Marco Nacional de
Formación de Fuerza Laboral en Ciberseguridad

OEA
Más derechos para más gente

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

RESUMEN EJECUTIVO

La acelerada transformación digital, exacerbada por la pandemia, ha incrementado significativamente las amenazas cibernéticas. Esto ha generado una demanda urgente de profesionales en ciberseguridad, mientras que la escasez de personal capacitado se ha vuelto una preocupación crítica. Costa Rica ha experimentado ciberataques significativos, como el ataque de ransomware de 2022 a instituciones gubernamentales, subrayando la necesidad de una fuerza laboral preparada para prevenir y responder a tales incidentes.

El *Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad de Costa Rica* ofrece una propuesta recomendatoria estructurada en áreas estratégicas para construir una fuerza laboral sólida en ciberseguridad. Alineado con la Estrategia Nacional de Ciberseguridad 2023-2027 de Costa Rica, el marco responde a la creciente importancia de la ciberseguridad en un mundo cada vez más digitalizado y con mayores amenazas cibernéticas.

El marco se articula en torno a cinco áreas estratégicas:

Administración y Gobernanza: fortalecer las estructuras de gestión y liderazgo en ciberseguridad, asegurando una administración sólida y la sostenibilidad de las iniciativas.

Concientización y Cultura: promover una cultura de ciberseguridad en toda la sociedad, sensibilizando y capacitando a la población para reducir los riesgos y amenazas.

Currículo y Programas Escolares: incorporar la ciberseguridad en la educación primaria y secundaria, adaptando el currículo escolar para desarrollar habilidades digitales desde temprana edad.

Educación Terciaria e Investigación: fortalecer la formación universitaria y la investigación en ciberseguridad, formando especialistas y promoviendo la innovación en el área.

Entrenamiento y Certificación: garantizar la capacitación y certificación continua de los profesionales, manteniendo sus conocimientos alineados con los estándares internacionales.

Para el desarrollo de una fuerza laboral en ciberseguridad, el documento identifica cinco desafíos críticos:

1. **Reducción de Brechas Digitales:** Disparidades en el acceso a la tecnología y conectividad, especialmente en áreas rurales y entre géneros.
2. **Fortalecimiento del Bilingüismo:** La falta de dominio del inglés limita el acceso a recursos y oportunidades en ciberseguridad.
3. **Incorporación Temprana de la Ciberseguridad en la Educación:** La falta de educación en ciberseguridad en los primeros niveles educativos obstaculiza la formación integral de futuros profesionales.
4. **Fomento de Conocimiento sobre el Potencial Laboral:** Poca visibilidad de las oportunidades y beneficios del sector de ciberseguridad.
5. **Sensibilización General:** Falta de conciencia sobre la importancia de la ciberseguridad entre la población.

El marco presenta recomendaciones específicas en cada área estratégica para superar estos desafíos y construir una fuerza laboral en ciberseguridad. **A continuación, se destacan algunas de las recomendaciones clave:**

Administración y Gobernanza:

- **Marco Regulatorio:** Crear un marco regulatorio que respalde la *Estrategia Nacional de Ciberseguridad* y legitime las decisiones de implementación.
- **Financiamiento para Infraestructura:** Asignar fondos para implementar infraestructura tecnológica avanzada en centros educativos y establecer centros especializados en ciberseguridad en zonas rurales.
- **Diálogo Público-Privado:** Fomentar el diálogo entre organismos públicos y el sector privado para establecer estándares de formación y asegurar que los programas educativos se adapten a las necesidades del mercado laboral.

Concientización y Cultura

- **Planificación Estratégica de Formación:** Convertir el interés en ciberseguridad en una formación estructurada, identificando competencias clave y educando a la población sobre los diversos roles en el sector.
- **Programas Inclusivos:** Crear programas inclusivos que aborden las brechas generacionales, de género, de acceso y de conectividad, promoviendo la equidad en la formación.

Currículo y Programa Escolar:

- **Enfoque STEAM:** Incluir la ciberseguridad dentro del enfoque STEAM desde los niveles iniciales, fomentando habilidades digitales, pensamiento crítico e integración de habilidades blandas y duras.
- **Competencias en Matemáticas:** Mejorar las competencias en matemáticas y pensamiento computacional desde el nivel inicial para preparar a los estudiantes para una formación en ciberseguridad.

Educación Terciaria e Investigación:

- **Actualización en Formación Docente:** Modernizar los planes de formación docente en todos los niveles educativos para incluir temas de ciberseguridad y brindar actualizaciones continuas.
- **Impulso a la Investigación en Ciberseguridad:** Generar datos, estadísticas e investigación en ciberseguridad que reflejen el contexto nacional y orienten las políticas del sector.

Entrenamiento y Certificación:

- **Estandarización de Certificaciones:** Unificar los criterios mínimos para la certificación nacional en ciberseguridad, asegurando que cumplan con estándares de calidad y relevancia.
- **Estandarización de Roles:** Estandarizar los roles existentes en ciberseguridad, definiendo claramente sus responsabilidades, competencias y límites para evitar improvisación en esta área.

Para la implementación de las recomendaciones, el marco propone un **cronograma organizado en tres fases y dividiendo las acciones en corto, mediano y largo plazo:**

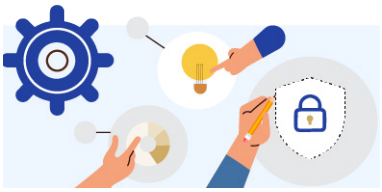
Corto Plazo:	Mediano Plazo:	Largo Plazo:
Creación del marco regulatorio, asignación de presupuesto, establecimiento del diálogo público-privado y lanzamiento de campañas de sensibilización.	Presentación formal del marco regulatorio, fortalecimiento del bilingüismo, alineación de certificaciones con estándares internacionales e impulso a la investigación nacional.	Implementación completa del marco regulatorio, desarrollo de proyectos de infraestructura, adopción de currículos actualizados y reducción de las brechas digitales.

Para asegurar la sostenibilidad del marco, se recomienda establecer un sistema de financiamiento continuo, destinado a proyectos de ciberseguridad y desarrollo de infraestructura, y una actualización constante del currículo y los estándares de certificación. Además, se recomienda fomentar la colaboración entre el sector público y privado mediante alianzas estratégicas, asegurando que el marco evolucione de acuerdo con las necesidades del sector y mantenga la preparación del país frente a nuevas amenazas cibernéticas.

TABLA DE CONTENIDOS

INTRODUCCIÓN

En la era post pandémica, el mundo ha experimentado una transformación acelerada hacia la digitalización, marcada por un aumento considerable del teletrabajo y la dependencia de tecnologías digitales para la mayoría de las actividades económicas y sociales. Esta nueva normalidad ha ampliado el panorama de amenazas y riesgos cibernéticos, exponiendo a gobiernos, empresas y ciudadanos a un entorno digital cada vez más vulnerable. En este contexto, la creación de un Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad en Costa Rica se torna esencial para abordar de manera proactiva los desafíos emergentes.



1. Transformación del mercado laboral y demanda creciente de profesionales

Los mercados laborales están atravesando un período de profunda transformación, en el que las habilidades tecnológicas y la capacidad de adaptación son más valoradas que nunca. La ciberseguridad se ha posicionado como una de las áreas de mayor demanda, debido al aumento exponencial de ciberataques durante y después de la pandemia. Sin embargo, esta demanda ha revelado una preocupante escasez de personal capacitado. A nivel global y nacional, la falta de profesionales calificados en ciberseguridad pone en riesgo la capacidad de las organizaciones para defenderse de ataques cibernéticos complejos. Ante esta realidad, Costa Rica debe asumir un rol proactivo para cerrar esta brecha mediante el desarrollo y ejecución de un marco de formación que impulse la generación de talento especializado en ciberseguridad.

2. Escasez de personal calificado en ciberseguridad

La escasez de personal especializado en ciberseguridad es un problema mundial que afecta tanto a países desarrollados como en vías de desarrollo. En Costa Rica, esta escasez se traduce en una vulnerabilidad ante ciberamenazas que pueden comprometer la estabilidad económica, la seguridad pública y la confianza en los sistemas digitales. La creación de un Marco Nacional de Formación de Fuerza Laboral es esencial para responder a esta necesidad urgente, asegurando la capacitación de profesionales altamente calificados que puedan integrarse en diversos sectores, desde la administración pública hasta la industria privada. Abordar esta escasez no solo es un imperativo para proteger la infraestructura digital del país, sino también una oportunidad para fomentar la creación de empleos bien remunerados y promover la innovación tecnológica.

3. Ciberataques recientes en Costa Rica: una amenaza nacional urgente

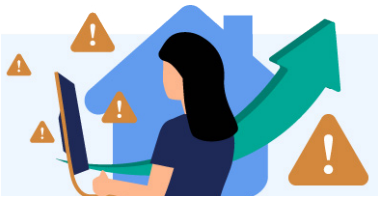
Costa Rica ha sido testigo directo de la creciente vulnerabilidad a los ciberataques. En 2022, el país sufrió uno de los ciberataques más graves de su historia, cuando un grupo de ransomware internacional comprometió sistemas clave del gobierno, afectando la funcionalidad de instituciones como el Ministerio de Hacienda, la Caja Costarricense de Seguro Social (CCSS) y otras entidades críticas. Este ataque tuvo consecuencias económicas y sociales devastadoras, con interrupciones en servicios esenciales, pérdida de datos y una desestabilización de la confianza pública en la infraestructura digital. Asimismo, el pasado dos de diciembre de 2024 el país sufrió otro ciberataque a la Refinadora Costarricense de Petróleo (**RECOPE**), la **Dirección de Migración y Extranjería** y la empresa de comunicación masiva, **Repretel**. Estos incidentes subrayan la urgencia de contar con una fuerza laboral en ciberseguridad preparada para detectar, prevenir y responder ante ataques similares en el futuro. La falta de personal capacitado en ciberseguridad hace que el país sea más susceptible a estos ataques, los cuales podrían aumentar en número y complejidad si no se toman medidas inmediatas.

4. Mitigación de riesgos y fortalecimiento de la resiliencia nacional

En este panorama de amenazas cibernéticas crecientes, es imperativo que las naciones promuevan el desarrollo de su fuerza laboral en ciberseguridad para mitigar los riesgos y abordar las amenazas emergentes. El Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad en Costa Rica permitirá estructurar un plan de acción que potencie las competencias de los profesionales en ciberseguridad y refuerce la capacidad del país para enfrentar ataques cibernéticos de forma coordinada y efectiva. Al fortalecer la resiliencia nacional, Costa Rica podrá proteger sus infraestructuras críticas, salvaguardar su economía digital y preservar la confianza del público en los servicios digitales, pilares esenciales para el desarrollo sostenido del país en la era digital.

5. Oportunidades para la competitividad y el liderazgo regional

Finalmente, la implementación del Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad en Costa Rica no solo abordaría las amenazas actuales, sino que también podría posicionar a Costa Rica como un referente regional en el desarrollo de talento especializado. En un contexto donde la demanda global de profesionales de ciberseguridad sigue en aumento, contar con una fuerza laboral calificada abre oportunidades para que Costa Rica exporte talento y servicios en esta área estratégica. Esto no solo beneficiaría a la economía nacional, sino que también promovería la colaboración internacional en la lucha contra el cibercrimen y en la promoción de un ciberespacio más seguro.



6. La era del teletrabajo y la ampliación del panorama de amenazas

El teletrabajo, que antes de la pandemia era una modalidad limitada a ciertos sectores, se ha convertido en una práctica común que continúa ganando terreno. Si bien esta tendencia ha permitido a las empresas mantener su productividad, también ha incrementado la superficie de ataque para los actores malintencionados. La infraestructura digital de las organizaciones y los dispositivos personales conectados desde ubicaciones remotas son objetivos atractivos para los ciberataques. En este escenario, contar con una fuerza laboral capacitada en ciberseguridad es crítico para mitigar los riesgos asociados a la expansión de la actividad digital y garantizar que tanto las empresas como los ciudadanos operen en un entorno seguro.

PROPÓSITO Y METAS

El presente Marco constituye un documento recomendatorio alineado con la Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027 que tiene como objetivo la generación tanto de fuerza laboral en ciberseguridad en el país como la constitución y consolidación de una fuerza laboral cibersegura, lo cual contribuye a la construcción de una sociedad cibersegura.

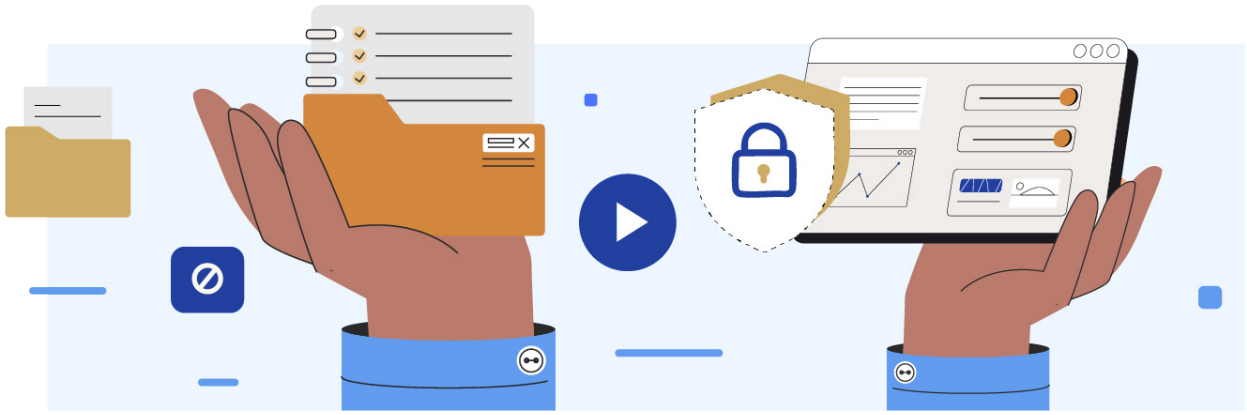
Este Marco cuenta con una visión y una misión detalladas a continuación:

Visión

El Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad busca crear una guía que facilite la construcción de una sociedad resiliente y cibersegura, en la cual tanto individuos como organizaciones cuenten con las habilidades y conocimientos necesarios para identificar, enfrentar y mitigar de manera proactiva y efectiva las amenazas cibernéticas. Este objetivo incluye el fortalecimiento continuo de la seguridad digital a nivel personal, profesional e institucional, promoviendo una cultura de prevención y respuesta ante los desafíos cibernéticos del presente y del futuro.

Misión

La misión del Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad es crear una hoja de ruta comprehensiva para el desarrollo de programas educativos integrales, inclusivos y accesibles que fomenten el desarrollo de competencias en ciberseguridad en todas las etapas de la vida. Desde la educación primaria hasta la formación profesional continua y la jubilación, estos programas estarían diseñados para empoderar a la ciudadanía, promoviendo el conocimiento crítico y técnico necesario para navegar en entornos digitales seguros. Asimismo, se pone especial énfasis en la inclusión de poblaciones vulnerables y en la promoción de la diversidad, garantizando que todas las personas tengan la oportunidad de adquirir habilidades en ciberseguridad y contribuir activamente a un entorno digital más seguro.



