitoreo estructurado de la evolución de Brasil en ciberseguridad.
Protección de servicios esenciales e infraestructura crítica	Enfoque en la infraestructura crítica general.	Ampliación hacia servicios esenciales y sus infraestructuras.	Mejora de resiliencia con estándares mínimos y certificación de produtos.
Innovación en PyMEs y Startups	Incentivo a la investigación y desarrollo.	Detallando mecanismos para incentivar startups y PyMES.	La nueva estrategia incluye acciones específicas para crear un entorno innovador para las pequeñas empresas.
Cooperación internacional	Previsión de alianzas internacionales.	Intensificación de las asociaciones y el intercambio con énfasis en el desarrollo de capacidades.	Refuerza las actividades de cooperación internacional.
Educación y Sensibilización	Campañas de sensibilización.	Formación de una cultura nacional de ciberseguridad, con énfasis en gestores públicos y privados.	La nueva estrategia promueve una cultura de ciberseguridad sostenible y arraigada en la sociedad.
Comunicación y respuesta a incidentes	Propuesta para mejorar la comunicación entre sectores.	Promoción de la protección contra riesgos, la protección y la respuesta a incidentes cibernéticos.	La mejora favorece una respuesta más ágil y eficaz, mejorando la capacidad de respuesta ante incidentes cibernéticos.

TEMA	E-Ciber 2020	E-Ciber 2025	DESCRIPCIÓN DE LA EVALUACIÓN
Adopción de tecnologías emergentes	Incentivo genérico.	Reducción de la deuda tecnológica del país en tecnologías emergentes y disruptivas	La nueva estrategia enfatiza la necesidad de acciones gubernamentales afirmativas e incrementales para hacerlo.
Plazo extendido	Plazo limitado a un período de 4 años.	Vigencia sin límite temporal, con acciones de corto, mediano y largo plazo.	La nueva estrategia considera y aborda temas con un horizonte más amplio que el de 4 años, que constituye una estrategia a largo plazo, ajustada a través de planes anuales.

1.5 Objetivos a Alcanzar

La evaluación de la eficacia de la E-Ciber se realizará mediante el avance en los criterios del modelo brasileño de madurez en ciberseguridad, a ser propuesto, y que servirá de línea de base para esta estrategia.

Se pretende que la E-Ciber permita que, en un horizonte de cinco años, Brasil alcance al menos el nivel *"Establecido"* en todos los criterios de madurez, sin retroceder en aquellos en los que ya haya alcanzado o superado dicho grado.

Los objetivos de la E-Ciber se derivan de los establecidos en la PNCiber:

- Garantizar la confidencialidad, integridad, autenticidad y disponibilidad del hardware, software y datos utilizados para el procesamiento, almacenamiento y transmisión electrónica o digital de información;
- Promover la soberanía nacional, la priorización de los intereses nacionales y la debida diligencia en el ciberespacio;
- Fomentar la adopción de medidas de protección cibernética y gestión de riesgos para prevenir, evitar, mitigar, reducir y neutralizar las vulnerabilidades, ataques e incidentes cibernéticos y sus impactos;
- Desarrollar la educación, la cultura y la formación técnico-profesional en ciberseguridad en la sociedad brasileña;
- Aumentar la acción coordinada y el intercambio de información sobre ciberseguridad entre:

  a) Unión, estados, Distrito Federal y municipios;

  b) Poderes Ejecutivo, Legislativo y Judicial;

  c) sector privado; y

  d) la sociedad en general;
- Promover la autonomía productiva y tecnológica en el área de ciberseguridad;

- Proporcionar el desarrollo nacional de productos, servicios y tecnologías orientadas a la ciberseguridad;
- Intensificar la lucha contra la ciberdelincuencia;
- Implementar estrategias de colaboración para desarrollar la cooperación internacional; y
- Fomentar la investigación científica, el desarrollo tecnológico y las actividades de innovación relacionadas con la ciberseguridad.

Con ello, se busca crear condiciones para una articulación efectiva entre la Unión, los estados, el Distrito Federal, los municipios, los tres Poderes, el sector privado y la sociedad en general, en el contexto de la ciberseguridad y la ciberresiliencia. La estrategia abarca a toda la nación, con atención especial a los llamados "Servicios Esenciales".

