UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

PROPUESTA DE ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

PERÚ, 2026-2028

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

PROPUESTA DE ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

PERÚ, 2026-2028

1. INTRODUCCIÓN

La transformación digital ha modificado profundamente la forma en que las personas, las empresas y las instituciones públicas desarrollan sus actividades. Los servicios públicos, las operaciones financieras, las comunicaciones, los sistemas de salud, el transporte, la educación y buena parte de las actividades económicas dependen actualmente de tecnologías digitales interconectadas.

Esta dependencia genera importantes oportunidades para el desarrollo del país, pero también incrementa la exposición frente a amenazas cibernéticas. Un incidente de seguridad puede dejar de ser un problema exclusivamente informático y convertirse en un acontecimiento capaz de afectar la continuidad de servicios esenciales, generar pérdidas económicas, comprometer información sensible, afectar derechos ciudadanos o incluso tener consecuencias para la seguridad nacional.

En este contexto se plantea la **Estrategia Nacional de Ciberseguridad del Perú 2026-2028 (ESNACIB)**. El documento reconoce que la ciberseguridad debe ser entendida como un componente estratégico del desarrollo nacional y no únicamente como una función técnica de las áreas de tecnologías de información.

La estrategia parte de una idea fundamental: un país digitalmente desarrollado necesita también contar con capacidades suficientes para prevenir, detectar, responder y recuperarse frente a incidentes cibernéticos. La protección de la información, de las infraestructuras críticas y de los servicios digitales constituye, por tanto, una condición para mantener la confianza de ciudadanos, organizaciones y empresas en el entorno digital.

La ESNACIB ha sido elaborada bajo el liderazgo de la **Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital**, con la participación del Centro Nacional de Seguridad Digital y otros actores del ecosistema digital peruano. Su horizonte temporal comprende los años 2026 a 2028.

El documento busca consolidar un Perú **ciberseguro, resiliente y confiable**, fortaleciendo las capacidades nacionales y contribuyendo a la protección de la soberanía digital, los derechos ciudadanos y el desarrollo económico y social.

2. CONCEPTO Y ALCANCE DE LA CIBERSEGURIDAD

Uno de los aspectos relevantes de la estrategia es que presenta una visión amplia de la ciberseguridad.

El documento recoge la definición establecida en el marco peruano y, a partir de estándares internacionales, entiende la ciberseguridad como un conjunto de políticas, directrices, metodologías, buenas prácticas, programas de formación, acciones, herramientas y soluciones destinadas a gestionar riesgos y proteger la **confidencialidad, integridad y disponibilidad** de los activos de información digitales conectados.

Esta perspectiva resulta importante porque permite comprender que la ciberseguridad no se limita a instalar antivirus, firewalls o mecanismos de protección tecnológica. La seguridad depende también de las personas, los procesos, las normas, la organización, la gestión de riesgos, la capacidad institucional y la coordinación entre diferentes actores.

Dentro de esta visión, los activos que deben protegerse comprenden información, bases de datos, aplicaciones, sistemas, dispositivos, redes, servicios, infraestructura, personal y otros elementos vinculados con el ecosistema digital.

La estrategia establece que su alcance comprende la protección de:

- Infraestructuras críticas.
- Activos de información digitales.
- Datos sensibles.
- Sistemas y plataformas digitales.
- Servicios digitales esenciales.
- Redes y sistemas tecnológicos.
- Información utilizada por las entidades públicas y privadas.

Asimismo, busca fortalecer la conciencia y la confianza de los usuarios, promover la cooperación público-privada e internacional y desarrollar un ecosistema digital seguro y resiliente.

Un aspecto especialmente importante para quienes estudian ciberseguridad es la relación entre **ciberseguridad y seguridad digital**. La estrategia recoge el enfoque de la OCDE, según el cual la seguridad digital tiene una dimensión económica y social. Por ello, la

protección digital tiene efectos directos sobre la confianza, la actividad económica, la prestación de servicios y el bienestar de las personas.

