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

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Guide to Developing a National Cybersecurity Strategy

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Guía para el Desarrollo de una Estrategia Nacional de Ciberseguridad

Tercera edición — 2025

Documento elaborado a partir de la tercera edición de la Guide to Developing a National Cybersecurity Strategy (NCS Guide), publicada en 2025 por la Unión Internacional de Telecomunicaciones (UIT/ITU) y el Banco Mundial, con participación de múltiples organizaciones internacionales, sector privado, academia y sociedad civil.

Propósito: *Presentar las ideas centrales de la guía para comprender cómo se diseña, financia, implementa y revisa una estrategia nacional de ciberseguridad.*

Nota de traducción: *Esta es una traducción/síntesis para fines académicos. La edición en inglés es la edición auténtica, según el aviso de la propia publicación.*

Fuente principal: ITU, World Bank et al. (2025), Guide to Developing a National Cybersecurity Strategy, 3rd Edition.

1. La ciberseguridad como asunto estratégico nacional

La principal idea de la tercera edición es sencilla, pero tiene implicaciones profundas: la ciberseguridad ya no puede tratarse como un asunto exclusivamente técnico. La digitalización sostiene actividades económicas, servicios públicos, comunicaciones, infraestructura y relaciones sociales. Por ello, una interrupción digital puede convertirse rápidamente en un problema económico, institucional o social.

La guía define la ciberseguridad como el conjunto de herramientas, políticas, directrices, enfoques de gestión del riesgo, acciones, capacitación, buenas prácticas, medidas de aseguramiento y tecnologías utilizadas para proteger la disponibilidad, integridad y confidencialidad de los activos de las infraestructuras conectadas. Es una definición amplia que incluye personas, infraestructura, aplicaciones, servicios digitales, telecomunicaciones y datos.

Desde esta perspectiva, una Estrategia Nacional de Ciberseguridad (NCS) no es simplemente un catálogo de controles tecnológicos. Es una expresión de la visión, objetivos, principios y prioridades que orientan a un país; identifica a los actores responsables y sus funciones; y establece los programas e iniciativas que permitirán proteger la infraestructura digital y aumentar la seguridad y resiliencia nacional.

El valor de la estrategia está en pasar de una lógica reactiva a una lógica de anticipación. En lugar de actuar únicamente después de un ransomware, una filtración o una interrupción de servicios, el Estado debe comprender su ecosistema digital, identificar dependencias, valorar riesgos, asignar recursos y establecer mecanismos de respuesta y recuperación.

Para un profesional de ciberseguridad, esta idea cambia la pregunta. Ya no basta con preguntar “¿qué herramienta necesitamos?”. La pregunta estratégica es “¿qué riesgo debemos reducir, qué servicio debemos proteger, quién es responsable, qué capacidades hacen falta y cómo sabremos si la inversión funcionó?”.

La tercera edición pone especial énfasis en riesgos asociados con tecnologías emergentes, dispositivos conectados, cadenas de

suministro complejas, infraestructura crítica e interdependencias transfronterizas. También refuerza la necesidad de financiar el ciclo completo de la estrategia, medir resultados y actualizarla de manera periódica.

En términos académicos, el aporte central puede resumirse así: la ciberseguridad debe estar integrada con el desarrollo digital, la seguridad nacional, la continuidad de servicios, la economía y la confianza pública, pero con un enfoque adaptado al contexto de cada país.

2. El ciclo de vida de una Estrategia Nacional de Ciberseguridad

La guía organiza el desarrollo de la estrategia en seis fases. No se trata de un proyecto que termina cuando se publica un documento: es un ciclo continuo que conecta planificación, análisis, financiación, implementación y evaluación.

- Fase I — Iniciación: se define la autoridad líder, la gobernanza, los actores que participarán, los recursos y el plan de trabajo.
- Fase II — Diagnóstico y análisis: se estudia la situación nacional de ciberseguridad, las capacidades existentes, las brechas y el panorama de riesgos.
- Fase III — Financiamiento sostenible y planificación de recursos: se traducen las prioridades estratégicas en recursos financieros, humanos y materiales sostenibles.
- Fase IV — Producción de la estrategia: se redacta el documento, se consulta con los actores relevantes, se obtiene la aprobación formal y se comunica públicamente.
- Fase V — Implementación: se desarrolla el plan de acción, se asignan responsables, recursos, plazos e indicadores.
- Fase VI — Monitoreo y evaluación: se mide el avance, se evalúan resultados y se revisa la estrategia para mantenerla vigente.