OBJETIVOS Y PRINCIPIOS DEL MARCO NACIONAL DE FORMACIÓN DE FUERZA LABORAL EN CIBERSEGURIDAD

Objetivos:

Desarrollo de una Fuerza Laboral de Ciberseguridad

El primer objetivo se centra en fomentar el desarrollo e implementación de programas educativos robustos que preparen a profesionales altamente capacitados para cubrir la creciente demanda de expertos en ciberseguridad. Estos programas deben incluir tanto formación técnica avanzada como habilidades prácticas, adaptándose a las tendencias emergentes y las nuevas amenazas digitales. El objetivo es asegurar que las organizaciones, empresas, organismos públicos y la sociedad en general cuenten con un capital humano capaz de proteger sus infraestructuras digitales y responder de manera eficiente a incidentes cibernéticos.

Desarrollo de una Fuerza Laboral Cibersegura

Este objetivo tiene como fin promover la formación continua y la concienciación en ciberseguridad no solo entre aquellos en roles técnicos, sino entre todos los empleados. Reconociendo que el factor humano es una de las principales vulnerabilidades en la ciberseguridad, es esencial que toda la fuerza laboral, independientemente de su rol, esté preparada para identificar riesgos y actuar de manera preventiva. Esto incluye programas de capacitación regulares, simulaciones y actualizaciones sobre las mejores prácticas para mitigar riesgos cibernéticos en el entorno laboral.

Fomento de una Sociedad Cibersegura

Fomentar una cultura de ciberseguridad en la sociedad es fundamental para garantizar que los individuos puedan protegerse a sí mismos y a sus comunidades en un entorno digital cada vez más complejo. Este objetivo implica la inclusión de la educación en ciberseguridad desde edades tempranas, así como campañas educativas dirigidas al público en general. Al empoderar a la ciudadanía con conocimientos en ciberseguridad, se contribuye a crear una sociedad más resiliente y consciente de las amenazas digitales.

Principios:

Colaboración multisectorial

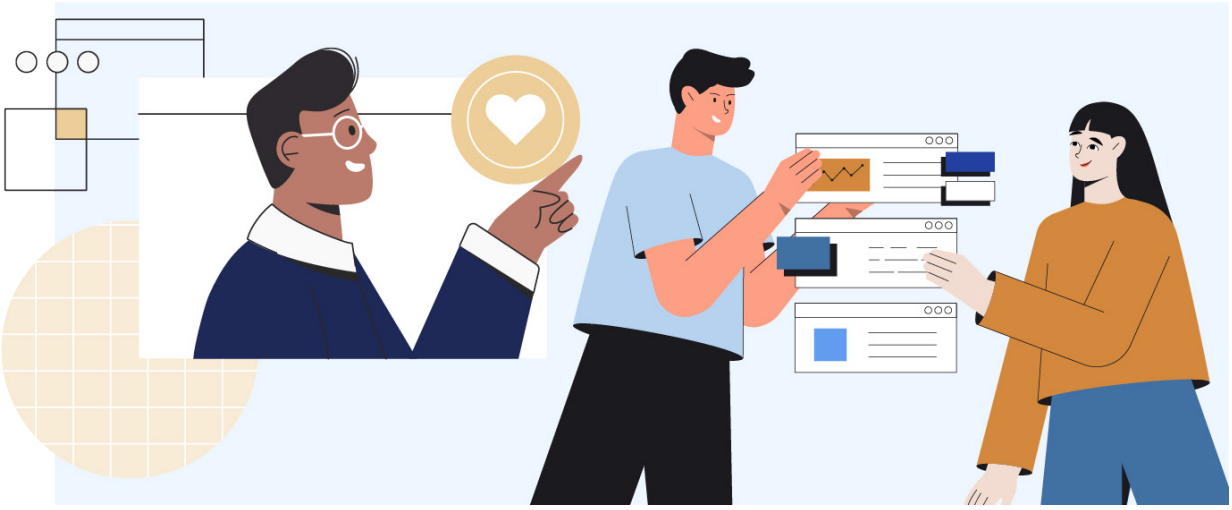
La colaboración entre la academia, las empresas, el gobierno y las organizaciones de la sociedad civil es crucial para que los programas de formación en ciberseguridad respondan a las necesidades reales del mercado laboral. Este objetivo promueve el establecimiento de alianzas estratégicas que faciliten el intercambio de conocimientos, la creación de estándares comunes y la implementación de programas de formación innovadores que reflejen las demandas actuales y futuras del sector.

Ética profesional

La ciberseguridad no se trata solo de habilidades técnicas, sino también de actuar con integridad y responsabilidad. Este objetivo busca integrar principios éticos y de responsabilidad social en todos los programas de formación en ciberseguridad. Es fundamental que los profesionales no solo se enfoquen en proteger sistemas, sino que también lo hagan respetando los derechos humanos, la privacidad y las normas legales, asegurando que el uso de tecnologías digitales sea siempre ético.

Investigación e innovación

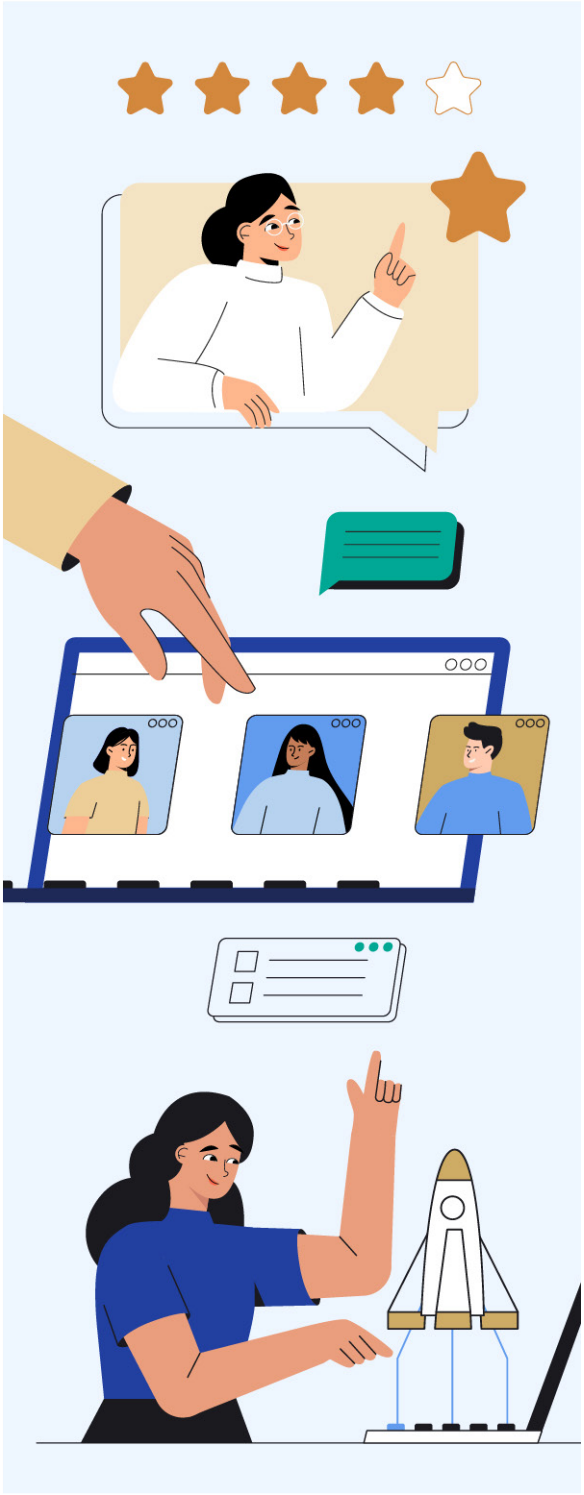
Finalmente, este objetivo incentiva la investigación y el desarrollo de nuevas tecnologías y métodos en ciberseguridad, promoviendo la innovación continua en el sector. A medida que las amenazas evolucionan, es necesario estar a la vanguardia en la creación de soluciones que respondan a desafíos emergentes. Al fomentar una cultura de innovación, se contribuye a la creación de un entorno digital más seguro y resiliente, con profesionales que lideren avances tecnológicos en el campo de la ciberseguridad.



Evaluación y adaptación
La implementación de un sistema continuo de evaluación permite que el marco de formación se mantenga relevante y eficaz en respuesta a las necesidades cambiantes de la ciberseguridad. Este principio busca asegurar una revisión periódica de las competencias, contenidos y metodologías, de manera que el marco pueda adaptarse rápidamente a nuevas amenazas, tecnologías y mejores prácticas. Mediante esta evaluación continua, la formación en ciberseguridad se alineará con los estándares internacionales y las exigencias locales, fortaleciendo la resiliencia y efectividad del sector.

Inclusión y diversidad
La construcción de una fuerza laboral diversa e inclusiva en ciberseguridad es esencial para abordar el complejo panorama de amenazas con perspectivas variadas e innovadoras. Este principio se enfoca en promover la participación de personas de diferentes géneros, etnias, y contextos socioeconómicos, fomentando un ambiente de aprendizaje y trabajo que valore y maximice la diversidad de pensamiento. Esto no solo enriquece las capacidades de respuesta y mitigación de amenazas, sino que también contribuye a una industria más equitativa y representativa de la sociedad.

Educación continua
En el contexto de ciberseguridad, donde los cambios son constantes, la educación continua es un principio fundamental. Este enfoque aboga por la creación de programas de actualización y especialización regulares, que permitan a los profesionales de ciberseguridad mantenerse al día con las últimas técnicas, herramientas y normativas. La educación continua refuerza una cultura de aprendizaje a lo largo de la vida, esencial para que la fuerza laboral no solo reaccione a las amenazas emergentes, sino que también adopte un papel proactivo en la protección y defensa de los activos digitales nacionales.



ALINEACIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2023-2027

El presente Marco se encuentra alineado con la Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027 tomando como base sus pilares, componentes y posibles líneas de intervención.

Pilares:

La **Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027** se sustenta en cinco pilares fundamentales que guían las acciones del país en su esfuerzo por fortalecer la ciberseguridad y garantizar la protección de sus ciudadanos y sus infraestructuras en el entorno cibernético. Estos pilares incluyen:

Pilar 1: Reforzar la gobernanza en ciberseguridad, optimizando la inversión pública y profundizando en la coordinación entre gobierno, industria, academia, sociedad y comunidad internacional.

Pilar 2: Adecuar el marco jurídico cibernético, promoviendo una cultura de cumplimiento y considerando las amenazas cibernéticas en evolución, los avances tecnológicos y las necesidades únicas de la Nación.

Pilar 3: Fortalecer la protección de infraestructuras y la ciber resiliencia nacional, protegiendo las infraestructuras críticas nacionales y gestionando adecuadamente los riesgos de ciberseguridad para que las partes interesadas puedan maximizar los beneficios del entorno digital y la ciudadanía esté más segura en línea.

Pilar 4: Reforzar las capacidades del ecosistema de ciberseguridad, educando, capacitando, formando y concientizando a todas las múltiples partes interesadas y promoviendo la investigación y desarrollo de ciberseguridad así como promoviendo habilidades digitales y matemáticas básicas en poblaciones rurales.

Pilar 5: Cooperar en el entorno digital, construyendo alianzas público-privadas y ejerciendo ciber diplomacia en pro de un orden internacional más seguro, próspero y abierto.

El presente marco se focaliza en el cuarto pilar, que pone el énfasis en el desarrollo de capacidades y la formación de una fuerza laboral especializada en ciberseguridad. Este pilar propone que

> *Costa Rica desarrollará una fuerza laboral capacitada en ciberseguridad a través de programas de educación, capacitación y formación, promoverá la conciencia de ciberseguridad entre el público y fomentará una cultura de comportamiento en línea responsable y seguro. De igual manera, promoverá la investigación y desarrollo de ciberseguridad para fomentar la innovación, mejorar las capacidades y mantenerse a la vanguardia de las amenazas cibernéticas en evolución. Este pilar enfatiza la importancia del desarrollo del capital humano y la participación pública, el cierre de la brecha de género en la fuerza laboral, así como el desarrollo de tecnologías, herramientas y metodologías de vanguardia para fortalecer las defensas nacionales de ciberseguridad."*

Dicho pilar establece diversas líneas de acción que se verán reflejadas en las recomendaciones presentes en el presente Marco.

En ese contexto, el Marco presentará recomendaciones en torno a potenciar las habilidades vinculadas de forma directa o indirecta con la ciberseguridad en los diversos niveles educativos a partir de propuestas transversales que tengan como objetivo general disminuir las diversas brechas digitales, con especial énfasis las de género. Se considera esencial que el desarrollo de la fuerza laboral en ciberseguridad en Costa Rica adopte un enfoque integral que incluya investigación y desarrollo, así como un diálogo constante y relevante entre el sector público y el privado. Esto también permitirá que el sector público comprenda las necesidades del sector privado.

ÁREAS ESTRATÉGICAS DEL MARCO NACIONAL DE FORMACIÓN DE FUERZA LABORAL EN CIBERSEGURIDAD

El presente Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad de Costa Rica toma como referencia cinco áreas estratégicas (Figura 1) seleccionadas considerando indicadores de madurez en ciberseguridad, al igual que las prioridades estipuladas en la Estrategia Nacional de Ciberseguridad 2023-2027, la cual establece un plan de acción integral para proteger la infraestructura digital del país y garantizar la seguridad en el entorno cibernético. Estas áreas estratégicas son clave para la implementación del Marco, ya que permiten desarrollar las competencias necesarias en la fuerza laboral para enfrentar los desafíos de ciberseguridad tanto a nivel nacional como internacional.

Por el otro lado, la alineación con la Estrategia Nacional de Ciberseguridad no solo garantiza que las acciones formativas estén orientadas a responder a las amenazas actuales, sino que también asegura que los esfuerzos en capacitación y desarrollo profesional sean coherentes con los objetivos nacionales a largo plazo. Al adoptar estos componentes como base, el Marco contribuye directamente al cumplimiento de los objetivos prioritarios de la estrategia, que incluyen la protección de infraestructuras críticas, la creación de una cultura de seguridad digital y la promoción de un ecosistema colaborativo entre los sectores público, privado y académico.

En particular, la Estrategia Nacional de Ciberseguridad 2023-2027 identifica la formación de talento especializado y la concientización de la ciudadanía como pilares fundamentales para fortalecer la seguridad digital del país. Por lo tanto, la alineación entre el Marco Nacional de Formación de Fuerza Laboral y esta estrategia no solo garantiza que Costa Rica cuente con una fuerza laboral preparada y bien equipada, sino que también asegura que dicha fuerza laboral esté en sintonía con los objetivos de la estrategia. Esto permitirá enfrentar eficazmente los retos de seguridad digital, promoviendo así el desarrollo económico y la confianza en los sistemas digitales.

Áreas estratégicas tomadas como referencia :

Figura 1: Áreas estratégicas para la formación de fuerza laboral en ciberseguridad. Fuente: OEA/CICTE.