3. ÁMBITO DE APLICACIÓN

La ESNACIB está diseñada para el ecosistema digital peruano.

Su aplicación comprende a las entidades del sector público en los diferentes niveles de gobierno, mientras que sus principios y orientaciones también involucran al sector privado, la academia, la sociedad civil y la ciudadanía.

Esta concepción resulta coherente con la naturaleza del ciberespacio. Una amenaza puede originarse en un país extranjero, afectar una infraestructura privada y terminar impactando un servicio público. Del mismo modo, una vulnerabilidad existente en un proveedor tecnológico puede convertirse en un riesgo para múltiples organizaciones.

Por ello, la estrategia plantea una responsabilidad compartida.

La ciberseguridad deja de ser una tarea exclusiva del responsable de tecnologías de información y pasa a involucrar a los niveles directivos, áreas jurídicas, responsables de continuidad, gestión de riesgos, protección de datos, recursos humanos, comunicaciones, proveedores y usuarios.

Para las entidades públicas, esto significa que la seguridad debe incorporarse progresivamente dentro de la planificación y de los instrumentos de gestión institucional. El documento señala, además, que la estrategia tiene un horizonte de tres años y contempla su revisión durante el último año de vigencia o cuando ocurran cambios relevantes de carácter estratégico, normativo o tecnológico.

4. MARCO NORMATIVO Y DE GOBERNANZA

La ESNACIB no se plantea de manera aislada. Se articula con el marco jurídico y de políticas públicas existente en el Perú.

Entre las principales normas consideradas se encuentran:

- Constitución Política del Perú.

- Ley N.º 30999, Ley de Ciberdefensa.
- Decreto Legislativo N.º 1412, Ley de Gobierno Digital.
- Decreto Supremo N.º 029-2021-PCM, Reglamento de la Ley de Gobierno Digital.
- Ley N.º 29733, Ley de Protección de Datos Personales.
- Decreto de Urgencia N.º 007-2020, que aprueba el Marco de Confianza Digital.
- Decreto Supremo N.º 017-2024-PCM, Reglamento de la Ley de Ciberdefensa.
- NTP ISO/IEC 27032:2024.
- NTP ISO/IEC 27001:2022.
- NTP ISO/IEC 27002:2022.
- NTP ISO/IEC 27005:2022.

El documento también relaciona la estrategia con la Política Nacional de Transformación Digital al 2030, la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030, el Plan Estratégico de Desarrollo Nacional al 2050 y el PESEM 2024-2030 del sector PCM.

La importancia de esta articulación radica en evitar que la ciberseguridad sea tratada como una política independiente del proceso de modernización del Estado.

La transformación digital y la ciberseguridad deben avanzar conjuntamente. Digitalizar servicios sin gestionar adecuadamente los riesgos puede ampliar la superficie de exposición de las instituciones y de los ciudadanos.

5. SITUACIÓN ACTUAL Y PRINCIPALES DESAFÍOS

La estrategia reconoce que el escenario internacional de ciberseguridad se ha vuelto considerablemente más complejo.

Los ataques digitales han evolucionado desde acciones relativamente simples hacia operaciones más organizadas, automatizadas y persistentes. El documento identifica amenazas como malware, ransomware, ataques DDoS, phishing, ataques dirigidos contra infraestructuras críticas, desinformación y deepfakes.

El Foro Económico Mundial, citado en el documento, identifica la ciberseguridad como un riesgo global y advierte sobre la combinación entre amenazas digitales y tecnologías emergentes.

En el caso peruano, la estrategia identifica diversos desafíos. Entre ellos destacan el crecimiento de los ciberataques, la insuficiente cultura de ciberseguridad, la expansión de la ciberdelincuencia organizada y la necesidad de continuar fortaleciendo las capacidades institucionales.

El documento señala que durante 2024 el Perú registró más de 64 millones de ataques según datos atribuidos a Kaspersky. También menciona como principales modalidades el ransomware, phishing, DDoS y malware.

Más allá de las cifras específicas recogidas por la propuesta, el aspecto fundamental es la tendencia: la exposición digital aumenta y, con ella, la necesidad de gestionar sistemáticamente los riesgos.