La primera lección práctica es la gobernanza. La guía recomienda una autoridad líder con mandato claro y capacidad real para coordinar a los distintos actores. Esta autoridad no necesariamente ejecuta todas las actividades; su función es asegurar dirección, coordinación y rendición de cuentas.

La segunda lección es que el diagnóstico debe preceder a las prioridades. Antes de decidir inversiones, es necesario mapear actores, responsabilidades, activos críticos, legislación, capacidades de respuesta, programas educativos, iniciativas de investigación, acuerdos internacionales y amenazas.

La tercera es financiera. Una estrategia sin presupuesto termina siendo una declaración de intenciones. El documento recomienda integrar la ciberseguridad en los procesos nacionales de presupuesto e inversión, considerar costos de operación y renovación y priorizar iniciativas que puedan financiarse de manera completa.

Finalmente, el ciclo debe cerrarse con medición. La tercera edición propone indicadores SMART y revisiones programadas, incluyendo controles intermedios y renovaciones periódicas. La estrategia debe ser tratada como un marco vivo, no como un documento estático.

3. Los diez principios transversales

La guía propone diez principios que deben acompañar todas las fases de la estrategia. No constituyen una lista de prioridades rígidas; funcionan como criterios de diseño para mantener coherencia.

- Visión: una visión clara de gobierno y sociedad completa qué se quiere proteger y hacia dónde se quiere avanzar.
- Enfoque integral y prioridades adaptadas: la estrategia debe considerar el ecosistema digital completo, pero responder a las circunstancias nacionales.
- Inclusión: deben participar gobierno, empresas, operadores de infraestructura, academia, sociedad civil y otros actores relevantes.
- Prosperidad económica y social: la ciberseguridad debe habilitar el desarrollo digital, no convertirse en un objetivo aislado.
- Derechos humanos fundamentales: privacidad, libertad de expresión, protección de datos y debido proceso deben formar parte del diseño.
- Gestión del riesgo y resiliencia: el riesgo no desaparece; se identifica, prioriza, mitiga y acepta de forma informada.
- Instrumentos de política adecuados: legislación, regulación, estándares, certificación, incentivos, educación e intercambio de información deben combinarse según el objetivo.

- Liderazgo, roles y recursos claros: las responsabilidades y los recursos deben estar explícitamente asignados.
- Entorno de confianza: la población y las organizaciones deben poder confiar en los servicios digitales.
- Prospectiva tecnológica y adaptabilidad: la estrategia debe anticipar cambios tecnológicos y revisar sus políticas.

Dos principios merecen especial atención para los estudiantes. Primero, la resiliencia: proteger no significa impedir todo incidente, sino preparar a las organizaciones y servicios para resistir, responder y recuperarse. Esto implica continuidad de negocio, recuperación ante desastres y gestión de crisis.

Segundo, la prospectiva tecnológica. La guía incorpora como principio nuevo la necesidad de observar tecnologías como inteligencia artificial, automatización, IoT, computación cuántica, 5G/6G y tecnologías de registro distribuido. La cuestión no es adoptar o rechazar una tecnología de forma automática, sino comprender cómo modifica el perfil de riesgo y ajustar la estrategia.

En conjunto, estos principios obligan a superar una visión reduccionista. Una estrategia técnicamente sofisticada puede fracasar si carece de liderazgo, presupuesto, legitimidad, coordinación o confianza.

4. Gobernanza, infraestructura crítica y servicios esenciales

La gobernanza constituye el punto de unión entre la política y la ejecución. La guía recomienda apoyo al más alto nivel de gobierno, una autoridad nacional competente y mecanismos de coordinación que permitan distribuir responsabilidades sin generar vacíos ni duplicidades.