Administración y Gobernanza:

La ciberseguridad requiere una sólida estructura de gestión y liderazgo que articule esfuerzos y recursos a nivel nacional. Esta área busca fortalecer los procesos de administración y gobernanza en ciberseguridad, asegurando que las políticas y normativas estén alineadas con las necesidades de Costa Rica. Contar con una administración sólida facilita la implementación de directrices claras y asegura la sostenibilidad de las iniciativas en ciberseguridad, permitiendo la continuidad y la adaptación a los cambios en el entorno digital.

Concientización y Cultura:

La construcción de una cultura de ciberseguridad es esencial para que la sociedad comprenda la importancia de proteger la información y los sistemas digitales. Esta área estratégica se enfoca en sensibilizar y capacitar a toda la población, incluyendo sectores fuera del ámbito técnico, como parte de un esfuerzo integral por reducir los riesgos y amenazas cibernéticas. Fomentar una cultura de ciberseguridad ayuda a fortalecer la resiliencia en todos los niveles y contribuye a un entorno digital más seguro y consciente de los riesgos.

Currículo y Programas Escolares:

Incorporar contenidos de ciberseguridad desde la educación primaria y secundaria es fundamental para preparar a las nuevas generaciones y despertar su interés en esta área. Esta área estratégica se centra en adaptar y enriquecer el currículo escolar, promoviendo el desarrollo de habilidades digitales básicas y avanzadas en los estudiantes. De esta forma, se busca no solo generar conocimiento en ciberseguridad, sino también motivar a jóvenes talentos a considerar carreras en este ámbito, creando una base temprana de profesionales en la materia.

Educación Terciaria e Investigación:

En un mundo donde las amenazas cibernéticas evolucionan constantemente, la investigación y el desarrollo académico en ciberseguridad son indispensables. Esta área se centra en fortalecer programas de grado y posgrado que formen especialistas en ciberseguridad y fomenten la investigación aplicada. Así, se promueve la creación de conocimiento especializado y la innovación en ciberseguridad, facilitando que Costa Rica esté a la vanguardia en técnicas de defensa y prevención frente a amenazas complejas.

Entrenamiento y Certificación:

La capacitación y certificación continua en ciberseguridad aseguran que los profesionales en este campo mantengan sus conocimientos actualizados y cumplan con los estándares internacionales. Esta área busca establecer programas de entrenamiento y certificación que validen la competencia y la especialización de los profesionales en ciberseguridad, garantizando así una fuerza laboral cualificada y preparada para enfrentar los desafíos actuales y futuros en este campo.

Cada una de estas áreas estratégicas ha sido seleccionada por su rol clave en la construcción de una fuerza laboral sólida y competente en ciberseguridad, asegurando una cobertura integral que aborde tanto la prevención como la respuesta ante los retos de la era digital en Costa Rica.

ESTADO DE SITUACIÓN

A partir de un taller organizado por la OEA/CICTE en junio de 2024, al igual que entrevistas posteriores con actores clave (Anexo 2), se identificaron cinco retos importantes para la formación de una fuerza laboral sólida en ciberseguridad en Costa Rica, los cuales se detallan en la Figura 2.

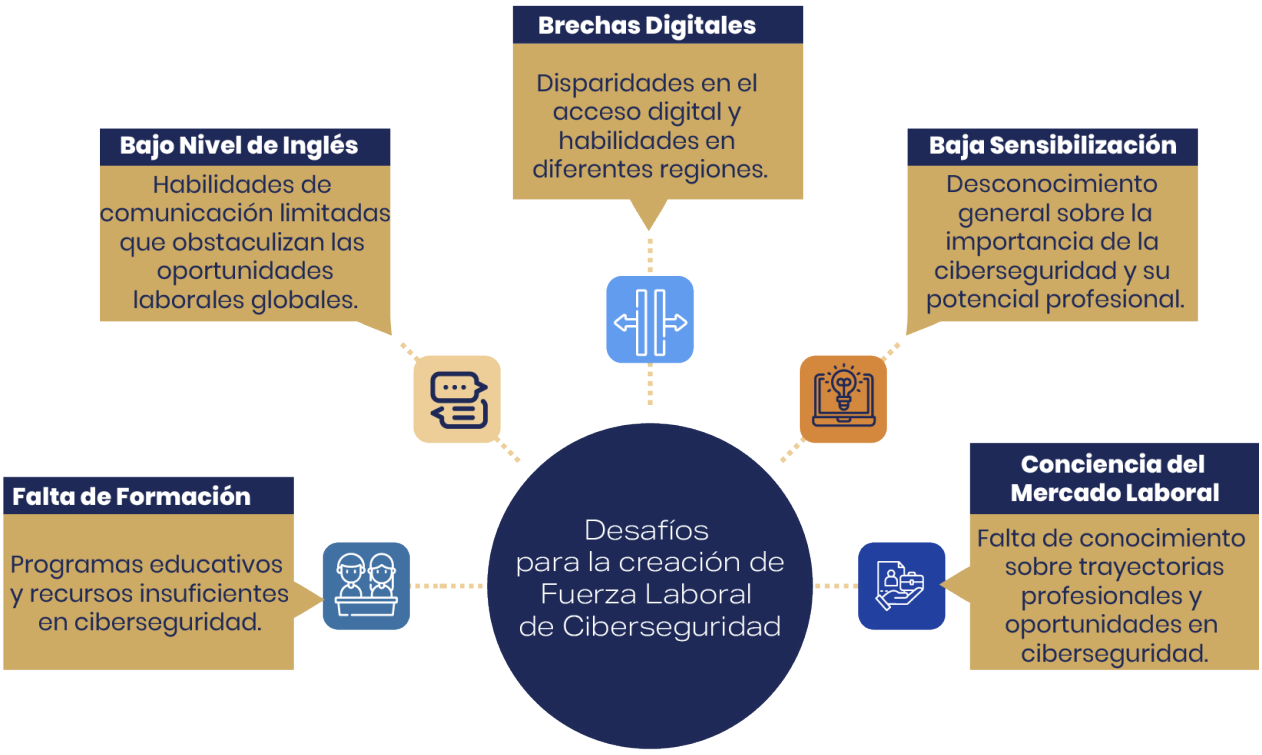
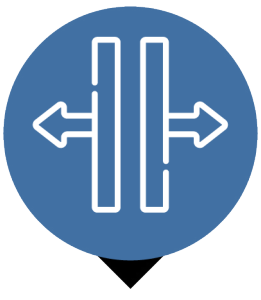


Figura 2: desafíos para la formación en ciberseguridad. Fuente: OEA/CICTE.

Brechas Digitales: Existen disparidades relevantes en el acceso a tecnologías e infraestructura digital, especialmente entre zonas urbanas y rurales, y entre géneros. Las áreas rurales tienen menor conectividad, recursos y centros de formación y práctica, lo cual limita el acceso a oportunidades en ciberseguridad para quienes residen fuera del Gran Área Metropolitana (GAM). Además, la brecha de género también es evidente en la tecnología y la ciberseguridad, con una menor representación femenina en estos campos, lo que plantea un reto para lograr una fuerza laboral diversa e inclusiva.



Bajo Nivel de Inglés: En ciberseguridad, el dominio del inglés es fundamental, ya que la mayor parte de los recursos técnicos, certificaciones y ofertas de empleo están en este idioma. Sin embargo, en Costa Rica, las escuelas públicas suelen ofrecer una formación en inglés insuficiente para cumplir con las demandas del sector. Esto crea una brecha que limita el acceso de muchos estudiantes a empleos bien remunerados y podría incluso la competitividad del país en el ámbito internacional.

Falta de Formación Integral desde el Nivel Inicial: La ciberseguridad no es una temática presente en los primeros niveles de la educación, y tampoco se aborda de forma transversal en el currículo escolar. Iniciar desde temprana edad con una formación en ciberseguridad, que abarque desde habilidades digitales hasta el conocimiento de los riesgos en el entorno virtual, es clave para desarrollar una comprensión profunda y preparar a las futuras generaciones para los desafíos de un mundo digitalizado.

Falta de Conciencia sobre el Potencial Laboral y los Beneficios del Sector: En general, no se percibe la ciberseguridad como una opción de carrera prometedora. La falta de información sobre la demanda creciente de profesionales en este campo y sobre los buenos salarios que ofrece este sector genera una baja atracción hacia esta área de formación. Crear conciencia sobre las ventajas laborales y salariales de la ciberseguridad ayudaría a atraer a más jóvenes y a diversificar la fuerza laboral en este campo.

Baja Sensibilización sobre la Importancia de la Ciberseguridad: Existe una falta de sensibilización general en la sociedad sobre la importancia de la ciberseguridad y su impacto en la vida cotidiana. Muchos ciudadanos desconocen los riesgos cibernéticos y la relevancia de contar con profesionales especializados para proteger la infraestructura digital del país. Incrementar la concienciación sobre estos temas contribuiría no solo a aumentar el interés en el área, sino también a fortalecer la seguridad digital en todos los niveles.

Estos desafíos resaltan la necesidad de una estrategia nacional para fomentar una fuerza laboral en ciberseguridad que sea inclusiva, bien formada y consciente de las oportunidades y beneficios de este sector.

Costa Rica ha realizado esfuerzos significativos para fortalecer su fuerza laboral en ciberseguridad, liderados por instituciones clave como el Ministerio de Educación Pública (MEP) y el Ministerio de Ciencia, Innovación, Tecnología y Comunicaciones (MICITT), que impulsan diversas iniciativas en esta área. No obstante, aún existen desafíos relacionados con la visibilidad de estas iniciativas, su alineación con las necesidades del mercado laboral y la equidad en el acceso a oportunidades de formación y empleo.

Desde el MEP, un logro fundamental es el desarrollo del **Marco Nacional de Cualificaciones**, que incluye componentes específicos de ciberseguridad. No obstante, la baja exigencia legislativa actual limita su obligatoriedad dentro de la propuesta curricular, lo que afecta su implementación uniforme en todos los niveles educativos y su efectividad como herramienta de formación.

El **Instituto Nacional de Aprendizaje (INA)** también desempeña un papel crucial, siendo el organismo responsable de la capacitación profesional de jóvenes mayores de 15 años en el país. El INA ha implementado diversas propuestas relacionadas con la ciberseguridad, adaptando sus programas para atender la demanda creciente de talento en esta área.

El MICITT, por su parte, enfrenta el desafío de fortalecer los vínculos entre el sector educativo y la **industria de ciberseguridad** para alinear las competencias formativas con las demandas del mercado laboral. La colaboración con el sector privado permitiría definir mejor los perfiles de puestos tanto en el ámbito público como privado, asegurando que los programas formativos respondan a las habilidades y competencias requeridas en el sector.

Otro actor clave es el **cybersec cluster**, que agrupa a las principales empresas del sector en el país y aboga por la mejora continua de procesos y estándares en la industria. Sin embargo, se observa la necesidad de una mayor planificación en la organización de trayectos profesionales y en la estandarización de perfiles de empleo en ciberseguridad en el sector privado. Por su parte, esto dificulta la adecuada planificación de la formación y la definición de las competencias prioritarias que deben desarrollarse para satisfacer la demanda laboral.

En ese contexto, se recomienda impulsar esfuerzos para sistematizar los avances logrados mediante legislación, diálogo intersectorial e inversión en estructura, con el objetivo de reducir las brechas previamente mencionadas.

Para apoyar estos esfuerzos, la Figura 3 ilustra los principales actores dentro del Marco Nacional de Formación de Fuerza Laboral en ciberseguridad, destacando las instituciones y organizaciones clave cuya colaboración y coordinación resultan esenciales para lograr una formación efectiva y alineada con las demandas del sector.

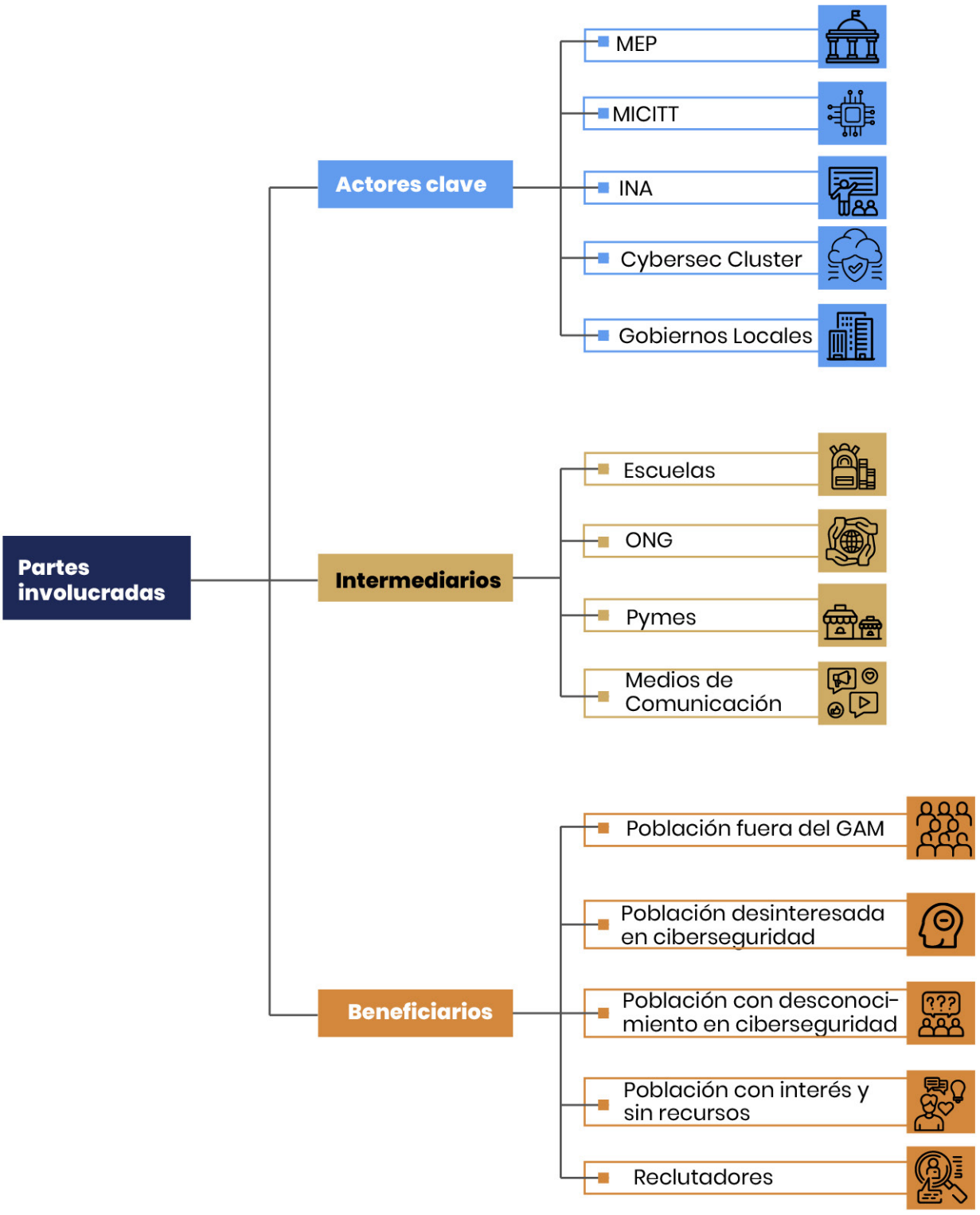
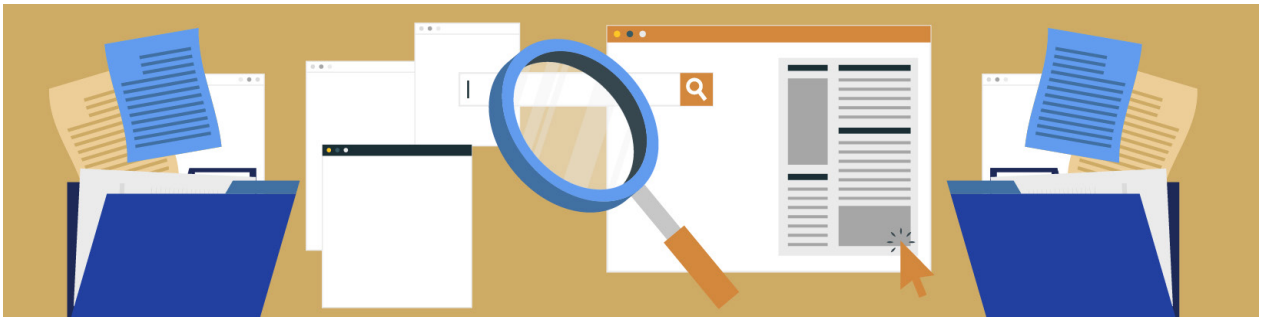