Otro desafío importante es la **brecha de talento especializado**. La estrategia recoge información internacional según la cual existe una escasez significativa de profesionales especializados en ciberseguridad. Esto tiene una consecuencia directa para las organizaciones: disponer de tecnología no garantiza seguridad si no existen personas capaces de administrarla, monitorearla y responder adecuadamente ante incidentes.

6. PRINCIPALES AMENAZAS Y TENDENCIAS

La estrategia identifica diversas amenazas que continuarán teniendo relevancia durante el horizonte 2026-2028.

6.1. Ransomware

El ransomware constituye una de las amenazas de mayor impacto para organizaciones públicas y privadas. Consiste en comprometer sistemas o información y restringir el acceso mediante mecanismos de cifrado, generalmente con el propósito de exigir un rescate.

Su peligrosidad no se limita a la pérdida temporal de información. Puede afectar la continuidad operativa, generar costos de recuperación, comprometer información sensible y producir impactos reputacionales.

La estrategia reconoce su incremento y señala que puede afectar empresas, instituciones gubernamentales y servicios esenciales.

6.2. Ataques contra infraestructuras críticas

Las infraestructuras críticas constituyen un objetivo prioritario debido al impacto que podría producir su interrupción.

Sectores como energía, telecomunicaciones, salud, transporte, saneamiento y finanzas dependen cada vez más de sistemas digitales. Una interrupción puede trascender el ámbito tecnológico y afectar directamente a la población.

La estrategia propone identificar y categorizar las entidades que poseen infraestructuras críticas o activos críticos nacionales, considerando su vulnerabilidad, exposición, nivel de riesgo, impacto potencial e interdependencias.

6.3. Ataques DDoS

Los ataques de denegación de servicio distribuido buscan afectar la disponibilidad de servicios mediante grandes volúmenes de tráfico originados desde múltiples equipos comprometidos.

Aunque pueden parecer técnicamente simples, su impacto puede ser considerable cuando afectan plataformas de servicios públicos, entidades financieras, sistemas empresariales o servicios digitales esenciales.

6.4. Inteligencia Artificial

La inteligencia artificial constituye simultáneamente una oportunidad y un riesgo.

Por una parte, puede contribuir a detectar patrones anómalos, automatizar análisis, identificar amenazas y mejorar la capacidad de respuesta. Por otra, puede ser utilizada por actores maliciosos para perfeccionar campañas de ingeniería social, generar contenidos fraudulentos, automatizar actividades y desarrollar ataques más sofisticados.

La estrategia recoge la creciente utilización de IA generativa por parte de adversarios para mejorar técnicas de ingeniería social y actividades maliciosas.

6.5. Computación cuántica

La estrategia también considera la computación cuántica como una tecnología que puede modificar el escenario de seguridad, especialmente por sus potenciales efectos sobre mecanismos criptográficos tradicionales.

Esto introduce la necesidad de pensar en la seguridad con una perspectiva de largo plazo y evaluar la transición hacia mecanismos criptográficos capaces de resistir futuros escenarios tecnológicos.

7. PRINCIPIOS RECTORES

La ESNACIB plantea principios que deben orientar la implementación de sus pilares.

Liderazgo y responsabilidades

La ciberseguridad requiere la participación conjunta del Estado, empresas, academia, sociedad civil y ciudadanía. No puede ser entendida como una responsabilidad aislada del área informática.

Protección de derechos digitales y privacidad

La seguridad debe desarrollarse respetando los derechos fundamentales. La estrategia reconoce la importancia de proteger la identidad digital, la privacidad, la libertad de expresión, el acceso a la información y otros derechos relacionados con el entorno digital.

Enfoque holístico

La ciberseguridad involucra aspectos tecnológicos, jurídicos, organizacionales, económicos y sociales. Por ello, requiere una aproximación interdisciplinaria y sistemas adecuados de gobernanza.

En términos prácticos, estos principios obligan a superar una visión exclusivamente tecnológica. Una organización puede disponer de sistemas avanzados de protección y, sin embargo, mantener un nivel elevado de riesgo si sus trabajadores desconocen los procedimientos de seguridad o si sus directivos no toman decisiones basadas en riesgos.

8. VISIÓN Y OBJETIVO GENERAL

La visión de la estrategia se orienta a consolidar un Perú ciberseguro, resiliente y confiable, donde la tecnología contribuya al desarrollo económico y social sin comprometer la seguridad de las personas, instituciones y activos digitales.

El objetivo general consiste en establecer un marco de acciones estratégicas para proteger infraestructuras críticas, plataformas tecnológicas, sistemas de información, datos sensibles y otros activos digitales, al mismo tiempo que se fortalecen las capacidades de respuesta frente a amenazas cibernéticas.

Esto demuestra que la estrategia tiene dos componentes inseparables:

Primero: prevenir y proteger.

Segundo: responder y recuperarse.

Una estrategia moderna no puede basarse únicamente en evitar que ocurra un incidente. Debe asumir que algunos incidentes serán inevitables y preparar a las organizaciones para mantener sus operaciones, limitar daños y recuperar los servicios en el menor tiempo posible.

9. LOS OCHO PILARES DE LA ESNACIB

La estrategia se estructura en ocho pilares que organizan los objetivos y acciones estratégicas.

Pilar 1. Gobernanza y liderazgo

Busca establecer una estructura nacional clara para dirigir, coordinar y supervisar la ciberseguridad.

El objetivo estratégico general consiste en establecer un marco holístico de gobernanza con capacidades de dirección y operación que permitan actuar coordinadamente en el ecosistema nacional.

La PCM, a través de la Secretaría de Gobierno y Transformación Digital, ocupa un papel central como ente rector en materia de Gobierno Digital, mientras que el Centro Nacional de Seguridad Digital cumple funciones de articulación e intercambio de información.

Este pilar resulta fundamental porque uno de los problemas habituales en materia de ciberseguridad es la fragmentación de responsabilidades.

Una adecuada gobernanza debe responder preguntas concretas: quién dirige, quién previene, quién detecta, quién responde, quién comunica y quién toma decisiones durante una crisis.

Pilar 2. Salvaguardar las infraestructuras críticas y activos de información digitales

Su objetivo es fomentar la protección y resiliencia de las infraestructuras críticas y activos de información digitales del país.

La estrategia propone incorporar la ciberseguridad como objetivo estratégico en los documentos de gestión de las entidades responsables de sectores críticos y asignar los recursos necesarios.

También plantea identificar y categorizar las entidades que poseen activos críticos nacionales, considerando vulnerabilidades, riesgos, impactos e interdependencias.

Este enfoque permite pasar de una protección genérica a una protección basada en criticidad.

No todos los sistemas tienen el mismo impacto. La caída de una aplicación administrativa puede ser inconveniente; la interrupción de un sistema que sostiene un servicio esencial puede afectar directamente a miles o millones de personas.

Pilar 3. Regulación y cumplimiento

Este pilar busca fortalecer el marco jurídico y regulatorio para que sea coherente, actualizado, completo y alineado con estándares internacionales.

La estrategia señala que no se trata simplemente de producir nuevas normas. El propósito es identificar brechas reales y establecer reglas que definan responsabilidades, obligaciones y mecanismos de cumplimiento.

Entre las prioridades se encuentran:

- Protección de infraestructuras críticas.
- Gestión de incidentes.

- Protección de activos digitales.
- Lucha contra la ciberdelincuencia.
- Cumplimiento de estándares.
- Certificación y mecanismos de acreditación.

Para los profesionales de ciberseguridad, esto implica comprender que el cumplimiento normativo forma parte de la gestión del riesgo y no debe considerarse un trámite separado de la seguridad técnica.

Pilar 4. Gestión de riesgos, resiliencia y respuesta a incidentes

Este es uno de los pilares centrales de la estrategia.

Su objetivo es gestionar integralmente los ciberriesgos asociados a los activos digitales y fortalecer las capacidades de resiliencia y respuesta.

La propuesta plantea desarrollar una metodología común para gestionar riesgos, identificar perfiles de riesgo por sector y establecer mecanismos de monitoreo.

También plantea:

- Identificación de activos.
- Evaluación de amenazas.
- Análisis de probabilidad e impacto.
- Tratamiento de riesgos.
- Monitoreo continuo.
- Planes de continuidad.
- Procedimientos de respuesta.
- Simulacros.
- Intercambio de información.
- Fortalecimiento de CSIRTs.
- Gestión nacional de cibercrisis.

Un aspecto particularmente relevante es la propuesta de crear un **Sistema Nacional de Gestión de Cibercrisis**, destinado a coordinar la prevención, respuesta y recuperación frente a incidentes de gran escala.

La estrategia también propone protocolos sistemáticos para prevenir, detectar, analizar, contener, responder y recuperar operaciones afectadas por incidentes.

Pilar 5. Contrarrestar la ciberdelincuencia

La estrategia propone enfrentar la ciberdelincuencia mediante un enfoque preventivo, proactivo y colaborativo.

Esto significa fortalecer la capacidad de investigación, monitoreo, análisis forense, recepción de denuncias y aplicación de sanciones dentro del marco legal.

También reconoce que la lucha contra el ciberdelito requiere coordinación entre instituciones públicas, sector privado, academia y organismos internacionales.

Un aspecto relevante es la necesidad de mantener el equilibrio entre seguridad y privacidad. Las capacidades de vigilancia digital deben utilizarse dentro de límites legales y respetando los derechos fundamentales.

Pilar 6. Consolidar la ciberdefensa

La ciberdefensa está relacionada principalmente con la protección de la seguridad nacional frente a amenazas que pueden afectar infraestructuras y activos estratégicos.

La estrategia plantea fortalecer las capacidades institucionales para prevenir, detectar y responder ante incidentes que puedan comprometer la seguridad nacional.

También propone anticipar y gestionar escenarios de incidentes masivos o de carácter estratégico, incluyendo situaciones vinculadas con conflictos en el ciberespacio.

Para ello resulta necesaria la coordinación entre las capacidades civiles y militares, particularmente cuando un incidente pueda superar el ámbito de la seguridad digital ordinaria y convertirse en un problema de seguridad nacional.

Pilar 7. Investigación, innovación y cultura en ciberseguridad

La estrategia reconoce que la tecnología cambia rápidamente y que la protección no puede depender exclusivamente de herramientas existentes.

Por ello, plantea impulsar investigación, desarrollo e innovación en áreas como:

- Inteligencia artificial aplicada a ciberseguridad.
- Análisis forense.
- Criptografía post-cuántica.
- Aprendizaje automático.
- Tecnologías emergentes.
- Resiliencia de infraestructuras críticas.

También otorga importancia a la educación y a la formación especializada.

Este pilar tiene una importancia especial para el desarrollo de profesionales. La estrategia considera necesario fortalecer las capacidades técnicas del país y desarrollar una cultura de seguridad desde el sistema educativo.

La formación no debe limitarse a especialistas. También debe alcanzar a trabajadores, estudiantes, funcionarios, empresas y ciudadanía.

Pilar 8. Cooperación internacional

El carácter transfronterizo de las amenazas hace indispensable la cooperación internacional.

Los atacantes pueden encontrarse en una jurisdicción, utilizar infraestructura tecnológica ubicada en otra y afectar víctimas situadas en diferentes países.

Por ello, la estrategia plantea fortalecer la cooperación bilateral y multilateral y promover la participación peruana en espacios internacionales relacionados con ciberseguridad.

Entre los organismos mencionados se encuentran la OEA, Unión Europea, ONU, INTERPOL, EUROPOL e INCIBE.

También se plantea establecer protocolos para responder coordinadamente ante ciberataques transfronterizos e impulsar la cooperación en investigación de ciberdelitos y ciberterrorismo.

10. INDICADORES Y MEDICIÓN DEL DESEMPEÑO

Una estrategia nacional solamente puede ser efectiva si sus resultados pueden medirse.

La ESNACIB contempla el uso de **indicadores clave de rendimiento (KPIs)** para evaluar el progreso de sus objetivos.

Entre los ejemplos planteados se encuentran:

- Reducción de incidentes de ciberseguridad.
- Número de incidentes detectados.
- Tiempo promedio de respuesta.
- Porcentaje de usuarios capacitados.
- Tiempo necesario para detectar y mitigar eventos.
- Porcentaje de sistemas actualizados.
- Resultados de pruebas de ethical hacking.
- Adopción de MFA.
- Implementación de sistemas de monitoreo.

Este enfoque es particularmente importante porque permite pasar de una evaluación basada en percepciones a una evaluación basada en resultados.

Por ejemplo, no basta con afirmar que una organización “mejoró su seguridad”. Es más útil conocer cuánto disminuyó el tiempo de detección, cuánto aumentó la cobertura de MFA, qué porcentaje de vulnerabilidades críticas fueron corregidas o cuánto tardó la organización en recuperar un servicio.

11. IMPLEMENTACIÓN Y RESPONSABILIDADES

La ESNACIB contempla un ciclo de vida compuesto por diferentes etapas, entre ellas planificación, ejecución, supervisión y evaluación.

El documento reconoce que la etapa de ejecución es especialmente crítica porque requiere recursos humanos y financieros y debe desarrollarse mediante un Plan de Acción que permita convertir la estrategia en actividades concretas.

La estrategia identifica entidades responsables y colaboradoras para las diferentes acciones.

Esto permite establecer una lógica de responsabilidad institucional:

Pilar → Objetivo estratégico → Objetivo específico → Acción estratégica → Entidad responsable → Entidades colaboradoras → Horizonte de implementación.

Este modelo facilita la asignación de responsabilidades y permite realizar seguimiento a los compromisos.

En otras palabras, la ESNACIB no debería permanecer como un documento declarativo. Su verdadero valor dependerá de su capacidad para convertirse en acciones, presupuestos, proyectos, procedimientos, capacidades técnicas y resultados verificables.

12. IMPORTANCIA DE LA ESTRATEGIA PARA EL PERÚ

La importancia de la ESNACIB puede analizarse desde cinco perspectivas.

12.1. Perspectiva institucional

Permite establecer una dirección común para las entidades públicas y mejorar la coordinación frente a riesgos e incidentes.

12.2. Perspectiva económica

La continuidad y seguridad de los servicios digitales son necesarias para mantener la actividad empresarial, financiera y productiva.

12.3. Perspectiva social

La protección digital permite reducir riesgos para ciudadanos y usuarios, especialmente respecto de identidad, privacidad, información y acceso a servicios.

12.4. Perspectiva de seguridad nacional

Las infraestructuras críticas y los activos digitales pueden convertirse en objetivos estratégicos. Su protección contribuye a la soberanía y continuidad del Estado.

12.5. Perspectiva de transformación digital

No existe una transformación digital sostenible si los usuarios no confían en las plataformas y servicios digitales.

La propia estrategia vincula la ciberseguridad con la competitividad, innovación y transformación digital del país. Asimismo, la relaciona

con los lineamientos del Plan Estratégico de Desarrollo Nacional al 2050.

13. PRINCIPALES RETOS PARA LA IMPLEMENTACIÓN

Desde una perspectiva de gestión, el éxito de la estrategia dependerá de superar algunos desafíos.

El primero es convertir los objetivos estratégicos en acciones concretas dentro de cada institución.

El segundo es asegurar recursos suficientes. La ciberseguridad requiere inversión continua en tecnología, infraestructura, capacitación, servicios especializados y talento.

El tercero es desarrollar capacidades humanas. La tecnología cambia rápidamente y las organizaciones necesitan profesionales capaces de comprender riesgos, arquitectura, gestión de incidentes, protección de datos, análisis forense y respuesta.

El cuarto es fortalecer la coordinación. Un incidente de gran magnitud no puede ser gestionado eficientemente si las instituciones trabajan de manera aislada.

El quinto es consolidar una cultura de prevención. Las personas continúan siendo un componente fundamental de la seguridad y, en muchos casos, una vulnerabilidad puede originarse por errores, desconocimiento, ingeniería social o falta de procedimientos.

Finalmente, la estrategia debe mantenerse actualizada. El horizonte 2026-2028 no significa que las amenazas permanecerán estáticas. Nuevas tecnologías, modelos de negocio y técnicas de ataque pueden modificar rápidamente el panorama.

14. CONCLUSIONES

La **Estrategia Nacional de Ciberseguridad Perú 2026-2028** representa una propuesta de carácter integral para fortalecer la capacidad del país frente a las amenazas digitales.

Su principal aporte consiste en plantear que la ciberseguridad debe ser gestionada como una política estratégica vinculada con la seguridad nacional, la transformación digital, el desarrollo

económico, la protección de derechos y la continuidad de los servicios esenciales.

La estrategia supera una visión exclusivamente tecnológica. Propone trabajar simultáneamente sobre gobernanza, infraestructura crítica, regulación, gestión de riesgos, respuesta a incidentes, lucha contra la ciberdelincuencia, ciberdefensa, innovación, cultura y cooperación internacional.

Los ocho pilares constituyen el núcleo de la propuesta y buscan generar una respuesta articulada frente a un escenario en el que las amenazas son cada vez más sofisticadas y donde tecnologías como la inteligencia artificial, la nube y la futura computación cuántica modificarán las condiciones de seguridad.

Uno de los mensajes centrales que puede extraerse del documento es que **la seguridad debe incorporarse desde la planificación y no después de ocurrido un incidente**.

Esto significa identificar los activos críticos, conocer los riesgos, establecer responsables, aplicar controles, capacitar al personal, monitorear continuamente, disponer de mecanismos de respuesta y preparar planes de continuidad y recuperación.

Otro aspecto fundamental es la corresponsabilidad. El Estado no puede proteger por sí solo todo el ecosistema digital. Las empresas, proveedores tecnológicos, instituciones académicas, organizaciones de la sociedad civil y ciudadanos también forman parte de la seguridad nacional en el ciberespacio.

La estrategia reconoce igualmente que la protección de la información debe coexistir con la protección de los derechos. La ciberseguridad no debe utilizarse como justificación para desconocer la privacidad, la libertad de expresión, el acceso a la información u otros derechos fundamentales.

En este sentido, la construcción de un país ciberseguro requiere equilibrio entre **seguridad, innovación, desarrollo, privacidad y derechos ciudadanos**.

Para los profesionales que se están formando en ciberseguridad, la ESNACIB ofrece además una perspectiva particularmente importante: el especialista ya no puede limitarse a conocer

herramientas técnicas. Necesita comprender la gestión de riesgos, la gobernanza, la normativa, la continuidad operativa, la protección de datos, la respuesta a incidentes y la coordinación institucional.

En consecuencia, la ciberseguridad debe entenderse como una disciplina multidisciplinaria que integra tecnología, gestión, derecho, estrategia y personas.

La propuesta de estrategia concluye que la ciberseguridad es un desafío global que requiere un enfoque integral y colaborativo. Su implementación busca reducir brechas tecnológicas, fortalecer la resiliencia y proteger infraestructuras críticas, generando servicios digitales más seguros y confiables.

En términos generales, el éxito de la ESNACIB no dependerá únicamente de la aprobación de normas o de la adquisición de tecnología. Dependerá de la capacidad del país para transformar la estrategia en **capacidades reales, responsabilidades claras, inversión sostenida, talento especializado, coordinación efectiva y resultados medibles**.

Por ello, la principal lección para un profesional de ciberseguridad es clara: **proteger el ciberespacio no consiste únicamente en evitar ataques; consiste en desarrollar la capacidad institucional y nacional para anticiparlos, resistirlos, responder a ellos y recuperar rápidamente las funciones afectadas.**