La protección de infraestructura crítica (CI), infraestructura crítica de información (CII) y servicios esenciales (ES) ocupa un lugar central. El documento reconoce que no existe una definición universal: cada país debe establecer sus categorías según su contexto, evaluación de riesgos y prioridades. Entre los ejemplos aparecen redes eléctricas, agua, transporte, telecomunicaciones, sistemas SCADA, centros de datos, hospitales, bancos centrales y otros servicios cuya interrupción produciría efectos relevantes.

El elemento decisivo es la interdependencia. Una falla en telecomunicaciones puede afectar salud; una interrupción energética puede paralizar centros de datos; un incidente contra un proveedor tecnológico puede repercutir simultáneamente en miles de organizaciones. Por ello, la identificación de infraestructura crítica debe considerar dependencias, redundancias, impacto y efectos en cascada.

La guía recomienda un proceso formal, repetible y basado en criterios para identificar CI/CII/ES y mantener un registro nacional de sectores, funciones, operadores y activos críticos. Este registro debe revisarse periódicamente o después de incidentes importantes y cambios tecnológicos.

Para los operadores se proponen líneas base de ciberseguridad proporcionales al riesgo. Un punto particularmente relevante es el enfoque orientado a resultados: en lugar de imponer permanentemente una tecnología concreta, la regulación debería definir el resultado de seguridad esperado. Esto permite adaptarse a nuevas tecnologías y evita que la normativa quede obsoleta.

En la práctica, la protección de infraestructura crítica requiere combinar regulación, auditorías, autoevaluaciones, reporte obligatorio, certificaciones, incentivos y asociaciones público-privadas. El objetivo no es aumentar controles por aumentar controles, sino conseguir que los operadores mantengan capacidades reales de prevención, detección, respuesta, continuidad y recuperación.

5. Gestión nacional del riesgo cibernético

La gestión del riesgo es el mecanismo que permite convertir información sobre amenazas y vulnerabilidades en decisiones de inversión y protección. La guía propone desarrollar un enfoque nacional coherente, capaz de conectar las evaluaciones sectoriales y organizacionales con la toma de decisiones estratégica.

El punto de partida consiste en identificar activos digitales, dependencias, vulnerabilidades y amenazas, y estimar la probabilidad y el impacto de posibles incidentes. La evaluación debe

ser dinámica: debe incorporar inteligencia de amenazas, factores geopolíticos, dependencias transfronterizas y riesgos derivados de tecnologías emergentes.

Un elemento destacado es el registro nacional de riesgos. Este registro debe mantenerse actualizado y permitir a las autoridades obtener una visión estratégica sin exponer innecesariamente información operativa sensible. Debe considerar niveles de riesgo, tolerancia, responsabilidades para su tratamiento y mecanismos de escalamiento.

La guía recomienda una metodología común basada, cuando sea posible, en estándares internacionales. Esa metodología debe cubrir el ciclo completo: valoración de activos, identificación de amenazas, estimación del riesgo, definición del apetito y tolerancia, tratamiento, mantenimiento de controles y aceptación del riesgo residual.

Una buena gestión nacional del riesgo también exige retroalimentación. Los resultados de incidentes, ejercicios y auditorías deben volver al proceso de identificación de riesgos. De esta manera, la estrategia aprende de la experiencia y evita repetir supuestos que ya demostraron ser incorrectos.

Desde la perspectiva profesional, esto tiene una consecuencia importante: el riesgo cibernético no debe expresarse únicamente como número de vulnerabilidades o cantidad de incidentes. La pregunta relevante es qué funciones sociales o económicas podrían verse afectadas, cuánto tiempo podrían interrumpirse, qué dependencias provocarían efectos en cascada y qué inversiones reducen de manera significativa ese impacto.

La gestión del riesgo, por tanto, funciona como lenguaje común entre especialistas técnicos, directivos, reguladores y responsables políticos. Permite justificar prioridades con criterios comparables y orientar los recursos hacia las oportunidades de reducción de riesgo más relevantes.

6. Respuesta a incidentes y resiliencia

Una estrategia nacional debe asumir que los incidentes ocurrirán. La diferencia entre un país vulnerable y uno resiliente está, en buena

medida, en la capacidad para detectar, coordinar, contener, recuperar y aprender de esos eventos.