Figura 3: principales actores dentro del Marco Nacional de Formación de Fuerza Laboral en ciberseguridad. Fuente: OEA/CICTE

RECOMENDACIONES

Alineado con los objetivos de la Estrategia Nacional de Ciberseguridad 2023-2027, en base a las áreas y componentes detalladas en el presente Marco y a partir de lo observado e investigado en las intervenciones de campo, se proponen las siguientes recomendaciones por área:



ADMINISTRACIÓN Y GOBERNANZA

Dentro de la Administración y gobernanza, y teniendo en cuenta el objetivo de formar fuerza laboral en materia de ciberseguridad, se observan en Costa Rica los siguientes actores principales. Cabe señalar que, aunque estos actores fueron destacados durante las consultas, no son los únicos involucrados en este proceso.

- **Ministerio de Educación Pública**
- **INA (Instituto Nacional de Aprendizaje)**
- **MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones)**
- **Ministerio de Planificación Nacional y Política Económica (MIDEPLAN)**
- **Ministerio de Relaciones Exteriores y Culto (MREC)**
- **Gobiernos locales y municipales**
- **Consejo Nacional de Rectores (CONARE)**
- **Asociación Nacional de Educadores y Educadoras (ANDE)**
- **CSE (Consejo Superior de Educación)**
- **Marco Nacional de Cualificaciones**
- **Procomer**
- **Servicio civil**

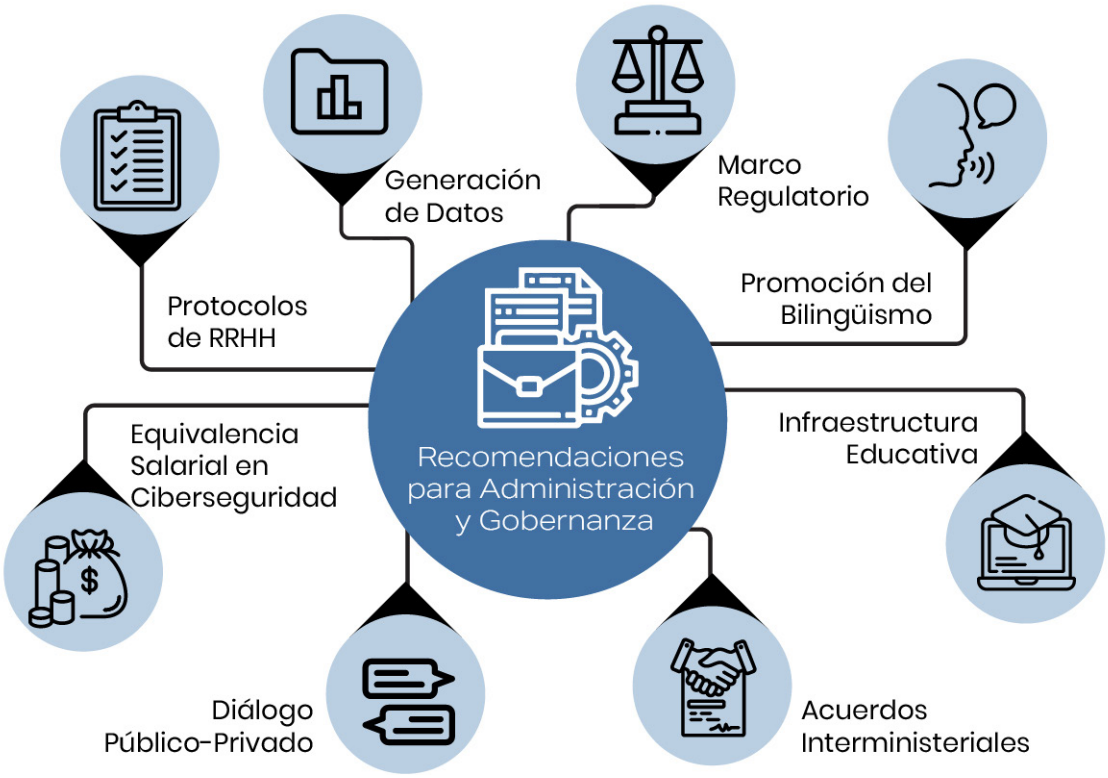


Figura 4: principales recomendaciones para el área estratégica de Administración y Gobernanza Fuente: OEA/CICTE

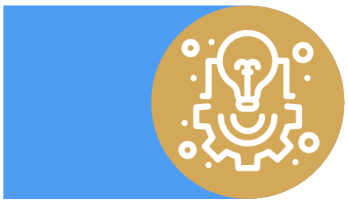
1. Generar un marco regulatorio que legitime las decisiones dentro de la Estrategia Nacional de ciberseguridad

Para garantizar la implementación y sostenibilidad del Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad, es esencial que las decisiones tomadas en su desarrollo tengan un respaldo jurídico sólido. La efectividad del marco nacional de capacitación en ciberseguridad aumentaría si estuviera alineado y respaldado en un marco legislativo que apoye la estrategia nacional de ciberseguridad. Es fundamental contar con esta estructura para garantizar que las recomendaciones sean aplicables y puedan implementarse de manera efectiva, incentivando así la participación del sector privado, la academia y los organismos internacionales. Este marco legislativo permitiría definir claramente los roles y responsabilidades de las instituciones involucradas, facilitando la ejecución de políticas y programas de ciberseguridad en todo el país.

2. Desarrollar fondos para infraestructura educativa

Uno de los principales desafíos que enfrenta la educación en ciberseguridad en Costa Rica es la disparidad en infraestructura educativa entre diferentes regiones. El acceso a tecnologías y laboratorios adecuados es fundamental para formar profesionales en ciberseguridad, y para lograrlo, se recomienda la creación de fondos específicos que permitan:

2.1 Instalar infraestructura tecnológica de vanguardia en centros educativos de todos los niveles.



Establecer centros educativos especializados en ciberseguridad en zonas fuera del Gran Área Metropolitana (GAM), para descentralizar la oferta educativa y garantizar que todas las regiones del país puedan acceder a la formación en este sector estratégico.

2.2 Diseñar estrategias que promuevan la educación dual en áreas rurales

El MEP en Costa Rica promueve la educación dual, en la que los estudiantes reciben formación teórica complementada con práctica en escuelas. Sin embargo, una de las brechas geográficas que impacta a las áreas fuera del GAM es la falta de oportunidades para desarrollar esta formación práctica. Por lo tanto, se recomienda implementar esfuerzos que permitan que estas prácticas sean sincrónicas o se realicen de manera que sean accesibles para esta población, proporcionando la asistencia necesaria para el traslado y otras necesidades específicas.

2.3 Elevar los salarios docentes universitarios en ciberseguridad

Aumentar los salarios de los docentes universitarios en ciberseguridad es recomendable para atraer a expertos del sector privado y motivar a profesionales calificados a dedicarse a la enseñanza. Esto es especialmente crucial en áreas de alta especialización como la ciberseguridad, donde la competencia por el talento con el sector privado es considerable.

3. Promover el diálogo entre organismos públicos y sector privado nacional con el objetivo de establecer estándares en formación en materia de ciberseguridad

La creación de estándares que brinden información actualizada sobre las necesidades del sector privado en materia de ciberseguridad resulta indispensable para generar programas de formación que tengan como objetivo cumplir con esos requerimientos. La falta de estos estándares podría generar brechas que dificulten capturar plenamente las necesidades y los estándares requeridos en los planes educativos, afectando la adecuación entre la formación y las demandas laborales.

Uno de los principales desafíos en la formación en ciberseguridad es la rapidez con la que evolucionan las tecnologías y las amenazas cibernéticas. Para mantener la relevancia de los programas educativos y garantizar que los profesionales reciban la capacitación adecuada, se recomienda que los organismos públicos y el sector privado trabajen de manera conjunta en la definición de los contenidos curriculares y los estándares de calidad. Esto incluiría la identificación de habilidades técnicas especializadas que respondan a las necesidades actuales del mercado laboral, así como la creación de sistemas de certificación reconocidos tanto a nivel nacional como internacional.

Las empresas privadas, que suelen estar a la vanguardia de la innovación tecnológica, pueden aportar experiencia y buenas prácticas que enriquezcan los programas formativos del país. Al mismo tiempo, los organismos públicos pueden garantizar que los estándares de formación se alineen con las políticas nacionales de ciberseguridad, promoviendo una fuerza laboral capacitada para proteger tanto los intereses del Estado como los del sector privado.

4. Importancia de generar acuerdos interministeriales y con organismos

La cooperación entre diferentes ministerios y organismos es crucial para el éxito de cualquier política educativa, especialmente en un área tan transversal como la ciberseguridad. Se recomienda que los ministerios consideren mecanismos de cooperación, tales como acuerdos de coordinación o colaboración, entre entidades como el Ministerio de Educación Pública (MEP), Ministerio de Relaciones Exteriores y Culto (MREC), Ministerio de Planificación Nacional y Política Económica (MIDEPLAN), el Ministerio de Economía, Industria y Comercio (MEIC), el MICITT y otras instituciones relevantes. Estos acuerdos permitirían crear sinergias, optimizar el uso de recursos y evitar duplicidad de esfuerzos, asegurando una integración efectiva de las iniciativas de ciberseguridad en los programas educativos y de formación.

5. Potenciar el bilingüismo en la educación pública

En el campo de la ciberseguridad, el dominio del inglés es una habilidad esencial, ya que gran parte de la literatura técnica, la documentación y los recursos educativos están disponibles en este idioma. Potenciar el bilingüismo en las escuelas públicas no solo facilita el acceso de los estudiantes costarricenses a estos recursos, sino que también mejoraría su competitividad en un mercado laboral global. A largo plazo, el fortalecimiento de la enseñanza del inglés en la educación pública contribuiría al desarrollo de una fuerza laboral altamente capacitada, capaz de integrarse en un ecosistema global de ciberseguridad.

Actualmente, hay una brecha en el bilingüismo entre la educación privada y pública. Para fomentar la igualdad de oportunidades y ampliar la cantidad de ciudadanos capacitados en ciberseguridad, se recomienda mejorar el nivel de enseñanza del idioma inglés en todas las escuelas del país. Además, sería beneficioso implementar programas extracurriculares de actualización para quienes ya han finalizado sus estudios secundarios. Para facilitar el acceso, especialmente para las personas que residen en zonas rurales, sería ideal que estos programas se ofrezcan de manera remota.

6. Equiparar los salarios en ciberseguridad entre el sector público y privado

Uno de los principales retos para la administración pública es la retención de talento en ciberseguridad. El desajuste salarial entre el sector público y privado provoca que muchos profesionales cualificados migren al sector privado, donde los salarios son significativamente más altos. Para evitar la fuga de talentos del Estado, se recomienda equiparar los salarios en ciberseguridad entre ambos sectores, ofreciendo incentivos y beneficios adicionales que hagan atractiva la carrera pública. Al asegurar que los profesionales de ciberseguridad en el sector público reciban remuneración competitiva, el gobierno puede garantizar una fuerza laboral capacitada que continúe protegiendo la infraestructura crítica del país.

7. Diseñar protocolos actualizados de Recursos Humanos dentro del Estado para los puestos vinculados a ciberseguridad

Es importante destacar que es una buena práctica contar con estándares técnicos actualizados para informar de manera más efectiva la contratación de personal y la elaboración de descripciones de puestos. La falta de información técnica relacionada con los puestos laborales en ciberseguridad puede dar lugar a estimaciones imprecisas en las búsquedas internas y a una desalineación entre los cargos y la formación de los solicitantes.

Por ello, se recomienda fomentar un diálogo entre los sectores de Recursos Humanos del Estado, las empresas del ámbito de la ciberseguridad y las áreas que requieren estos puestos, con el fin de crear perfiles técnicos precisos que optimicen las búsquedas y las aplicaciones.

8. Generar diagnósticos, datos y relevamientos

Un componente esencial para cualquier marco de formación es contar con información precisa sobre el estado actual de la ciberseguridad en el país y las necesidades específicas del mercado laboral. La generación de diagnósticos y relevamientos periódicos permitiría conocer las brechas de competencias, identificar las áreas prioritarias de intervención y diseñar programas formativos que respondan a las demandas reales de la industria. Contar con datos actualizados es clave para evitar la improvisación y asegurar que las políticas educativas y de formación en ciberseguridad estén alineadas con las necesidades del país.

9. Apoyar a las familias más vulnerables en materia de conectividad

Las diversas brechas digitales existentes en Costa Rica requieren de diversas estrategias. Las familias más vulnerables se encuentran excluidas digitalmente, tanto por la dificultad para comprar dispositivos como por la falta de acceso a fibra óptica o conectividad.

Para mejorar la inserción presente y futura de dichas poblaciones en materia de ciberseguridad, ampliando la oferta y generando asimismo una posibilidad de ascenso social, es indispensable comenzar por mejorar las estructuras y posibilidad de conexión.

Asimismo y en forma complementaria, se requiere del diseño de programas educativos para las familias de los sectores vulnerados que les posibiliten comprender los usos básicos de los entornos digitales y así acompañar a sus hijos en su desarrollo profesional.

10. Generar un diálogo entre Servicio Civil, INA y el cybersec cluster

El desfase actual entre la malla curricular del INA, los requisitos para los puestos del Estado proporcionados por el Servicio Civil y las demandas del sector privado, según lo señalado por el cybersec cluster, indica una oportunidad para mejorar la coordinación entre estos actores. Sería beneficioso considerar la creación de una mesa de diálogo que reúna a los tres sectores, con el fin de unificar criterios en la malla curricular y en los perfiles requeridos tanto en el ámbito público como en el privado. Esta colaboración podría fomentar una retroalimentación constructiva y optimizar los esfuerzos de todos los involucrados.