1.6 Beneficios esperados

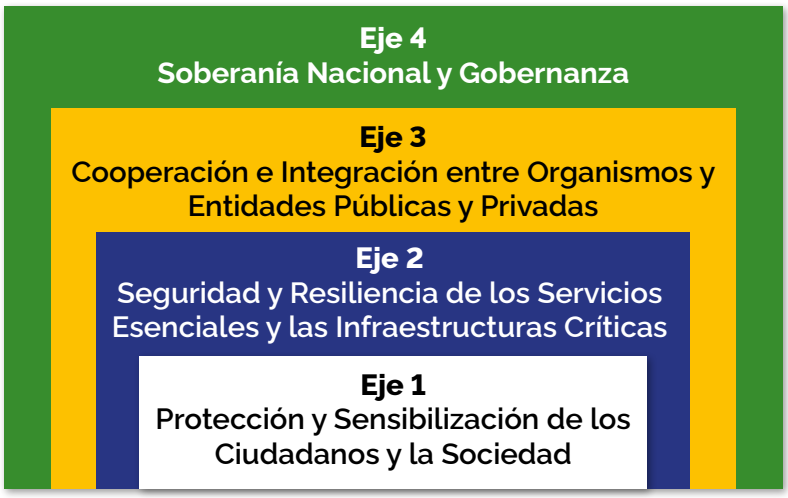
Las estimaciones del Foro Económico Mundial (2024) indican que las pérdidas financieras derivadas de ciberofensas en Brasil podrían haber alcanzado el equivalente al 14% del PIB global en 2024 (aproximadamente 1,5 billones de reales proyectados al caso brasileño), con severos impactos negativos sobre la recaudación tributaria.

Se espera que la implementación de E-Ciber aumente la conciencia de la sociedad, la preparación de las instituciones para la prevención y la resiliencia ante incidentes cibernéticos, particularmente en lo que respecta a los proveedores de servicios esenciales y los operadores de infraestructuras críticas, conteniendo la evolución de las pérdidas y reduciendo el riesgo de interrupción de los servicios relevantes que puedan generar inestabilidades en la sociedad.

El decreto tiene alcance normativo en el ámbito del Poder Ejecutivo Federal y ejerce un efecto inductivo-colaborativo sobre los demás Poderes y sobre la sociedad en su conjunto.

2 Presentación

La E-Ciber 2025 fue desarrollada con base en cuatro Ejes Temáticos que se complementan y se apoyan mutuamente, como se representa en la Figura 1.



Estos Ejes Temáticos agrupan un conjunto de Acciones Estratégicas, que serán implementadas mediante Iniciativas Estratégicas que se detallarán en el Plan Nacional de Ciberseguridad, conforme lo establece la PNCiber.

2.1 Eje 1 – Protección y concienciación del ciudadano y de la sociedad

La protección y sensibilización de la ciudadanía y la sociedad tiene como objetivo garantizar el uso seguro de los servicios digitales, con especial atención a las personas en situación de vulnerabilidad, como los niños y adolescentes, las personas mayores y las personas neurodivergentes. Para ello, se priorizaron las siguientes acciones estratégicas:

- **Desempeño seguro en el ciberespacio:** fomentar la adopción de comportamientos responsables y seguros por parte de los usuarios al utilizar herramientas digitales, con la promoción de prácticas que reduzcan los riesgos cibernéticos.
- **Apoyo a las víctimas:** promoción de la ampliación de los servicios de apoyo a las personas afectadas por delitos y otras prácticas ilícitas en el entorno digital, con foco en la acogida y orientación.
- **Identificación y autenticación:** fomento del uso de mecanismos de identificación y autenticación de usuarios de acuerdo con las necesidades de cada servicio digital, respetando siempre la privacidad.
- **Formación de docentes y directivos:** buscando la cualificación de profesionales de la educación, tanto de la red pública como privada, para capacitarlos para impartir temas relacionados con la ciberseguridad.
- **Ciberseguridad en la educación:** fomentar la inclusión de contenidos de ciberseguridad en los planes de estudio escolares a todos los niveles, promoviendo la formación de ciudadanos más concienciados digitalmente.
- **Participación en foros y eventos:** integración de estudiantes, profesionales e investigadores en foros, congresos y actividades técnicas centradas en la ciberseguridad.
- **Orientación a pequeñas empresas:** apoyo a microempresas, pequeñas empresas y startups en la gestión de ciber-riesgos y en la recuperación posterior a incidentes.
- **Planes de cumplimiento flexibles:** evaluación de modelos de cumplimiento de ciberseguridad adaptables para que los organismos públicos puedan implementarlos de acuerdo con su realidad.
- **Planes de contingencia y pruebas:** incentivo a la elaboración de planes institucionales de respuesta a incidentes, con realización de pruebas y simulaciones para evaluar el nivel de seguridad cibernética.
- **Lucha contra la ciberdelincuencia:** promover una acción integrada entre los diferentes sectores de la sociedad para prevenir y combatir los delitos digitales, el fraude y otras amenazas en el ciberespacio.
- **Difusión de tratados internacionales:** divulgación de la Convención sobre

Ciberdelincuencia (Convenio de Budapest) y de otros instrumentos nacionales e internacionales en vigor en Brasil.