La guía recomienda establecer capacidades nacionales de respuesta, normalmente mediante CERT, CSIRT o CIRT, complementadas por equipos sectoriales y organizacionales. Estas capacidades deben cubrir funciones proactivas y reactivas, incluyendo respuesta a incidentes, gestión de vulnerabilidades, conciencia situacional, inteligencia de amenazas, intercambio de información y transferencia de conocimiento.

También se destaca el papel de los SOC y de los PSIRT en el sector privado. La coordinación entre capacidades nacionales, sectoriales y empresariales es esencial porque los primeros minutos de un incidente suelen depender de la organización directamente afectada.

La planificación de contingencias debe integrarse con el marco nacional de gestión de emergencias y contemplar planes específicos para sectores críticos. Debe definir escalamiento, clasificación de incidentes, comunicaciones, prioridades y mecanismos de recuperación ante desastres.

El intercambio de información es otro componente esencial. La guía recomienda mecanismos formales e informales, incluyendo ISAC, ISAOs y asociaciones público-privadas. El intercambio debe ser bidireccional: el Estado debe aportar información útil para generar confianza y, al mismo tiempo, crear condiciones para que el sector privado comparta inteligencia y observaciones.

Los ejercicios permiten validar estos mecanismos. Simulaciones, ejercicios de mesa y ejercicios operativos ayudan a probar procedimientos, canales de comunicación y preparación de los equipos. Además, permiten descubrir dependencias entre sectores que pueden no resultar evidentes durante la operación normal.

Finalmente, los incidentes deben clasificarse según severidad e impacto, incluyendo efectos sobre servicios esenciales, población, infraestructura y sistemas interdependientes. Las lecciones aprendidas deben regresar al proceso de planificación, convirtiendo cada incidente en una oportunidad para mejorar la resiliencia nacional.

7. Capacidades, talento, conciencia, legislación y regulación

La tecnología por sí sola no crea ciberresiliencia. La guía dedica una atención considerable al factor humano: habilidades, educación, capacitación, conciencia e instituciones determinan si las políticas realmente funcionan.

El desarrollo de capacidades debe entenderse como un proceso continuo. Se recomiendan trayectorias educativas que conecten la formación inicial con programas avanzados, certificaciones, prácticas y oportunidades profesionales. También se destaca la necesidad de atraer y retener talento y de desarrollar programas adaptados a diferentes grupos y sectores.

La concienciación tampoco debe limitarse a campañas genéricas. Debe ajustarse a la audiencia y a los riesgos concretos: ciudadanos, funcionarios, directivos, operadores críticos, pequeñas empresas, profesionales técnicos y otros grupos requieren mensajes y capacidades diferentes.

En el ámbito jurídico, la guía plantea una visión integral. La legislación y regulación deben traducir los objetivos de política pública en obligaciones, competencias, mecanismos de supervisión y salvaguardas. Deben contemplarse cibercrimen, evidencia electrónica, protección de datos, debido proceso y derechos humanos.

La proporcionalidad es fundamental. Un marco jurídico efectivo debe ser suficientemente sólido para proteger a la sociedad, pero evitar duplicidades, cargas innecesarias o regulaciones que pierdan vigencia rápidamente. La armonización jurídica y la cooperación transfronteriza adquieren especial importancia porque los incidentes y las evidencias digitales no respetan fronteras.

Para los estudiantes del diplomado, la conclusión práctica es que un programa de cumplimiento no debe evaluarse solamente por la existencia de una norma. Debe preguntarse si la organización conoce sus obligaciones, tiene responsables, dispone de capacidades, reporta adecuadamente, puede demostrar cumplimiento y revisa sus controles cuando cambian los riesgos.

La combinación de talento, conciencia, regulación y capacidades institucionales constituye una capa de defensa que complementa las herramientas técnicas. Sin ella, incluso una arquitectura tecnológica avanzada puede ser difícil de sostener.

8. Cooperación internacional y adaptación tecnológica

El ciberespacio es transfronterizo. Una estrategia nacional, aunque se concentre en las prioridades internas, debe reconocer que proveedores, infraestructuras, delincuentes, datos, cadenas de suministro y servicios digitales pueden estar distribuidos en distintos países.

La tercera edición fortalece la relación entre ciberseguridad y política exterior. Recomienda participar en procesos internacionales sobre derecho y normas, medidas de fomento de la confianza, organismos de estandarización y redes especializadas. También promueve cooperación práctica entre CERT/CSIRT/CIRT, autoridades policiales y plataformas multiactor.

La cooperación internacional tiene una dimensión operativa. Compartir inteligencia, coordinar respuestas, facilitar investigaciones y fortalecer capacidades entre países puede reducir tiempos de respuesta y limitar impactos. Los ejercicios internacionales también ayudan a probar dependencias que un ejercicio puramente nacional no puede revelar.

La adaptación tecnológica aparece como una obligación permanente. La estrategia debe incorporar mecanismos de prospectiva y observación del horizonte para anticipar cambios. Inteligencia artificial, automatización, IoT, computación cuántica, 5G/6G y tecnologías de registro distribuido pueden generar nuevas oportunidades, pero también modificar amenazas y vulnerabilidades.

La idea no es predecir el futuro con precisión. Es construir una capacidad institucional para detectar señales tempranas, evaluar escenarios y ajustar políticas antes de que los cambios tecnológicos se conviertan en problemas difíciles de gestionar.

Esto conduce a una visión de la estrategia como sistema adaptativo. Una NCS debe poder cambiar sin perder su dirección. Por eso son

importantes las revisiones, los indicadores, la evaluación de resultados, la participación de industria y academia y los mecanismos que convierten la experiencia en decisiones.

En un diplomado de ciberseguridad, este enfoque resulta especialmente útil: la competencia profesional no consiste únicamente en dominar tecnologías actuales, sino en comprender cómo los cambios tecnológicos alteran el riesgo y cómo traducir esa comprensión en decisiones de seguridad, gobierno y resiliencia.

9. Conclusiones ejecutivas para el profesional de ciberseguridad

La tercera edición de la guía plantea una idea central: una estrategia nacional de ciberseguridad solo tiene valor cuando logra conectar visión, riesgo, gobernanza, recursos, capacidades y resultados. El documento no ofrece una receta idéntica para todos los países; propone un marco adaptable al contexto nacional.

- La ciberseguridad debe integrarse con el desarrollo digital y socioeconómico.
- Las prioridades deben surgir de una evaluación nacional y sectorial del riesgo.
- La gobernanza debe asignar autoridad, responsabilidades y rendición de cuentas.
- La infraestructura crítica y los servicios esenciales requieren protección basada en riesgo e interdependencias.
- La respuesta a incidentes debe integrar capacidades nacionales, sectoriales y privadas.
- El talento y la capacitación deben financiarse como inversiones permanentes.
- La legislación debe equilibrar seguridad, proporcionalidad, privacidad, derechos humanos y cooperación.
- La cooperación internacional es parte de la resiliencia nacional, no un complemento opcional.
- El financiamiento debe cubrir todo el ciclo de vida, incluidos operación, mantenimiento y renovación.
- La estrategia debe medirse, revisarse y adaptarse.

Para un profesional de ciberseguridad, la principal lección es que la madurez no se mide por la cantidad de herramientas adquiridas, sino por la capacidad de una organización o un país para entender sus

riesgos, priorizar, coordinar, responder y aprender. El SOC, el CSIRT, el SIEM, la gestión de vulnerabilidades o los controles de acceso son piezas importantes, pero su valor depende del gobierno que los orienta y del riesgo que buscan reducir.

La guía también deja una advertencia práctica: una estrategia sin recursos, responsables e indicadores puede convertirse en un documento declarativo. Por el contrario, una estrategia con prioridades realistas, financiación sostenible, mecanismos de coordinación y revisiones periódicas puede convertirse en un instrumento de transformación.

Como conclusión académica, el enfoque de la NCS Guide 2025 puede resumirse en cinco verbos: comprender, priorizar, proteger, responder y aprender. Comprender el ecosistema digital y sus dependencias; priorizar los riesgos que realmente importan; proteger los activos y servicios críticos; responder de manera coordinada; y aprender de incidentes, ejercicios, auditorías y cambios tecnológicos.