11. Reducción de brecha de género digital

Establecer lineamientos y políticas públicas que incentiven la participación activa de mujeres en el ámbito de la ciberseguridad, como por ejemplo, cuotas de género en programas nacionales y comités estratégicos. Crear alianzas público-privadas para desarrollar iniciativas específicas como bolsas de empleo inclusivas, programas de liderazgo femenino y seguimiento de indicadores que evalúen el progreso en la incorporación de mujeres en roles técnicos y de toma de decisiones en ciberseguridad.

CONCIENTIZACIÓN Y CULTURA

Dentro de la Concientización y cultura, y teniendo en cuenta el objetivo de formar una fuerza laboral en materia de ciberseguridad, se identifican en Costa Rica los siguientes actores principales. Cabe señalar que, aunque estos actores fueron destacados durante las consultas, no son los únicos involucrados en este proceso.

- **Ministerio de Cultura y Juventud**
- **Ministerio de Educación Pública**
- **INA (Instituto Nacional de Aprendizaje)**
- **MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones)**
- **Organización de la sociedad civil**
- **Empresas que realicen acciones de Responsabilidad Social Empresaria**
- **Medios de comunicación**
- **Universidades y centros de investigación**
- **Cámaras y asociaciones empresariales**
- **Familias**

Figura 5: principales recomendaciones para el área estratégica de Concientización y Cultura Fuente: OEA/CICTE

La formación de una fuerza laboral en ciberseguridad en Costa Rica no solo depende de la creación de programas educativos técnicos, sino también de la construcción de una cultura que valore y priorice la ciberseguridad desde diferentes ámbitos de la sociedad. Este enfoque cultural y de concientización es clave para fomentar vocaciones, disminuir brechas de acceso y hacer que la ciberseguridad sea comprendida como una responsabilidad compartida por todos los sectores. A continuación, se desarrollan los principales desafíos que Costa Rica enfrenta en esta área:

1. Transformar el interés en ciberseguridad en una formación planificada

El creciente interés en la ciberseguridad ha generado un "boom" en la búsqueda de programas y trabajos en este campo. No obstante, uno de los principales desafíos es que este interés muchas veces no está acompañado de una planificación adecuada. Sin una estrategia clara, las personas que desean ingresar al sector pueden no estar desarrollando las habilidades específicas que son realmente necesarias en el mercado laboral.

Es crucial canalizar este interés a través de una planificación estratégica que identifique las competencias clave que deben adquirirse para enfrentar las amenazas actuales y futuras. Para ello, se recomienda que el gobierno y el sector privado trabajen juntos en la creación de programas formativos que no solo fomenten el interés por la ciberseguridad, sino que también aseguren que los individuos reciban capacitación en áreas críticas como la seguridad en redes, la gestión de riesgos cibernéticos y la resiliencia frente a ataques. Asimismo, también es fundamental educar a la población sobre la amplitud del campo de la ciberseguridad, resaltando la diversidad de roles especializados que existen, más allá del simple manejo de tecnologías.

2. Generar programas que disminuyan las brechas generacionales, sociales, de acceso, de género y de conectividad

El acceso a la educación en ciberseguridad no es uniforme. En Costa Rica, persisten ciertas brechas estructurales que limitan la participación de ciertos grupos en este campo. Las brechas generacionales excluyen a los adultos mayores, las brechas sociales y de acceso marginan a comunidades rurales, y la brecha de género perpetúa la subrepresentación de las mujeres en carreras tecnológicas. Además, la falta de conectividad en ciertas regiones impide que los estudiantes puedan acceder a recursos y oportunidades formativas en ciberseguridad.

Para mitigar estas desigualdades, se recomienda desarrollar programas inclusivos que reduzcan estas brechas, enfocándose en promover la equidad, tanto en términos de acceso a la tecnología como en la oferta de oportunidades para comunidades vulnerables. Asimismo, es recomendable fomentar la participación de mujeres en la ciberseguridad mediante campañas que desafíen los estereotipos y ofrezcan modelos de rol femeninos. La implementación de programas de capacitación en línea accesibles a todas las regiones del país, con subsidios o equipos tecnológicos para quienes lo necesiten, también puede ser una medida efectiva para cerrar estas brechas.

3. Fomentar el interés de la población en trabajos futuros en ciberseguridad

A pesar del crecimiento del sector, un obstáculo a superar es motivar a la población para que se forme en ciberseguridad. Un aspecto atractivo es que los salarios en este campo son considerablemente más altos que el promedio en Costa Rica, lo que podría servir como incentivo para muchos. Sin embargo, resaltar los beneficios económicos por sí solo no es suficiente; también es importante promover el valor social de la ciberseguridad.

También se sugiere fomentar un mayor acercamiento a la formación en ciberseguridad, de manera que las poblaciones menos familiarizadas con el tema se sientan más confiadas para iniciar su formación. Implementar lemas o campañas que conecten la ciberseguridad con diferentes comunidades, junto con programas escalonados, adaptados y accesibles, sería un primer paso valioso en esta dirección.

Se recomienda diseñar campañas con enfoque específico en poblaciones vulnerables como mujeres, personas adultas mayores y jóvenes de áreas rurales para garantizar que los esfuerzos de concientización sean más inclusivos y efectivos.

4. Incorporar la ciberseguridad en la vida pública, social y cultural desde la primera infancia

Se recomienda cultivar el interés en ciberseguridad desde la infancia. Introducir el tema de la ciberseguridad de manera lúdica y educativa a los niños y jóvenes puede ser una estrategia poderosa para crear una conciencia colectiva desde edades tempranas. Los niños que crecen familiarizados con los principios de la ciberseguridad estarán mejor preparados para enfrentarse a los desafíos digitales del futuro.

Este desafío implica desarrollar campañas de sensibilización dirigidas a la población general, usando enfoques lúdicos y educativos que hagan que el tema sea accesible y atractivo. Propuestas como juegos, plataformas interactivas, y actividades educativas vinculadas

al entretenimiento pueden ayudar a que las personas, desde la infancia hasta la adultez, se familiaricen con conceptos clave de ciberseguridad. Asimismo, se recomienda que se implementen programas que integren la ciberseguridad en el currículo escolar, desde los niveles más básicos hasta la educación secundaria. Esto es esencial para fomentar una cultura de seguridad digital a largo plazo.

5. Implementar programas de formación en ciberseguridad para diferentes roles jerárquicos.

Se recomienda implementar programas de formación en ciberseguridad diseñados específicamente para atender las necesidades de diversos niveles jerárquicos dentro de las organizaciones. Estos programas deben ser personalizados, ajustando los contenidos según los roles y responsabilidades de cada grupo, desde altos ejecutivos hasta personal técnico y operativo. Esto permitirá que cada participante desarrolle competencias pertinentes para identificar, mitigar y responder a amenazas digitales de manera efectiva, alineando las capacidades individuales con los objetivos estratégicos de ciberseguridad.

6. Fomentar la inclusión sin estereotipos de género

Se recomienda desarrollar campañas de sensibilización que combatan los estereotipos de género en el campo de la ciberseguridad, visibilizando a mujeres referentes en el ámbito tecnológico. Es importante que estas campañas lleguen a escuelas, empresas y la sociedad en general para fomentar un cambio cultural y estimular el interés temprano de las niñas en áreas STEM.

CURRÍCULO Y PROGRAMA ESCOLAR

En el currículo y programa escolar, y considerando el objetivo de formar una fuerza laboral en ciberseguridad, el principal actor es el Ministerio de Educación Pública (MEP), en colaboración con otros organismos del sector privado, de la sociedad civil y del sector público, así como el cybersec cluster. Esta colaboración es esencial para actualizar los programas escolares. Además, es importante reconocer al INA como un actor clave en este proceso. Cabe señalar que, aunque estos actores fueron destacados durante las consultas, no son los únicos involucrados en este proceso.

Se recomienda que la educación en ciberseguridad sea un proceso integral que inicie desde las primeras etapas escolares. Esto implica no solo la inclusión de conocimientos técnicos, sino también el desarrollo de habilidades diversas y la mejora de áreas clave que preparen a los estudiantes para el futuro.

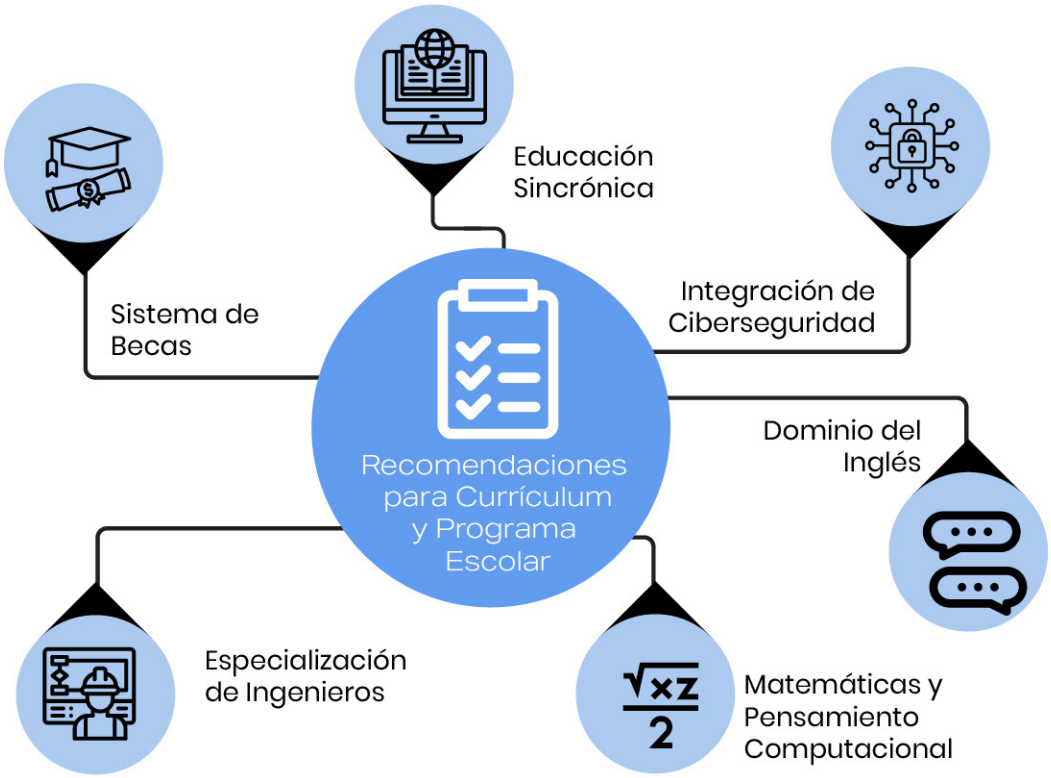


Figura 6: principales recomendaciones para el área estratégica de Currículum y programa escolar Fuente: OEA/CICTE

1. Incluir la ciberseguridad dentro de la herramienta STEAM

La inclusión de la temática de ciberseguridad debe alinearse con un enfoque STEAM (Ciencia, Tecnología, Ingeniería, Artes y Matemáticas) desde los niveles iniciales. Esto implica no tratar la ciberseguridad como un tema aislado, sino como parte de una estrategia educativa más amplia que fomente habilidades digitales, pensamiento crítico, y la integración de habilidades blandas y duras.

Se recomienda especialmente priorizar la educación técnica como un sector educativo estratégico para implementar la herramienta STEAM y fortalecer así la ciberseguridad.

El desafío está en diseñar un currículo que motive a los estudiantes desde edades tempranas a desarrollar competencias digitales, impulsando el interés por la tecnología y la ciencia de datos. A través de actividades prácticas y colaborativas, el enfoque STEAM puede generar en los niños una comprensión integral no solo de la ciberseguridad, sino también de la importancia de la creatividad y la resolución de problemas. Además, este enfoque puede preparar a los estudiantes para navegar con seguridad en un mundo digitalizado y para considerar la ciberseguridad como una futura carrera.

2. Mejorar el nivel de enseñanza del inglés en la educación pública

El bilingüismo es una necesidad crítica para la inserción laboral en ciberseguridad, ya que gran parte del conocimiento técnico en este campo está en inglés. El desafío es lograr una mejora sustancial en el nivel de inglés de los estudiantes de la educación pública, equipándolo con los estándares que demandan las industrias tecnológicas internacionales.

La barrera idiomática limita el acceso de muchos estudiantes a recursos educativos avanzados, certificaciones internacionales, y oportunidades laborales en el extranjero. Por lo tanto, se recomienda que el sistema educativo público implemente programas de inmersión en inglés desde edades tempranas, asegurando que los estudiantes adquieran un dominio adecuado del idioma. Esto les permitirá desenvolverse eficazmente en el mundo profesional de la ciberseguridad, donde la mayor parte de la literatura, software y foros técnicos están en inglés.

3. Mejorar las competencias en matemáticas y pensamiento computacional desde el nivel inicial

Para que los estudiantes puedan enfrentar de manera efectiva una formación en ciberseguridad, es esencial que lleguen con bases sólidas en matemáticas y pensamiento computacional. Sin estos fundamentos, las materias relacionadas con la ciberseguridad, como la criptografía, el análisis de riesgos, y la programación, pueden resultar extremadamente desafiantes.

En este contexto, la gamificación se presenta como una estrategia didáctica efectiva para fomentar competencias en ciberseguridad, además de servir como plataforma para incubar talento y desarrollar habilidades.

El desafío es crear un currículo que fortalezca las competencias matemáticas desde las primeras etapas de la educación. Esto incluye no solo el aprendizaje de operaciones básicas, sino también el fomento del pensamiento lógico y abstracto, habilidades necesarias para el desarrollo de competencias en programación y seguridad digital. Además, se recomienda implementar programas que acerquen el pensamiento computacional a los estudiantes a través de actividades lúdicas y prácticas, como el uso de la robótica y la programación básica, que motiven a los estudiantes a entender el impacto de estas disciplinas en el mundo real.

4. Motivar a los ingenieros a especializarse en ciberseguridad

Costa Rica cuenta con una estructura sólida de ingenieros en diversas ramas tecnológicas, pero hay un desafío en motivar a estos profesionales a hacer la transición al sector de ciberseguridad. Esta área ofrece una oportunidad de movilidad social gracias a los altos sueldos que se ofrecen en el sector, tanto a nivel local como internacional.

El reto radica en generar incentivos atractivos que impulsen a los ingenieros actuales y futuros a considerar la especialización en ciberseguridad. Estos incentivos pueden incluir programas de actualización profesional, becas para estudios avanzados en ciberseguridad, y la promoción de esta carrera como prestigiosa y bien remunerada.

En cuanto a los profesionales en ingeniería con trayectoria por fuera de la ciberseguridad, se recomienda hacer especial énfasis en programas de upskilling que promuevan la actualización con vistas a la inserción laboral en materia de ciberseguridad.