- **Acciones contra la ciberdelincuencia:** apoyo a iniciativas que aumenten la eficacia de las operaciones de ciberdelincuencia mediante la mejora de las investigaciones y las respuestas.
- **Canales de notificación:** fomento de la mejora jurídica y técnica de las estructuras disponibles para denunciar los delitos cibernéticos, con el fin de hacerlos más accesibles y eficaces.
- **Capacitación de organismos de persecución penal:** incentivo a la formación continua de profesionales de instituciones responsables de la investigación y represión del cibercrimen, con el fin de mejorar su capacidad de actuación.

2.2 Eje 2 – Seguridad y resiliencia de servicios esenciales e infraestructuras críticas

El eje de seguridad y resiliencia de los servicios esenciales e infraestructuras críticas tiene como propósito ofrecer instrumentos eficaces para prevenir y responder a ciberincidentes. Para ello, se proponen las siguientes acciones estratégicas:

- **Promoción de la gestión de riesgos por parte de los reguladores:** fomento de que las entidades con funciones reguladoras promuevan la gestión de los riesgos cibernéticos y adopten medidas de protección y respuesta a los ciberincidentes en sus respectivos sectores.
- **Fortalecimiento de la regulación y el control:** desarrollo de mecanismos de regulación, inspección, coordinación y control para garantizar la seguridad, la resiliencia y la continuidad de los servicios esenciales, con especial atención al uso seguro de las tecnologías de la información y operativas.
- **Mecanismos de alerta de riesgo:** adopción de sistemas de alerta que alerten de riesgos relevantes en la prestación de servicios digitales, permitiendo respuestas rápidas y eficaces.
- **Lista de alto riesgo de ciberseguridad:** creación y mantenimiento de una lista de alto riesgo que sirva de base para la gestión sectorial del riesgo.
- **Normas mínimas para datos sensibles:** fomentar la definición y adopción de normas mínimas de ciberseguridad para la protección de datos relevantes y sensibles, especialmente en contextos críticos.

- **Sello nacional de ciberseguridad:** institución de un sello de certificación nacional para indicar el nivel de seguridad de los activos cibernéticos, proporcionando una mayor fiabilidad a los productos, servicios y sistemas certificados.
- **Seguro de ciberincidentes:** incentivo para que los proveedores de servicios esenciales y los operadores de infraestructuras críticas aumenten sus medidas de resiliencia, como la contratación de seguros específicos para cubrir los daños derivados de ciberincidentes.
- **Ejercicios y simulaciones:** promoción de ejercicios y simulaciones periódicas, tanto en sectores específicos como en contextos multisectoriales, con el objetivo de probar y fortalecer la resiliencia cibernética de los servicios esenciales.
- **Mejora regulatoria continua:** fomento a la actualización constante de la normativa relacionada con la ciberseguridad, incluyendo la definición de estándares mínimos de control y la elaboración de guías técnicas.
- **Seguridad en la interoperabilidad de los datos:** buscando fortalecer la seguridad en el intercambio y compartición de datos entre sistemas, así como en los canales digitales utilizados para la prestación de servicios.
- **Apoyo a las empresas brasileñas:** incentivos para que las empresas nacionales busquen y utilicen productos y servicios alineados con los estándares mínimos de ciberseguridad, promoviendo un ecosistema digital más seguro.

2.3 Eje 3 – Cooperación e integración entre organismos y entidades públicas y privadas

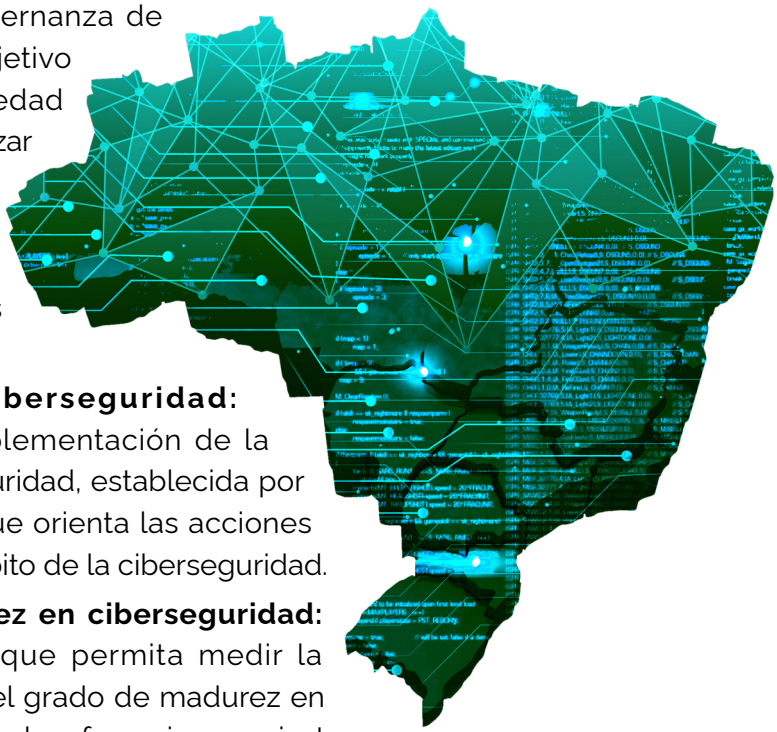
El eje de cooperación e integración busca promover el debate y el intercambio de informaciones sobre ciberseguridad, tanto en el escenario nacional como internacional. Para ello, se establecen las siguientes acciones estratégicas:

- **Creación de estructuras especializadas en ciberseguridad:** fomento a la conformación de equipos de prevención y respuesta a incidentes cibernéticos, esenciales para una actuación rápida en un contexto de crecientes ciberamenazas. Incluye también la promoción de centros de análisis y compartición de información (ISACs), instrumentos que contribuyen a una respuesta coordinada, así como el incentivo a la instalación de laboratorios especializados capaces de realizar pruebas, investigaciones y desarrollos en la materia

- **Notificación nacional de ciberincidentes:** creación de un mecanismo unificado de notificación de ciberincidentes en el país, facilitando la respuesta ágil, el mapeo de amenazas y la coordinación entre actores públicos y privados.
- **Cooperación con instituciones y agencias académicas:** fortalecer las relaciones de confianza y colaboración entre instituciones académicas y agencias nacionales e internacionales, buscar el desarrollo de acciones conjuntas de ciberseguridad y ciberdefensa, fomentar el intercambio de información y experiencias, promover la divulgación coordinada de vulnerabilidades y actuar para combatir los delitos cibernéticos y otras actividades ilícitas en el entorno digital.
- **Fortalecimiento de la ciberseguridad en los países vecinos:** apoyo a la ampliación de la capacidad de ciberseguridad de los países del entorno estratégico de Brasil, a través de iniciativas bilaterales o multilaterales, con el objetivo de promover la estabilidad regional y la ciberseguridad.
- **Participación internacional de Brasil:** fomento de la presencia activa de Brasil en foros y organizaciones internacionales enfocadas en ciberseguridad, favoreciendo el intercambio de experiencias, la definición de buenas prácticas y la alineación con los estándares globales de protección digital.

2.4 Eje 4 – Soberanía nacional y gobernanza

La soberanía nacional y la gobernanza de la ciberseguridad tienen como objetivo proteger los intereses de la sociedad brasileña en el ciberespacio y garantizar un entorno digital confiable que favorezca el crecimiento económico y tecnológico de Brasil, con base en las siguientes acciones estratégicas:



- **Política Nacional de Ciberseguridad:** actualización, difusión e implementación de la Política Nacional de Ciberseguridad, establecida por el Decreto nº 11.856/2023, que orienta las acciones estratégicas del país en el ámbito de la ciberseguridad.
- **Modelo nacional de madurez en ciberseguridad:** elaboración de un modelo que permita medir la evolución del sector, evaluar el grado de madurez en ciberseguridad en Brasil y servir de referencia para ajustes en la planificación estratégica nacional.
- **Formación técnica y profesional:** ampliación de la formación y capacitación técnica en ciberseguridad, en una escala adecuada a las demandas reales del país, preparando profesionales calificados para actuar en todos los sectores de la economía.
- **Reducción del déficit tecnológico:** adopción de acciones afirmativas y progresivas para disminuir la dependencia externa en tecnologías emergentes y disruptivas, fortaleciendo la base tecnológica nacional.

- **Evaluación de conformidad en seguridad:** estímulo al desarrollo de capacidades para evaluar de forma continua la conformidad en seguridad de productos, servicios y tecnologías vinculados a la ciberseguridad, aumentando la confiabilidad y calidad de las soluciones utilizadas en el país.
- **Sistemas seguros de intercambio de información:** fomentar el uso de sistemas seguros para compartir información sensible en el ámbito de la ciberseguridad, promoviendo una mayor protección e integridad de los datos**.**
- **Incentivo al sector privado:** apoyo al sector privado en la creación y oferta de productos, servicios y tecnologías en ciberseguridad, con especial atención a microempresas, pequeñas empresas y startups.
- **Alianzas con institutos de investigación:** fomento al establecimiento de asociaciones con institutos brasileños de investigación y desarrollo, fortaleciendo la producción científica y tecnológica nacional mediante residencias tecnológicas (pasantías supervisadas en temas de ciberseguridad).
- **Líneas de investigación y becas de estudio:** promoción de líneas de investigación en programas de grado y posgrado stricto sensu, así como la concesión de becas para formar especialistas y docentes brasileños en ciberseguridad.
- **Desarrollo de soluciones nacionales:** incentivo a la producción de productos, servicios y tecnologías nacionales que contribuyan a la mejora de la ciberseguridad en Brasil, reduciendo la dependencia externa y promoviendo la innovación local.

2.5 El Plan Nacional de Ciberseguridad (P-Ciber)

La E-Ciber, en tanto estrategia nacional, posee un horizonte temporal indefinido y prevé que sus Acciones Estratégicas se desdoblen en Iniciativas Estratégicas de corto y mediano plazo, las cuales integrarán el Plan Nacional de Ciberseguridad (P-Ciber). El P-Ciber deberá ser actualizado anualmente o a cada dos años, elaborado por el CNCiber y aprobado por el Gabinete de Seguridad Institucional de la Presidencia de la República (GSI/PR), tras la anuencia de los representantes de los organismos gubernamentales que integran el Comité. El Plan contendrá las iniciativas estratégicas detalladas, su cronograma de ejecución y la estructura de gobernanza correspondiente.

Expediente

Luiz Inácio Lula da Silva
Presidente de la República Federativa de Brasil

Geraldo Alckmin
Vicepresidente

Marcos Antonio Amaro dos Santos
Ministro de Estado Jefe del Gabinete de Seguridad Institucional de la Presidencia de la República

Washington Rocha Triani
Secretario Ejecutivo del GSI/PR

Lincoln Bernardes Júnior
Secretario Ejecutivo Adjunto

Secretaría de Seguridad de la Información y Cibernética

André Luiz Bandeira Molina
Secretario de Seguridad de la Información y Cibernética

Luiz Fernando Moraes da Silva
Director del Departamento de Seguridad Cibernética

Danielle Ayres
Directora del Departamento de Seguridad de la Información

Marcelo Antonio Osller Malagutti
Asesor Especial del Ministro

Asesoría

Marco Aurélio de Andrade Lima
Jefe de Gabinete del Ministro

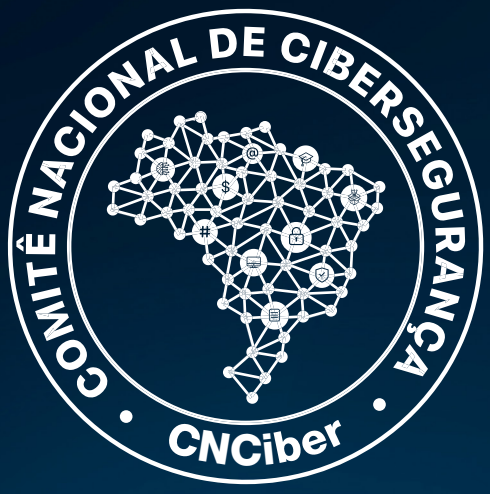
Cel (EB) R/1 Sergio Martins Rocha
Asesor Jefe Militar

Comunicación Social

Heron Clementino de Andrade
Jefe de la Asesoría Especial de Comunicación Social del GSI/PR

Diagramación editorial
1º Ten EB Djalma Martins

Redacción, revisión y traducción de textos
Marcelo Antonio Osller Malagutti
Carlos Eduardo de Souza Gomes Fonseca
Maj EB Mayara Azeredo Alves
Primer Secretario Reynaldo Collares


COMITÊ NACIONAL DE CIBERSEGURANÇA
CNCiber