Además, es fundamental revisar y actualizar las descripciones de puestos en Recursos Humanos para garantizar que se busquen las habilidades adecuadas y que los profesionales con experiencia puedan realizar la transición efectivamente, por ejemplo a través de certificaciones adicionales. Las alianzas con el sector privado también pueden facilitar este proceso, generando más oportunidades laborales en este campo emergente.

5. Establecer un sistema de becas y pasantías en materia de ciberseguridad

Con el objetivo de disminuir las diversas brechas y ampliar la oferta de fuerza laboral, se recomienda generar programas de becas y pasantías para que estudiantes que se encuentran culminando su ciclo escolar, puedan insertarse en forma inmediata en programas de formación terciaria vinculados a ciberseguridad o programas de empleo en empresas de ciberseguridad.

Se recomienda establecer un programa de becas que facilite el acceso de estudiantes a centros de formación, con el apoyo del Estado. En este contexto, es fundamental que las becas incluyan refuerzo en el idioma inglés, así como recursos para materiales y traslados.

6. Generar instancias de educación sincrónica en ciberseguridad para zonas fuera del GAM

Uno de los desafíos fundamentales en la formación de la fuerza laboral en ciberseguridad en Costa Rica es garantizar el acceso equitativo a la educación especializada, particularmente en las escuelas situadas fuera de la Gran Área Metropolitana (GAM). Muchas de estas escuelas enfrentan dificultades para acceder a docentes capacitados en temas específicos de tecnología y ciberseguridad debido a su ubicación geográfica y la falta de recursos especializados.

La educación sincrónica emerge como una solución efectiva para superar este obstáculo, permitiendo que los estudiantes de zonas rurales o fuera de San José accedan a clases en tiempo real, impartidas por especialistas en ciberseguridad que pueden encontrarse en cualquier parte del país o incluso en el extranjero. Esta metodología, basada en plataformas digitales de videoconferencias y recursos en línea, tiene múltiples beneficios.

La implementación de clases sincrónicas no solo expone a los estudiantes a conocimientos especializados, sino que también fomenta el aprendizaje autónomo y la mejora de las competencias digitales. Los estudiantes deben familiarizarse con el uso de plataformas tecnológicas y gestionar su aprendizaje en un entorno virtual, lo cual es una habilidad clave en el campo de la ciberseguridad.

La implementación de programas de educación sincrónica en ciberseguridad también abre la puerta a la colaboración entre el sector público y el sector privado. Empresas tecnológicas y universidades pueden aportar su experiencia y recursos para desarrollar contenidos de alta calidad, brindar capacitaciones a los docentes y compartir buenas prácticas de enseñanza en plataformas digitales.

Estas alianzas pueden contribuir a asegurar que los contenidos sean actualizados, relevantes y alineados con las demandas del mercado laboral, y al mismo tiempo permitir que se difundan a través de redes educativas nacionales.

7. Alineación con estándares internacionales

Se recomienda seguir estándares internacionales como el marco NICE (National Initiative for Cybersecurity Education) en la formación de nivel secundario para garantizar que los estudiantes adquieran competencias relevantes y alineadas con las demandas globales en ciberseguridad. Este enfoque permitiría estructurar currículos que aborden habilidades técnicas, pensamiento crítico y ética profesional desde etapas tempranas, preparando a los jóvenes para integrarse a un mercado laboral altamente competitivo y en constante evolución. Además, adoptar estándares como el marco NICE fomenta la cohesión entre sistemas educativos nacionales e internacionales, facilitando la movilidad estudiantil y profesional, y fortaleciendo la capacidad de respuesta de los países ante las crecientes amenazas cibernéticas.

8. Reducción de brecha de género digital

Se sugiere diseñar contenidos curriculares que incluyan ejemplos de mujeres destacadas en tecnología y ciberseguridad, con el objetivo de derribar estereotipos de género que limitan la percepción de niñas y jóvenes sobre su capacidad para sobresalir en estas áreas. Asimismo, se recomienda implementar programas de mentoría que permitan a estudiantes de primaria y secundaria interactuar con mujeres profesionales de la ciberseguridad. Por otro lado, se puede lograr un impacto significativo al colaborar con organizaciones no gubernamentales, empresas tecnológicas y universidades para desarrollar recursos educativos, talleres y eventos diseñados con un enfoque inclusivo, que ofrezcan a las niñas oportunidades prácticas de aprendizaje.

EDUCACIÓN TERCIARIA E INVESTIGACIÓN

Dentro de Educación terciaria e investigación y teniendo en cuenta el objetivo de formar fuerza laboral en materia de ciberseguridad, se observan que los principales actores son las universidades públicas y privadas en alianza con sectores vinculados a la ciberseguridad como el cybersec cluster. Cabe señalar que, aunque estos actores fueron destacados durante las consultas, no son los únicos involucrados en este proceso.

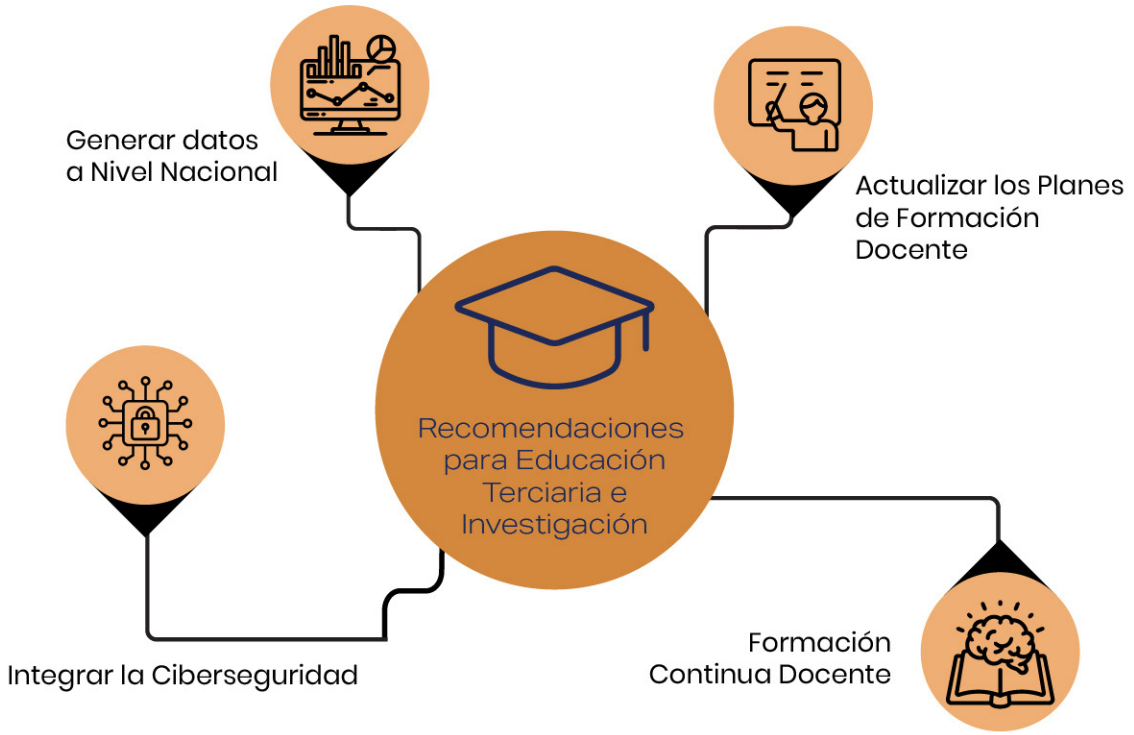


Figura 7: principales recomendaciones para el área estratégica de Educación Terciaria e Investigación. Fuente: OEA/CICTE

1. Actualización de los planes de formación docente en todos los niveles educativos

Uno de los principales desafíos en esta área es la actualización de los planes de formación docente para que la ciberseguridad sea parte integral de la educación desde los primeros niveles hasta la enseñanza universitaria. La ciberseguridad no debe considerarse como un tema especializado reservado para carreras técnicas, sino que debe ser vista como una competencia fundamental para todos los docentes, independientemente del nivel o la materia que enseñan.

Esto implica que las universidades y centros de formación docente incluyan contenidos específicos de ciberseguridad en sus planes de estudio, tanto en programas de pregrado como en aquellos de formación continua. Por lo tanto se recomienda que los futuros docentes reciban una formación integral que les permita comprender los riesgos y desafíos del entorno digital, para así poder transmitir este conocimiento a sus estudiantes desde las primeras etapas educativas.

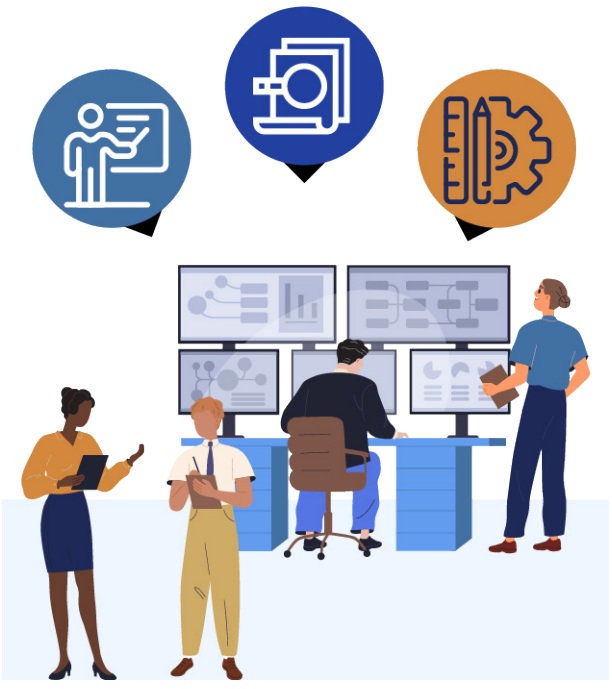
2. Actualizaciones continuas durante la carrera docente

En un campo tan dinámico como la ciberseguridad, se recomienda que los docentes, una vez insertos en el sistema educativo, tengan acceso a actualizaciones regulares que les permitan mantenerse al día con las últimas tendencias, herramientas y enfoques en la materia. Este es un desafío clave, ya que la formación continua garantizará que los educadores puedan abordar los nuevos riesgos y oportunidades que surgen en el panorama de ciberseguridad.

Por lo tanto se recomienda promover programas de capacitación y actualización profesional en ciberseguridad en universidades y otras instituciones educativas, en colaboración con el gobierno y el sector privado. Estas capacitaciones no solo mejorarían las habilidades de los docentes, sino que también permitirían una mayor innovación en las estrategias pedagógicas, incorporando enfoques tecnológicos y cibernéticos en el aula.

3. Incorporación de la ciberseguridad como tema transversal en diversas carreras terciarias

Si bien la ciberseguridad es una disciplina técnica, su impacto es amplio y afecta a todas las áreas del conocimiento. Por ello, es importante que las universidades incluyan la ciberseguridad como tema transversal en diversas carreras terciarias, no solo en carreras tecnológicas o ingenierías, sino también en docencia, investigación, ciencias sociales, entre otras.



Esto permitirá que futuros profesionales de distintas disciplinas comprendan los desafíos de la ciberseguridad desde sus respectivos campos, fomentando así una cultura de seguridad digital en diferentes áreas de la sociedad. Por ejemplo, los profesionales en ciencias sociales pueden estudiar el impacto de la ciberseguridad en la sociedad, la privacidad y las políticas públicas, mientras que los educadores pueden integrar la ciberseguridad en sus planes de enseñanza de manera más efectiva.

4. Generación de datos, estadísticas e investigación sobre ciberseguridad en el contexto nacional

Para diseñar e implementar un marco efectivo de formación en ciberseguridad, es crucial contar con una base sólida de datos, estadísticas e investigación que permita comprender el estado actual del sector en Costa Rica. La falta de información detallada sobre el estado de situación, las habilidades desarrolladas, las brechas en la formación, las necesidades laborales y el conocimiento social sobre el tema dificulta la creación de estrategias que se ajusten a las verdaderas necesidades del país.

Es indispensable promover la investigación académica en ciberseguridad para generar un diagnóstico preciso que sirva de base para el desarrollo de políticas educativas y laborales. Se recomienda que las universidades y centros de investigación trabajen en conjunto con el gobierno y el sector privado para recopilar y analizar datos que incluyan:

- **Habilidades actuales y faltantes en la fuerza laboral en ciberseguridad.**
- **Cupos laborales requeridos por el mercado.**
- **Interés y conocimientos de la sociedad en general sobre la ciberseguridad.**
- **Estadísticas de incidentes y vulnerabilidades cibernéticas que afecten al país.**

Además, es importante que estas investigaciones identifiquen amenazas emergentes y tendencias en ciberseguridad, lo que permitirá informar mejor sobre las necesidades educativas y mantener los programas actualizados con respecto a los desafíos actuales. Esta información es clave para ajustar los programas educativos y asegurarse de que la formación de la fuerza laboral se alinee con las necesidades del país y las tendencias globales.

5. Programa de pasantías y prácticas profesionalizantes

Se recomienda que los docentes en educación terciaria participen en pasantías y prácticas profesionalizantes en el ámbito de la ciberseguridad para enriquecer su experiencia práctica y alinear su enseñanza con las demandas actuales del sector. Estas experiencias permiten a los docentes familiarizarse con los desafíos, herramientas y dinámicas reales que enfrentan las organizaciones en el campo de la ciberseguridad, fortaleciendo su capacidad para diseñar planes de estudio actualizados y relevantes. Al involucrarse directamente en entornos laborales especializados, los educadores pueden trasladar ese conocimiento aplicado al aula, fomentando una formación más práctica y conectada con las necesidades del mercado laboral en ciberseguridad.

6.Colaboración entre sector privado y público para el fomento de I+D

La colaboración entre el sector privado y la academia en Costa Rica es fundamental para fortalecer la formación práctica de los futuros profesionales y para responder a las necesidades del mercado laboral. Este enfoque es especialmente relevante en modelos educativos como el de la Universidad Invenio, que opera bajo un sistema dual combinando teoría y práctica. A través de alianzas estratégicas, los estudiantes tienen la oportunidad de participar en proyectos reales, como consultorías y pasantías, donde aplican sus conocimientos en un entorno empresarial y contribuyen a resolver problemas concretos. Estas sinergias no solo enriquecen la experiencia educativa, sino que también impulsan la innovación, el desarrollo económico y la capacidad del país para competir en un entorno globalizado.

Por otro lado, CEDES Don Bosco en Costa Rica es un excelente ejemplo de cómo el sistema educativo privado, enfocado en la formación técnica, ha logrado integrar de manera efectiva la educación práctica con el acceso a laboratorios de alta tecnología proporcionados por empresas del sector. Esta colaboración permite a los estudiantes adquirir habilidades prácticas en entornos equipados con tecnología de punta, lo cual los prepara para las demandas actuales del mercado laboral y fortalece el vínculo entre la educación y el desarrollo industrial.

7. Alineación con estándares internacionales

Seguir estándares internacionales como el marco NICE (National Initiative for Cybersecurity Education) en la formación terciaria es esencial para desarrollar programas académicos que respondan a las necesidades globales en ciberseguridad. Estos estándares proporcionan una guía estructurada para diseñar currículos que integren competencias técnicas avanzadas, habilidades analíticas y una sólida base ética, formando profesionales altamente capacitados para enfrentar los desafíos del entorno digital. Además, al alinear los programas terciarios con estándares como NICE, se promueve la armonización internacional de las credenciales educativas, facilitando la empleabilidad global y fortaleciendo la capacidad de los países para abordar amenazas cibernéticas de manera estratégica y colaborativa.

8. Reducción de brecha de género digital

Se sugiere crear becas y programas específicos para mujeres en carreras relacionadas con ciberseguridad, así como fomentar proyectos de investigación liderados por mujeres en este campo. También sería beneficioso desarrollar alianzas con universidades para establecer redes de apoyo entre estudiantes y mujeres profesionales. Además, se recomienda ofrecer formación específica para docentes en perspectiva de género y su aplicación en el aula, ayudándoles a identificar y combatir sesgos inconscientes que puedan desmotivar a las niñas y/o jóvenes a involucrarse en áreas STEM (Ciencia, Tecnología, Ingeniería y Matemáticas).

ENTRENAMIENTO Y CERTIFICACIÓN

Dentro de entrenamiento y certificación y teniendo en cuenta el objetivo de formar fuerza laboral en materia de ciberseguridad, se observa que los principales actores son los detallados a continuación. Cabe señalar que, aunque estos actores fueron destacados durante las consultas, no son los únicos involucrados en este proceso.

- **Las universidades e institutos terciarios**
- **Marco Nacional de Cualificaciones**
- **El cybersec cluster**
- **Otras empresas del sector no incluídas en el cybersec cluster**

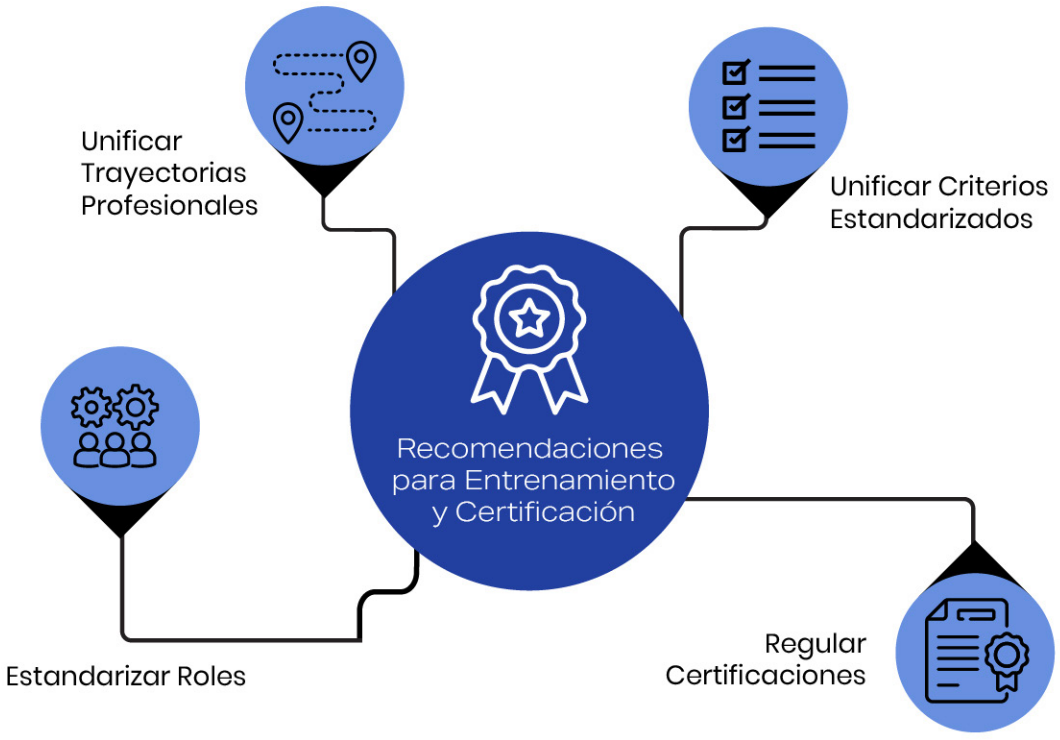


Figura 8: principales recomendaciones para el área estratégica de Entrenamiento y Certificación.. Fuente: OEA/CICTE

1. Unificación de criterios mínimos estandarizados para la certificación nacional en ciberseguridad

Un desafío clave es lograr la unificación de criterios que permitan que las certificaciones nacionales en ciberseguridad cumplan con estándares mínimos de calidad y relevancia. Actualmente, existe una proliferación de programas y certificaciones sin una homologación clara, lo que puede llevar a una formación inconsistente.

El Marco Nacional de Cualificaciones de Costa Rica estableció en el año 2020 un estándar en materia de ciberseguridad que en la actualidad algunas instituciones tanto del INA como de algunos centros terciarios están utilizando.

Se sugiere fomentar una mayor colaboración por parte del cybersec cluster para proporcionar estándares actualizados que alineen el marco con los requisitos del mercado.

Además, se recomienda la creación de regulaciones que establezcan criterios oficiales para la entrega de certificados en ciberseguridad, limitando esta posibilidad únicamente a las instituciones que cumplan con los estándares propuestos por el marco.

2. Regularización y control de propuestas de entrenamiento

Existe una gran diversidad de propuestas de entrenamiento en ciberseguridad, algunas de las cuales no están debidamente reguladas o supervisadas. Esto genera un desafío en cuanto a la calidad y la relevancia del contenido impartido. Es importante que todas las propuestas de formación y certificación en ciberseguridad sigan criterios unificados que garanticen que se estén formando profesionales con las competencias necesarias para el mercado laboral actual. La existencia del Marco Nacional de Cualificaciones y su estándar en ciberseguridad 2020 podría proponerse como un rector de dicha unificación.

El control y regulación de los programas de entrenamiento permitiría evitar la proliferación de programas que no cumplan con los estándares necesarios y asegurar que todos los entrenamientos contemplen criterios formativos alineados con las necesidades del país y del mercado laboral. Unificar estos criterios no solo mejora la calidad de la formación, sino que también genera confianza en el sistema de certificación por parte de empleadores y profesionales.

3. Estandarización de roles en ciberseguridad

Uno de los principales problemas en el campo de la ciberseguridad es la improvisación de funciones y roles laborales, donde las descripciones de puestos varían significativamente entre empresas o sectores. Esto genera una falta de claridad tanto en el desarrollo de trayectorias profesionales como en la formación requerida para cumplir con esos roles.

La estandarización de los roles existentes en carreras y desempeños laborales de ciberseguridad es clave para evitar esta improvisación. Debe existir una clasificación clara y bien definida de los diferentes roles dentro del campo de la ciberseguridad, con sus respectivas responsabilidades, competencias y límites. Esta estandarización no solo ayudará a las instituciones educativas a diseñar programas más enfocados, sino que también brindará claridad a los empleadores y a los profesionales sobre las expectativas de cada rol.

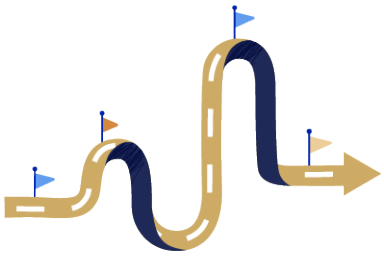
Para alcanzar este objetivo, sería beneficioso contar con el apoyo del cybersec cluster y de otras empresas no incluidas en él, para que proporcionen de manera continua información sobre sus necesidades, los tipos de perfiles y cargos requeridos, así como sus características y requisitos específicos.

4. Unificación de criterios de trayectorias profesionales (career path)

Otro desafío importante en este sector es la falta de previsibilidad en la industria en cuanto a las trayectorias profesionales (career path) en ciberseguridad. Actualmente, no existen rutas claras y estandarizadas que guíen a los profesionales sobre cómo pueden avanzar en su carrera dentro del campo de la ciberseguridad, lo que genera incertidumbre y falta de motivación para quienes buscan ingresar o crecer en el sector.

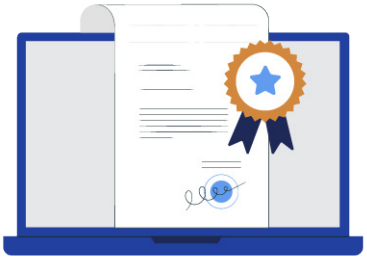
Es fundamental unificar los criterios de trayectorias profesionales y establecer una ruta clara y previsible para los profesionales en ciberseguridad. En el marco del modelo NICE (National Initiative for Cybersecurity Education), una recomendación clave para abordar la falta de criterios unificados en las trayectorias profesionales es desarrollar un marco estandarizado que defina las competencias, habilidades y conocimientos específicos requeridos en cada etapa de las carreras en ciberseguridad. Esto implica:

1 **Establecer Rutas de Carrera Definidas:** Crear trayectorias profesionales bien delineadas, con rutas claras y predecibles que abarquen desde roles de entrada hasta posiciones avanzadas. Esto permite a los profesionales visualizar sus posibilidades de crecimiento y facilita la planificación de su desarrollo.



2 **Definir Perfiles de Competencia:** Alinear los roles de ciberseguridad con un marco de competencias como el NICE Cybersecurity Workforce Framework, identificando habilidades específicas para cada posición, tales como seguridad en la nube, análisis de amenazas o gestión de incidentes. Esto proporciona claridad tanto a los profesionales como a los empleadores sobre las habilidades requeridas en cada rol.

3 **Incorporar Certificaciones y Entrenamiento Estandarizado:** Establecer estándares en cuanto a las certificaciones y programas de capacitación recomendados para cada nivel de trayectoria. Esto facilita el reconocimiento de habilidades a nivel nacional y asegura que los profesionales estén preparados para avanzar en sus carreras.



4 **Fomentar la Movilidad Horizontal y Vertical:** Crear mecanismos que faciliten la transición entre áreas de especialización y niveles jerárquicos, permitiendo una mayor flexibilidad en las carreras de ciberseguridad y promoviendo la adquisición de habilidades diversificadas.

Al implementar estas recomendaciones, el marco NICE ayudaría a Costa Rica a consolidar rutas profesionales coherentes y orientadas al mercado, mejorando la retención de talento en ciberseguridad y asegurando una fuerza laboral capacitada y alineada con los estándares internacionales.

5. Reducción de brecha de género digital

Ofrecer programas de formación continua y certificaciones en ciberseguridad con becas exclusivas para mujeres y horarios flexibles que se ajusten a necesidades diversas. Incorporar capacitaciones sobre equidad de género para todos los participantes y garantizar entornos de aprendizaje inclusivos y libres de discriminación.

6. Programas de formación y certificación para sectores productivos

Se recomienda el diseño e implementación de programas de formación y certificación dirigidos a diferentes organizaciones y sectores productivos, incluyendo las áreas de manufactura y tecnología, con especial énfasis en la protección de infraestructuras críticas y la generación de capital humano competente en el área de ciberseguridad, de manera transversal a lo largo de las cadenas de producción y desarrollo.

CRONOGRAMA DE TRABAJO

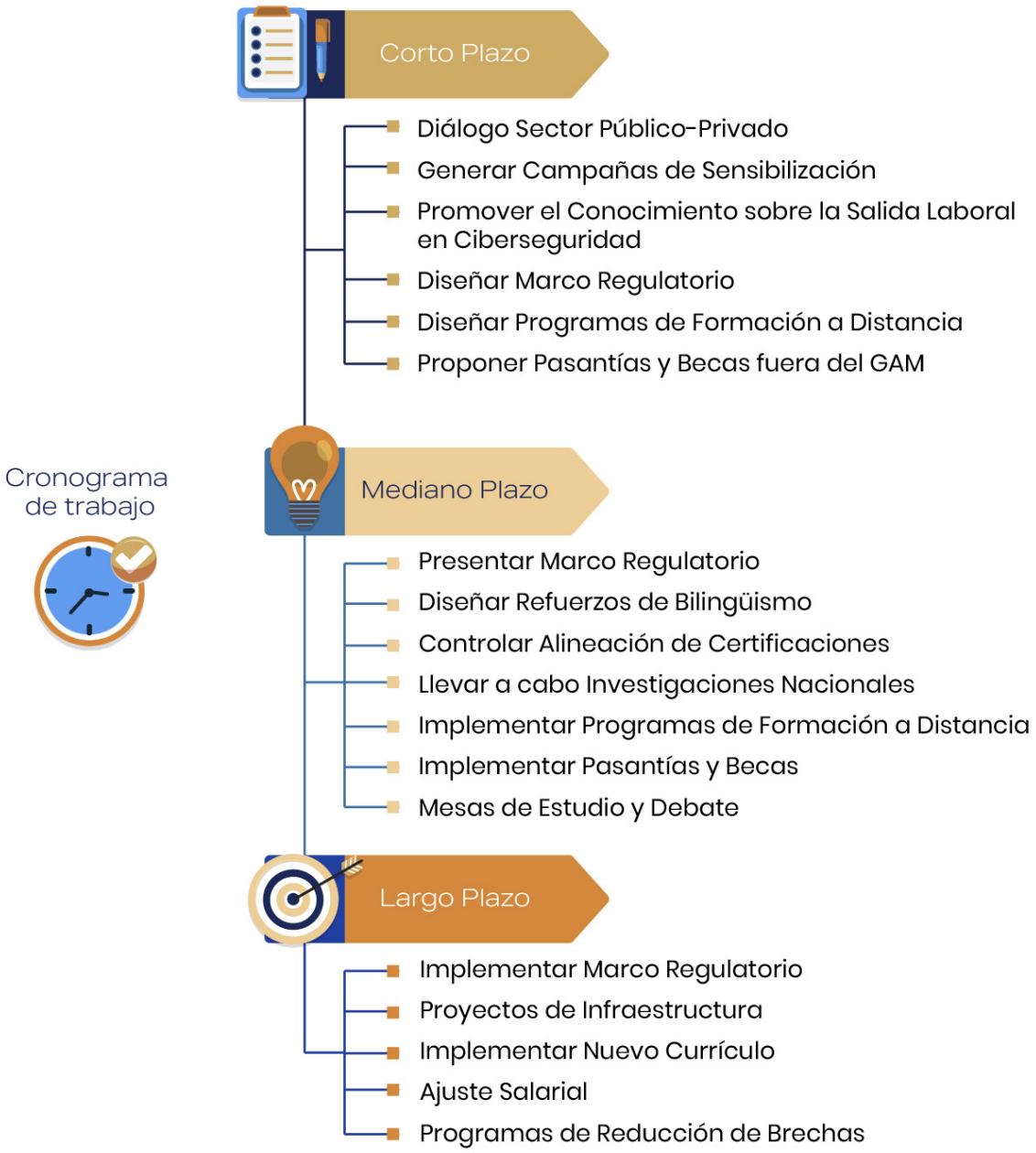


Figura 9: Cronograma de recomendaciones. Fuente: OEA/CICTE

Para facilitar la implementación progresiva de las recomendaciones, la Figura 9 presenta un cronograma detallado que orienta los pasos a seguir en el corto, mediano y largo plazo.

En el **corto plazo**, se recomienda priorizar el diseño de un marco regulatorio que facilite la sistematización de estas iniciativas, incluyendo la asignación de presupuesto para infraestructura, programas de becas, actualización de currículas, formación docente y mecanismos de control para certificaciones.

En segunda instancia, dentro del corto plazo, se sugiere incentivar el diálogo entre el sector público y privado para alinear criterios en relación con los perfiles de trabajo, salarios y necesidades formativas en ciberseguridad. También resulta fundamental iniciar campañas de sensibilización que fomenten la comprensión y el interés de la ciudadanía en torno a la importancia de la ciberseguridad.

Para fortalecer el atractivo de este campo, sería beneficioso implementar acciones informativas que resalten las oportunidades laborales en ciberseguridad y su impacto positivo en el desarrollo profesional.

Con el fin de reducir brechas digitales, especialmente en áreas rurales, es valioso considerar el desarrollo de programas de formación a distancia, así como la promoción de pasantías y becas dirigidas a personas fuera del Gran Área Metropolitana. Estas medidas contribuirían a la equidad en el acceso a oportunidades de capacitación y empleo en ciberseguridad dentro de un Marco Nacional de Formación de Fuerza Laboral en Costa Rica.

En el **mediano plazo** se propone la presentación formal del marco regulatorio diseñado, con el fin de ordenar y dar estructura a las acciones en ciberseguridad. Un aspecto relevante sería fortalecer en esta etapa la enseñanza del bilingüismo en las escuelas públicas, promoviendo así habilidades esenciales para este campo. Igualmente, se sugiere asegurar la alineación de las certificaciones con los estándares nacionales e internacionales, garantizando su validez y pertinencia.

Además, resultará valioso iniciar investigaciones a nivel nacional para comprender a fondo las necesidades y oportunidades en ciberseguridad, a fin de orientar mejor los esfuerzos en formación y capacitación. Este periodo también podría aprovecharse para implementar los programas de formación a distancia previamente desarrollados, junto con iniciativas de pasantías y becas que faciliten el acceso de la población a estas oportunidades.

Finalmente, se recomienda establecer mesas de estudio y debate para la reflexión conjunta entre actores clave de distintos sectores, fomentando un entorno colaborativo que permita avanzar de manera articulada en el Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad para Costa Rica.

En el **largo plazo** se recomienda implementar el marco regulatorio elaborado, consolidando así una estructura formal que sustente el desarrollo continuo de la ciberseguridad en Costa Rica. En este contexto, sería esencial ejecutar los proyectos de infraestructura necesarios que permitan sostener y expandir las capacidades formativas y laborales en este campo.

Asimismo, la implementación del nuevo diseño curricular y la adopción de currículos actualizados reforzarán la preparación técnica y práctica de los futuros profesionales en ciberseguridad. También sería pertinente considerar un ajuste salarial que equipare los ingresos entre sectores y valorice el talento especializado en esta área, promoviendo la estabilidad y la retención de profesionales calificados.

Por último, en aras de la inclusión y equidad digital, se sugiere implementar programas específicos destinados a reducir diversas brechas digitales, de modo que todas las personas tengan acceso a formación y oportunidades en ciberseguridad, independientemente de su ubicación geográfica o condiciones socioeconómicas.

CONCLUSIONES, SOSTENIBILIDAD Y EVALUACIÓN

El Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad en Costa Rica representa un paso fundamental hacia el fortalecimiento de la resiliencia digital del país y la creación de una base de talento calificado. Alineado con los objetivos de la Estrategia Nacional de Ciberseguridad 2023-2027, este marco prioriza la creación de capacidades, el fortalecimiento de la gobernanza en ciberseguridad y la cooperación multisectorial, promoviendo una cultura de seguridad digital en todos los sectores. Además, se integra con el compromiso de la Estrategia Nacional de Costa Rica de proteger los activos digitales y reforzar las competencias técnicas que demanda un entorno de ciberseguridad robusto y preventivo.

Este marco se construye sobre los esfuerzos previos realizados en Costa Rica en esta área, reconociendo que aún queda mucho por construir y consolidar a partir de lo logrado. Es clave sistematizar los avances alcanzados y generar un marco normativo que ofrezca la estructura necesaria para la sostenibilidad de esta iniciativa. A través de un enfoque colaborativo que involucra tanto al sector público como privado, el marco impulsa un ecosistema de conocimiento y práctica profesional en ciberseguridad que se ajusta a las realidades locales y que contribuye al desarrollo económico y social del país.

Para garantizar la sostenibilidad del marco, se recomienda establecer una gobernanza que impulse la cooperación entre actores clave, incluyendo instituciones educativas, el gobierno, empresas privadas y organizaciones internacionales.
La implementación debe priorizar la obtención de resultados medibles. Esto incluye mecanismos de evaluación continua que aseguren que el marco se mantenga actualizado y pertinente frente a los desafíos tecnológicos y cibernéticos emergentes.

Asimismo, se recomienda implementar mecanismos de evaluación y seguimiento sobre las diversas propuestas establecidas en el documento con especial énfasis en aquellas vinculadas con la apropiación social respecto de la ciberseguridad en los distintos niveles educativos y sectores de la población.

La sostenibilidad se propone en torno a cuatro ejes principales:

Financiamiento continuo: Desarrollo de fuentes de financiamiento que garanticen recursos constantes para la implementación y actualización de programas de formación y certificación.

Actualización continua del currículo: Mantener el contenido de los programas de estudio en línea con las necesidades cambiantes del mercado laboral y las amenazas emergentes de ciberseguridad.

Desarrollo de infraestructura y estándares de certificación: Es fundamental invertir en infraestructura que respalde la capacitación, como laboratorios de ciberseguridad y centros de innovación. Además, se recomienda establecer estándares claros para la certificación que eleven los requisitos en la validación de competencias, asegurando que estén alineados tanto con la Estrategia Nacional de Ciberseguridad 2023-2027 como con el Marco Nacional de Cualificaciones.

Fortalecimiento de la colaboración público-privada: Crear alianzas estratégicas para compartir recursos, experiencias y conocimientos, así como fomentar la investigación conjunta y el desarrollo de innovaciones que fortalezcan el talento costarricense.

ANEXO 1: GLOSARIO

Ciberseguridad:
Conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos contra ataques, accesos no autorizados o daños. La ciberseguridad abarca una serie de medidas que incluyen la protección de información personal y corporativa, la defensa frente a ciberamenazas, y la preservación de la integridad y disponibilidad de los activos digitales.

STEAM:
Un enfoque educativo interdisciplinario que integra ciencia, tecnología, ingeniería, artes y matemáticas para fomentar el pensamiento crítico, la resolución de problemas y la creatividad en los estudiantes. STEAM promueve el aprendizaje basado en proyectos y el desarrollo de habilidades técnicas y artísticas, preparando a los estudiantes para enfrentar desafíos complejos en un mundo cada vez más interconectado y tecnológico.

Formación sincrónica:
Método de enseñanza y aprendizaje en el que los participantes interactúan en tiempo real, a través de plataformas en línea o en un entorno presencial. Este tipo de formación permite la comunicación directa entre instructores y estudiantes, facilitando la retroalimentación inmediata, la colaboración activa y el intercambio de ideas en el momento.

Bilingüismo:
Capacidad de una persona o comunidad para comunicarse de manera competente en dos idiomas. El bilingüismo implica el dominio funcional de ambas lenguas, permitiendo a los hablantes comprender, expresarse y participar en contextos culturales y sociales diversos. Existen distintos grados de bilingüismo, desde la competencia básica hasta el dominio avanzado en ambas lenguas, y puede desarrollarse de manera simultánea (aprendiendo ambos idiomas desde la infancia) o secuencial (aprendiendo un segundo idioma después de haber adquirido el primero).

Pensamiento computacional:
Proceso mental que permite resolver problemas de forma lógica y sistemática, utilizando conceptos y técnicas propias de la informática. Incluye habilidades como la descomposición de problemas complejos en partes más manejables, la abstracción para identificar patrones y soluciones generales, el diseño de algoritmos y la evaluación de soluciones. El pensamiento computacional no se limita a la programación, sino que es aplicable en diversas disciplinas, promoviendo el análisis crítico, la creatividad y la capacidad de resolver problemas de manera estructurada y eficiente.

Clúster:
Son grupos de servidores que se gestionan juntos y participan en la gestión de carga de trabajo. Un clúster puede contener nodos o servidores de aplicaciones individuales.

Brechas digitales:
Son las desigualdades en el acceso, uso y habilidades para utilizar las tecnologías de la información y comunicación (TIC) entre distintos grupos de personas. Estas disparidades pueden estar influenciadas por factores como la ubicación geográfica, el nivel socioeconómico, la edad, y la educación. Las brechas digitales afectan la capacidad de los individuos para participar en la sociedad digital, limitando su acceso a recursos educativos, laborales y sociales en línea.

Brecha de género digital:
Se refiere a las desigualdades en el acceso y uso de las TIC entre hombres y mujeres. Estas desigualdades pueden deberse a factores sociales, económicos y culturales que influyen en la capacidad y disposición de las mujeres para aprovechar las oportunidades digitales. Además de incluir diferencias en el acceso a dispositivos y conectividad, esta brecha también abarca la baja representación de mujeres en carreras tecnológicas, así como la falta de oportunidades para desarrollar habilidades digitales avanzadas, lo que limita su participación equitativa en la economía digital.

Brecha de género por ruralidad:
Se refiere a las diferencias en el acceso y uso de tecnologías de la información y comunicaSión (TIC) entre hombres y mujeres que viven en áreas rurales en comparación con aquellos en áreas urbanas. Esta brecha es el resultado de una combinación de factores económicos, sociales y culturales que afectan de manera desproporcionada a las mujeres en contextos rurales.

Gamificación:
Es el proceso de integrar elementos característicos de los juegos, como la asignación de puntos, niveles, recompensas, desafíos o competencias, en contextos no lúdicos con el objetivo de fomentar la motivación, el compromiso y la participación. Esta estrategia se aplica en ámbitos como la educación, el trabajo o la salud para transformar actividades tradicionales en experiencias más atractivas, promoviendo conductas deseadas, mejorando el aprendizaje o aumentando la productividad, mientras se incentiva a los participantes a alcanzar objetivos de manera efectiva y lúdica.

ANEXO 2: METODOLOGÍA IMPLEMENTADA PARA EL DESARROLLO DE RECOMENDACIONES POR ÁREA ESTRATÉGICA

La metodología utilizada para la recolección y sistematización de la información clave en la elaboración del Marco Nacional de Formación de Fuerza Laboral en Ciberseguridad constó de dos etapas diferenciadas. La primera etapa incluyó un taller colaborativo desarrollado por la Sección de Ciberseguridad de la OEA/CICTE con el apoyo de la Unión Internacional de Telecomunicaciones (UIT) como parte de un esfuerzo global por fortalecer la capacidad nacional en educación en ciberseguridad.

Este taller, organizado en colaboración con el MICITT y el Cybersec Cluster, reunió a actores relevantes de los sectores académico, público y privado, así como de organizaciones no gubernamentales (ONG), con la finalidad de aplicar un enfoque sistémico a la formación y el desarrollo de la fuerza laboral en ciberseguridad. Este enfoque sistémico busca abordar desafíos complejos de políticas públicas mediante una metodología holística que diseña intervenciones considerando la interacción y relación de los elementos individuales en su entorno.

Los objetivos centrales de este enfoque sistémico son:

Comprensión holística de los desafíos: Proporciona una visión integral de la brecha en la fuerza laboral de ciberseguridad, permitiendo identificar los factores interrelacionados que la influyen y caracterizan.

Planificación e implementación estratégicas: Facilita la formulación de intervenciones específicas para distintas etapas educativas, con el fin de construir una base sólida y adaptativa en ciberseguridad.

Participación de las partes interesadas: Involucra activamente a una amplia gama de actores, promoviendo la colaboración y el compromiso para construir un ecosistema de ciberseguridad resiliente.

A través de este enfoque, el taller permitió comprender integralmente los desafíos y oportunidades en el ámbito de la ciberseguridad, fomentar el intercambio de buenas prácticas, y definir los próximos pasos estratégicos hacia el desarrollo de un marco nacional robusto y sostenible.

La segunda etapa de la metodología consistió en entrevistas en profundidad, realizadas después del taller. En esta fase, se seleccionaron actores clave que no habían participado en el taller o que requerían entrevistas adicionales para profundizar en ciertos aspectos. Estas entrevistas complementaron la información obtenida en la primera fase, enriqueciendo la comprensión de los desafíos y oportunidades en la formación de fuerza laboral en ciberseguridad a nivel nacional.

Partes involucradas

Participantes del taller desarrollados durante el mes de junio en San José:

Nombre completo	Institución
Abel Brenes Arce	Universidad de Costa Rica
Adrian Barrientos	PROCOMER
Alvaro Solano Mena	Universidad Latina de Costa Rica
Armando Rojas Esquivel	CONARE
Christian Sánchez	PROCOMER
Christopher Sánchez	Ministerio de Relaciones Exteriores y Culto
Daniel Chaves	CyberSec Cluster / Equifax
Daniel Gomez Guillen	Unidad Especial de Intervencion
Danny Silva	CONARE
Ginnette Rojas Arias	Marco Nacional de Cualificaciones de la Educación y Formación Técnica Profesional de Costa Rica
Hans Lothar Lara	INA
Herson Esquivel Vargas	Tecnológico de Costa Rica
Ingrid Trejos Marín	INAMU
JD Delgado	Akamai Technologies
Jonathan Solano González	Sofistic
Kevin Ludeke	Embajada EEUU
Laura Montoya	DOS
Magda López Alemán	PROCOMER
Margarita Esquivel Porras	CONARE-División Académica
María Paula Bermudez Ureña	Publicis Resources
Maryelin Moran Martínez	Ministerio de Relaciones Exteriores y Culto
Mauricio Arroyo Herrera	Instituto Tecnológico de Costa Rica (TEC)
Melvin Chaves	Universidad Internacional Universal
Miguel Pérez Montero	Universidad Cenfotec
Patricia Rojas Figueredo	Promotora Costarricense de Innovación e Investigación
Paulo De Oliveira Mata	Human Genetics Foundation y QUARK Tech Investigation Clúster
Ronald Arias Huertas	Unidad Especial de Intervención
Víctor Rojas Monge	Promotora Costarricense de Innovación e Investigación
Wilberth Molina	Universidad Fidélitas
Willy Carvajal	Unión Europea
Yenory Rojas Hernández	Universidad INVENIO

Entrevistas en profundidad:

- Ginnette Rojas Arias, Ente Nacional de Cualificaciones
- Magda López Alemán, Promotora del Comercio Exterior de Costa Rica (PROCOMER)
- Melvin Chaves, Universidad Internacional Universal
- Laura Vargas Jimenez, Marco Nacional de Cualificaciones
- Gezer Ramiro Molina Colomer, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)

Marco Nacional de
Formación de Fuerza Laboral en Ciberseguridad

OEA
Más derechos para más gente

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA