Costa Rica

Estrategia Nacional de

CIBERSEGURIDAD

2022-2027

micitt
MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

Índice

1. Resumen ejecutivo

En las últimas décadas se ha incrementado exponencialmente el uso de las Tecnologías de la Información y la Comunicación (TIC) y las oportunidades socioeconómicas y políticas que se derivan de ello (CEPAL, 2018). La transformación digital que se está viviendo a nivel global es un poderoso facilitador de un desarrollo inclusivo y sostenible, pero también puede presentar una nueva fuente de problemas si la infraestructura subyacente y los servicios que dependen de ella no son seguros ni están protegidos frente a las amenazas cibernéticas.

La naturaleza cambiante del ciberespacio, la mayor dependencia a las TIC y la proliferación de riesgos digitales, exigen mejoras continuas a las estrategias nacionales de ciberseguridad. La mayoría de los países han acelerado su transformación digital abordando las amenazas inmediatas y futuras a sus servicios críticos, infraestructuras, sectores, instituciones y empresas, así como a la paz y la seguridad internacionales, que podrían alterarse por el mal uso de las tecnologías digitales y la falta de resiliencia.

Para aprovechar los actuales beneficios que brinda la tecnología y gestionar los desafíos a los que conlleva la digitalización, el gobierno de Costa Rica confirma su compromiso para mantener un ciberespacio seguro a partir de la puesta al día de su Estrategia Nacional de Ciberseguridad.

Las estrategias forman parte de un proceso continuo de evaluación, desarrollo e implementación. Son herramientas vivas que se han de ajustar a las necesidades del país y reajustarse periódicamente para responder a las necesidades políticas, económicas, financieras y tecnológicas del momento. Considerando los avances a nivel nacional de Costa Rica en la madurez cibernética, resultaba necesario revisar y actualizar el marco político, a fin de que refleje las oportunidades y desafíos actuales que permitan una mejora en el ámbito de la ciberseguridad en el futuro.

El propósito de esta estrategia es proveer al país de un documento integral que articule y priorice objetivos, señale políticas de apoyo y mecanismos estructurales, establezca roles y responsabilidades, asignación de recursos y rendición de cuentas.

La Estrategia Nacional de Ciberseguridad de Costa Rica 2017 (ENC 2017) proporcionó un marco estratégico para lograr los objetivos socioeconómicos que dependían de la seguridad del ciberespacio. A medida que ha aumentado la necesidad de proteger el espacio digital para contribuir a la prosperidad del país, se ha vuelto necesaria la puesta al día de dicha estrategia para que se convierta en el pilar esencial para el diseño e implementación de instrumentos de política pública frente a los riesgos emergentes que amenazan el funcionamiento básico de la sociedad.

La actual estrategia se divide en dos partes diferenciadas. La primera, de los numerales 1 a 4, pone en contexto la realidad de Costa Rica desde el punto de vista de la ciberseguridad. Se hace un repaso de los antecedentes históricos y recientes, se repasan los incidentes cibernéticos que amenazan al país y se hace un análisis internacional sobre las posiciones internacionales. En la segunda parte, que comienza a partir de la explicación de la metodología utilizada para la redacción de la propia estrategia, recoge los principales objetivos que intentará conseguir este documento a partir de la definición de una serie de ejes transversales que requieren protección específica y un plan de acción y evaluación de la estrategia.

2. Antecedentes

El domingo 17 de abril, Costa Rica recibe un ciberataque de índole extorsivo sin precedentes en la historia reciente que afecta a distintas instituciones, incluido el Ministerio de Hacienda, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Instituto Meteorológico Nacional (IMN), la Radiográfica Costarricense Sociedad Anónima (RACSA), el Ministerio de Trabajo y Seguridad Social (MTSS), el Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) y la Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC), la Caja Costarricense del Seguro Social (CCSS).

En el caso de alguna de estas instituciones, el incidente provocó que sus plataformas digitales fueran deshabilitadas por días y en algunos casos meses, circunstancia que generó una grave afectación en toda la población nacional y que repercutió en pérdidas comerciales relativas a la importación, la exportación, el pago de impuestos o la atención médica entre otros.

Esta estrategia fue concebida antes de estos incidentes, pero sin lugar a duda ha sido impactada por los mismos. Los retos identificados y las lecciones aprendidas a partir de los ataques han servido para componer un documento más robusto e informado que incrementará la capacidad del país para hacer frente a los incidentes cibernéticos.

2.1. Las cifras del cibercrimen

El delito cibernético está progresando a un ritmo vertiginoso gracias a la dependencia, cada vez más acentuada, que la sociedad tiene de las tecnologías de la información y la comunicación. La pandemia COVID-19 no ha hecho sino acrecentar esta tendencia ofreciendo nuevos objetivos para estos ataques (agencias de salud pública, instituciones sanitarias, hospitales, entre otros) así como nuevas formas de engaño.

Según la agencia investigadora Cybersecurity Ventures, los costos globales del delito cibernético crecerán un 15% al año durante los próximos cinco años, alcanzando los $10,5 billones de dólares anuales para 2025, frente a los $3 billones de dólares de 2015[1]. Estos costos incluyen: daño y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación de fondos, fraude, interrupción del curso normal del negocio posterior al ataque, investigación forense, restauración y eliminación de datos pirateados.

En febrero de 2022 Trend Micro publicó junto con el Programa de Ciberseguridad del CICTE/OEA un reporte sobre el estado de la ciberseguridad en Latinoamérica y el Caribe[2] que examinó los datos del panorama de amenazas a los estados miembros de la OEA y los comparó con las tendencias globales identificadas en su reporte de 2021.

El *Ransomware*, los ataques dirigidos y las estafas continúan proliferando y evolucionando, involucrando herramientas cada vez más sofisticadas y dirigiéndose hacia blancos más grandes. Tan solo el primer semestre de 2021 se detectó más de 7,3 millones de ataques de *ransomware*, siendo una de las tendencias más notables el incremento de detecciones de

[1] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[2] https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/trend-micro-specialized-cybersecurity-report-for-latin-america-and-the-caribbean

ransomware moderno que utiliza herramientas y técnicas similares a aquellas utilizadas por amenazas avanzadas persistentes (APTs por sus siglas en inglés).

La pandemia ha sido catalizadora de una adopción más amplia de tecnologías como la nube y el internet de las cosas en las organizaciones, pero las fallas de configuración y la falta de educación de los usuarios ha puesto en peligro a muchas de ellas. La adopción por parte de casi todas las organizaciones públicas y privadas del trabajo remoto ha implicado la conexión de computadoras y otros dispositivos de trabajo a redes domésticas, algo que ha sido aprovechado por actores maliciosos a través de estafas y malware que involucra a estos sistemas de conexión.

Incluso antes de la pandemia, muchas organizaciones ya estaban adoptando nuevas tecnologías como plataformas en la nube o internet dando por sentado la seguridad de estas herramientas. Las fallas de configuración y la falta de actualizaciones, sin embargo, han estado entre las causas más comunes de infiltraciones exitosas en los sistemas de estas organizaciones. Un tema persistente a lo largo de estos incidentes de ciberseguridad fue la presencia de elementos de minería de criptomonedas, el tercer tipo de malware más detectado en los estados miembros de la OEA en la primera mitad de 2021.

Las amenazas a la cadena de suministro, por otra parte, han sido una preocupación de seguridad durante muchos años, pero durante 2021 se ha incrementado al identificarse ataques más organizados. A medida que aumenta el costo de los ataques directos contra organizaciones bien protegidas, los atacantes prefieren atacar su cadena de suministro, lo que permite afectar a un número potencialmente mayor de organizaciones y un impacto transfronterizo a gran escala. Estos ataques lograron tener costos significativos en términos de tiempo de inactividad de los sistemas, pérdidas monetarias y daños a la reputación, por nombrar solo algunos. Un reciente reporte[3] La Agencia de la Unión Europea para la Ciberseguridad (ENISA) concluyó que alrededor del 50 % de los ataques a la cadena de suministro estudiados se atribuyeron a grupos APT conocidos. El estudio también determinó que las principales motivaciones de los atacantes eran acceder al código fuente y a los datos de los clientes.

[3] ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

2.2. Costa Rica en el ámbito internacional

Como lo estableció la primera Estrategia Nacional de Ciberseguridad, la Cooperación Internacional es uno de sus principios rectores, debido a que la temática de la ciberseguridad debe ser atendida desde una perspectiva global.

Las amenazas cibernéticas al no conocer fronteras requieren que los países indispensablemente generen alianzas y estrechen lazos no solo con otros países sino también con organismos multilaterales, y otros actores del sistema internacional.

Esas alianzas además de permitir posicionar al país, generar redes de acompañamiento y acciones conjuntas internacionales, contribuyen también con el incremento de las capacidades nacionales en este tema.

Se han establecido alianzas estratégicas de larga duración con organismos multilaterales como el Organismo de Estados Americanos (OEA). Organismo que contribuyó desde 2016 en el proceso de construcción de la Estrategia Nacional de Ciberseguridad y a través del acercamiento con el Comité Interamericano contra el terrorismo (CICTE) de la OEA hemos generado procesos de formación y capacitación a jóvenes en ciberseguridad y además de formación específica para mujeres en ciberseguridad. De igual manera a través de esta alianza, se han podido conocer de cerca las experiencias de países exitosos en el tema de ciberseguridad como España y Estonia, y se han logrado hacer los contactos necesarios para intercambio de buenas prácticas y participación en redes de apoyo en ciberseguridad.

A raíz de estos acercamientos con países europeos, hoy Costa Rica participa en el proyecto Cyber4Dev financiado por la Unión Europea cuyo objetivo específico es incrementar la ciber resiliencia en los terceros países mientras se promueve un enfoque inclusivo basado en los derechos múltiples partes interesadas y que garantice el cumplimiento del estado de derecho y los principios de buen gobierno.

Aunado a estas alianzas estratégicas, MICITT ha procurado continuar con su acercamiento a instancias que contribuyan en mejorar cada vez más el conocimiento y la generación de capacidades nacionales, por lo que también con apoyo del Banco Centroamericano de Integración Económica (BCIE), KISA Corea y el Global Cybersecurity Center for Development (GCCD) de Corea se han generado alianzas para formación y capacitación.

Asimismo, se han generado acuerdos de fortalecimiento de las capacidades institucionales en ciberseguridad con apoyo de la Embajada de Israel en Costa Rica y el clúster de ciberseguridad de Israel.

De igual manera, Costa Rica cuenta como aliado en este proceso de fortalecimiento de capacidades y de acompañamiento al gobierno de los Estados Unidos, quiénes a través de sus programas de capacitación han becado a diversos funcionarios públicos, de MICITT y de otras instancias gubernamentales para la participación en capacitaciones en ciberseguridad impartidas por el gobierno de los Estados Unidos.

En 2017, la Asamblea Legislativa aprobó la adhesión de Costa Rica al Convenio sobre Ciberdelincuencia, también conocido como el Convenio de Budapest. Se trata del primer tratado internacional que aborda los delitos informáticos y de Internet mediante la armonización de las leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Este instrumento es una herramienta internacional que puede castigar los delitos informáticos independientemente del lugar en donde se produzcan.

Costa Rica fue uno de los primeros países de la región en formar parte de este convenio que está conformado por los países europeos y otras naciones como Canadá, Japón, Sudáfrica y Estados Unidos. El Convenio de Budapest reconcilia la visión de una Internet libre, donde la información debe fluir libremente y se puede acceder a ella y compartirla, con la necesidad de una respuesta de justicia penal eficaz en casos de uso delictivo. Las restricciones están estrictamente definidas; sólo se investigan y enjuician delitos penales específicos, y los datos específicos que se necesitan como prueba en procedimientos penales específicos se obtienen con sujeción a las salvaguardias de los derechos humanos y el estado de derecho.

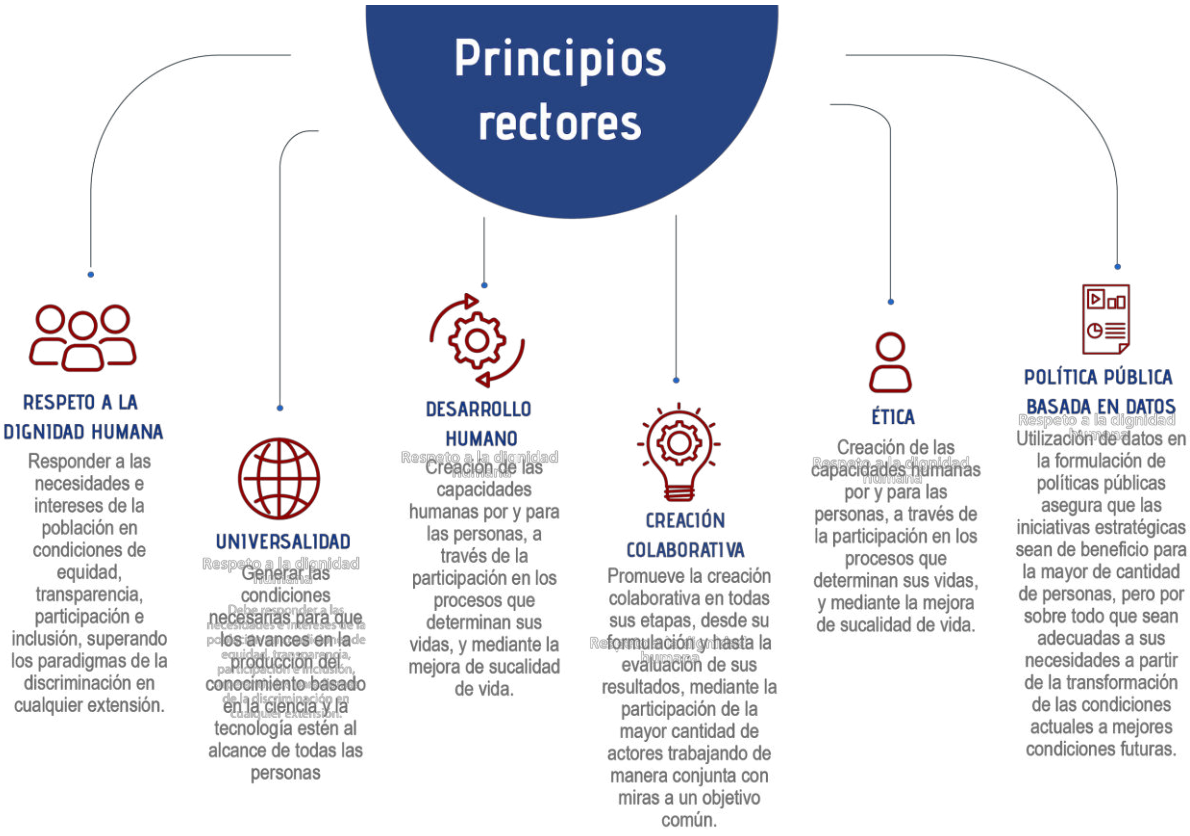
El Convenio de Budapest sigue siendo el tratado internacional vinculante más relevante sobre delitos cibernéticos y pruebas electrónicas. Con su lenguaje tecnológicamente neutral, la Convención posibilita además el ejercicio de facultades procesales y herramientas de cooperación internacional en relación con cualquier delito que implique prueba electrónica.

3. Principios rectores

La Estrategia Nacional de Ciberseguridad 2022-2027, se rige al igual que la Política Nacional de Sociedad y Economía Basada en Conocimiento (PNESBC) en los siguientes principios rectores:

- **Respeto a la dignidad humana:** debe responder a las necesidades e intereses de la población en condiciones de equidad, transparencia, participación e inclusión, superando los paradigmas de la discriminación en cualquier extensión.
- **Universalidad:** debe generar las condiciones necesarias para que los avances en la producción del conocimiento basado en la ciencia y la tecnología estén al alcance de todas las personas.
- **Desarrollo humano:** creación de las capacidades humanas por y para las personas, a través de la participación en los procesos que determinan sus vidas, y mediante la mejora de su calidad de vida.
- **Creación colaborativa:** promueve la creación colaborativa en todas sus etapas, desde su formulación y hasta la evaluación de sus resultados, mediante la participación de la mayor cantidad de actores trabajando de manera conjunta con miras a un objetivo común.
- **Ética:** garantiza que sus acciones estén dirigidas a socializar el conocimiento científico generado por la investigación y la innovación, desarrollando acciones éticas que sigan los códigos de conducta, promoviendo la creatividad y la productividad.
- **Política pública basada en datos:** La utilización de datos en la formulación de políticas públicas asegura que las iniciativas estrategias sean de beneficio para la mayor de cantidad de personas, pero por sobre todo que sean adecuadas a sus necesidades a partir de la transformación de las condiciones actuales a mejores condiciones futuras.

Ilustración 2: Ejes transversales



Fuente: Elaboración propia.

Además, esta estrategia tiene, cuatro principios adicionales:

1. **Las personas son la prioridad**

   Las personas son el eje central en la estrategia. El uso de las TIC en los diferentes ámbitos de la vida cotidiana nos obliga a hacer partícipes de esta estrategia a todos los habitantes del país, por lo que la corresponsabilidad en la creación y el uso individual de la tecnología, así como la manipulación de dispositivos y redes será fundamental. Por lo anterior, se promoverá el uso de las TIC como un instrumento para el mejoramiento de la calidad de vida de manera segura, procurando generar conciencia por medio de la educación, para las personas todas las edades, sobre los efectos del uso responsable. Se procurará que cualquier acción tenga como prioridad considerar la atención y mitigación de los riesgos que impacten prioritariamente a las poblaciones vulnerables como la niñez, la adolescencia, los adultos mayores, la población indígena y las personas con algún tipo de discapacidad.

2. **Respeto a los Derechos Humanos y la Privacidad.**

   Garantizar el respeto a los derechos humanos, especialmente los relacionados con el acceso a las TIC, el acceso a la información y el respeto a la privacidad es fundamental. Las medidas y acciones que resulten de esta estrategia deberán en todo momento salvaguardar los derechos humanos y la privacidad de la información de los habitantes del país. Por lo tanto, esta estrategia se ha desarrollado teniendo en cuenta la necesidad de equilibrar la protección de todos los habitantes y el respeto de los derechos humanos

básicos y fundamentales, con la necesidad de implementar medidas para mantenerlos seguros en línea. Esto incluye el respeto a la libertad de expresión, la libertad de palabra, el derecho a la privacidad, la libertad de opinión y la libertad de asociación. Del mismo modo, la presente estrategia emplea un enfoque de género para asegurar la igualdad de las personas en el ciberespacio.

3. **Coordinación y corresponsabilidad de múltiples partes interesadas.**

   La ciberseguridad es una responsabilidad compartida de todos los actores que participan en el ecosistema digital, lo cual incluye a las personas usuarias. Es imperativo que todas las acciones que se deriven de esta estrategia consideren, siempre que sea pertinente, la participación y aporte de todas las partes interesadas, la corresponsabilidad de estos y la necesidad de coordinación entre los distintos actores. Para el proceso de implementación, el apoyo de todos los sectores es fundamental, por esto, se deben considerar y promover los modelos público-público, público-privado y público-sociedad civil; según la idoneidad, requerimientos y alcances de los objetivos a implementar.

4. **Cooperación Internacional**

   La naturaleza transfronteriza de las tecnologías digitales hace que la temática de la ciberseguridad deba ser atendida desde una perspectiva global. Las amenazas cibernéticas no tienen fronteras, por ello la cooperación internacional se convierte en un eslabón primordial tanto para la atención de las amenazas como para la transferencia de conocimiento y el desarrollo de acciones locales y globales que ayuden a incrementar la confianza y la seguridad global. Por tanto, la construcción articulada de alianzas, acuerdos y estrechamiento de lazos con otras entidades públicas y privadas que atienden las temáticas relacionadas a la ciberseguridad tanto a nivel regional e internacional deben ser elementos clave dentro de esta estrategia.

4. Análisis situacional

Costa Rica ha llevado un proceso de acciones para mejorar la ciberseguridad nacional, lo cual llevó al país en el año 2017 a generar un norte común desarrollando su primera Estrategia Nacional de Ciberseguridad, que articuló una visión nacional para la coordinación en respuesta a las amenazas cibernéticas. Un documento que se estructuraba a partir de una serie de principios rectores, un marco con un objetivo general y ocho objetivos específicos.

En 2012, el Decreto 37.052 creaba el CSIRT Nacional bajo el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), para coordinar la seguridad cibernética y de información, y para formar un equipo de expertos destinado a prevenir y responder tanto amenazas como ataques cibernéticos contra las instituciones gubernamentales. El trabajo del CSIRT Nacional no empieza a ser efectivo, sin embargo, hasta 2018, cuando se convierte en el verdadero director de orquesta de los temas de ciberseguridad a nivel nacional y coordinador del resto de organismos del país como institución responsable de la mejora de las capacidades de las instituciones en ciberseguridad.

El objetivo era el de posicionar a Costa Rica entre los países con mayor madurez en ciberseguridad de la región, al tiempo que se mejoraron las capacidades de todos sus sectores, tanto desde el punto de vista de la inversión en tecnología como el aprovechamiento de las oportunidades que de este desarrollo pudieran surgir.

El MICITT ha liderado los trabajos para mejorar los estándares técnicos que tienen que cumplir las instituciones que evalúa la Contraloría General y que incluyen aspectos de mejora en las capacidades cibernéticas y cumplimiento de estándares a nivel país.

Gracias a este trabajo, el país ha ido mejorando posiciones en los diferentes índices que miden la madurez cibernética del país. El Global Cybersecurity Index, situó a Costa Rica en el número 76[4] a nivel global y la posición 8 de América, mejorando 39 lugares respecto de la anterior medición. El reporte del Estado de la Ciberseguridad de la OEA/BID también refleja las mejoras del país en las cinco dimensiones en las que este informe basa el nivel de madurez en ciberseguridad de los países. Este informe destaca especialmente la madurez del país respecto a los marcos legales y regulatorios y a los marcos de capacitación profesional. En general, Costa Rica ha demostrado que está dispuesto a invertir el capital político, el tiempo, el dinero y los recursos para contar con un ciberespacio más seguro para sus ciudadanos.

4.1. Incidentes cibernéticos

El CSIRT Nacional en su labor diaria realiza monitoreo de los sitios web públicos de las instituciones del sector público, atención de tiquetes relacionados con incidentes de ciberseguridad, reportes de sitios de *phishing* así como la elaboración de alertas técnicas, lo cual contribuye con la prevención ante los incidentes cibernéticos.

Durante los últimos años se ha observado un incremento de los reportes de sitios webs de *phishing* tramitados por el CSIRT Nacional. Desde 2019, fecha en que se inicia este tipo de

[4] https://ncsi.ega.ee/country/cr/

reporte, se ha producido un incremento del 54% de webs de *phishing* reportadas. Tanto los incidentes por tiquetes como las alertas generadas también han aumentado durante los últimos años. Pasando, en el caso de los tiquetes de 89 en 2018 a más de 300 en 2021; y de 1 a 305, en el caso de las alertas técnicas.

Pese al incremento de las actividades del CSIRT Nacional sigue siendo necesaria la mejora de los servicios nacionales de respuesta a incidentes, así como el fortalecimiento del mismo.

El análisis de vulnerabilidades a entidades de gobierno central y agencias descentralizadas que realiza el CSIRT Nacional no pudo detectar la amenaza que paralizó las plataformas digitales de las principales agencias del país. La cantidad de datos comprometidos y el tiempo que se tardó en restaurar los servicios de estas plataformas son argumentos que vienen a reafirmar la necesidad del fortalecimiento del marco de ciberseguridad que esta estrategia trata de definir.

4.2. Revisión de la Estrategia Nacional de Ciberseguridad de 2017

Como parte del trabajo de mejora continua que indica la línea estratégica 8.2 de la ENC 2017-2021, se realizó una revisión de dicho documento, para obtener una realimentación con el propósito de seguir mejorando las capacidades en ciberseguridad del país a partir de la implementación, seguimiento y evaluación de esta que permita evaluar el cumplimiento de las líneas de acción y proponer los ajustes según se requiera. En concreto, la línea estratégica 8.2 establece que se realice una revisión y actualización de la Estrategia Nacional de Ciberseguridad.

Siguiendo este mandato, en septiembre de 2020, el Gobierno de Costa Rica solicitó formalmente la asistencia técnica especializada del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE) para llevar a cabo una revisión y elaboración oportuna de la ENC 2017 y en vistas de renovar el marco de ciberseguridad.

Con esta revisión se inició el proceso para actualizar la Estrategia Nacional de Ciberseguridad de Costa Rica, que pretendía crear una hoja de ruta de trabajo común que permitiera, entre otros, generar nuevos ejes de desarrollo como educación, oportunidad de actividades económicas, desarrollo seguro del turismo y fortalecimiento de la ciberseguridad país.

El análisis presentado en este informe estuvo basado en la recopilación de información obtenida por representantes de los sectores interesados que fueron identificados por MICITT. Se distribuyeron dos cuestionarios complementarios en línea, un cuestionario general abarcando todos los objetivos específicos de la estrategia, al igual que un cuestionario para actores específicos. Ambos cuestionarios fueron distribuidos con el propósito de evaluar el nivel de implementación de la ENC 2017 a fin de obtener conclusiones y recomendaciones que informasen la nueva estrategia. Entre estas, las más destacables incluyen :

i. Consolidación del CSIRT-CR y MICITT. El análisis de respuestas recopiladas por parte de las partes interesadas sugiere que uno de los elementos más exitosos de la ENC 2017 fue la consolidación del CSIRT-CR como una entidad clave en la coordinación nacional en seguridad cibernética.

ii. Adquisición de una cultura nacional en ciberseguridad. Debido al aumento de iniciativas de concienciación que se están implementando.

iii. Costa Rica país líder regional en materia de ciberseguridad refrendado por el número de iniciativas que se están llevando a cabo en colaboración con socios internacionales en distintas áreas distintivas de seguridad cibernética, demostrando el compromiso de cooperación internacional del país.

La revisión de la ENC 2017 también señala una serie de oportunidades de mejora para el país. Como la posibilidad de implementar una estrategia de comunicación que dé visibilidad a las diferentes iniciativas derivadas de la implementación de las líneas de acción de la ENC, y la mejora de la coordinación interinstitucional y del sector privado para llevar a cabo iniciativas conjuntas y alianzas que repercutan en una mayor seguridad cibernética para el país. Del mismo modo, dado que existen algunos programas de educación secundaria en el campo de la ciberseguridad se recomienda considerar un mapeo de estos cursos y centralizar el acceso a la información sobre de manera que los esfuerzos en materia de educación y ciberseguridad sean llevados a cabo de manera conjunta con el ministerio responsable.

Por último, y dado que el sector turístico en Costa Rica representa el 6% de su PIB, la ciberseguridad debe ser un elemento por considerar, a fin de contribuir a la sostenibilidad económica del mismo. Debido a ello, esta revisión recomendaba que se tuviera en cuenta en la siguiente estrategia actividades que promuevan la interdependencia de la ciberseguridad como elemento fundamental en la escalabilidad y sostenibilidad de los sectores económicos más importantes del país.

4.3. Marco Normativo

En esta parte se muestra un mapeo de los principales aspectos jurídicos relacionados con la temática, incorpora principales Leyes, Decretos, Directrices, programas y otros instrumentos relacionados para la creación de esta Estrategia.

Leyes, Decretos, Directrices

En 2012, Costa Rica aprobó la Ley N° 9048 del 10 de julio de 2012 y la Ley N° 9135 del 24 de abril de 2013 y, mediante el cual se reformó el Código Penal para actualizar las disposiciones para el delito cibernético en Costa Rica. En el año 2012 se promulgó el Decreto 37.052 que creó el CSIRT Nacional bajo el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). Todo ello antes de desarrollar su primera Estrategia Nacional de Ciberseguridad en 2017.

El carácter transversal de la ciberseguridad, no obstante, provoca que temas relativos a la seguridad cibernéticas se hayan incluido en otros cuerpos normativos. Todos ellos conforman el marco legislativo de la ciberseguridad en el país:

- **Ley Promoción Desarrollo Científico y Tecnológico y Creación del MICIT (Ministerio de Ciencia y Tecnología), N°7169:** El artículo 4º, inciso b), contempla como deber del Estado:

  […] b) a través de la coordinación del Ministerio de Ciencia, Innovación, Tecnología, y Telecomunicaciones formular, supervisar la ejecución y evaluar el impacto y los resultados de las políticas y planes nacionales, sobre ciencia, tecnología e innovación en consulta con las entidades y los organismos públicos y privados que integran el Sistema Nacional de Ciencia, Tecnología e Innovación.

- **Decreto Ejecutivo Nº 31659-MP-RE-SP-H-J-MOPT:** Establece la creación del Consejo Interinstitucional sobre Terrorismo (CISTE) para que se desempeñe en el "desarrollo de proyectos de seguridad informática y en el establecimiento de Centros de Respuesta de Incidentes Informáticos CSIRTS, por sus siglas en inglés, en apego a la normativa vigente de la Organización de Estados Americanos (OEA)." (Considerando 6°).

- **Decreto Ejecutivo Nº 37052-MICIT, Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR:** Decreta, en su artículo 1, que el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), regido por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, (MICITT), cuenta:

  > *con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.*

- **Código Penal, Ley N°4573:** mediante esta reforma legal Costa Rica incluyó varios delitos informáticos dentro del ordenamiento jurídico nacional. Entre ellos, en el artículo 196 bis, tipificando la violación de comunicaciones electrónicas para descubrir los secretos o vulnerar la intimidad de otros cuando esta información se encuentre en dispositivos electrónicos, informáticos, magnéticos y telemáticos.

- **Ley N° 8968, Protección de la Persona frente al Tratamiento de sus Datos Personales.** El artículo 10 ubicado, en la Sección III, sobre Seguridad y Confidencialidad del tratamiento de los datos, especifica que "el responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley."

- **Normas técnicas para la gestión y el control de las Tecnologías de Información:** dicho documento establece, en su Principio de Cumplimiento, las instancias institucionales en materia de Tecnologías de Información y Comunicaciones para

asegurar: “el uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo” (p. 7).

En la sección correspondiente a “Procesos de marco de gestión de TI”, en el apartado XI, sobre Seguridad y Ciberseguridad (p. 13), se aborda lo relativo a la ciberseguridad, postulando que las instituciones deben generar acciones que administren la seguridad de la información y la ciberseguridad mediante política nacional enfatizando la preservación de la confidencialidad, integridad y disposición de la información.

Además, en el ámbito de los recursos humanos, se postula que: “las prácticas deben apoyar el reclutamiento, selección, contratación, inducción y capacitación continua”.

- **Norma Nº36274 para crear la Comisión Nacional de Seguridad en Línea.** En el artículo 1 se postula como labor de la Comisión: “diseñar las políticas sobre el buen uso de Internet y las Tecnologías Digitales contribuyendo a generar una cultura de comprensión, análisis y responsabilidad personal, que permita beneficiarse de las ventajas de su utilización, y tener una actitud consciente y proactiva frente a los riesgos inherentes a su uso”

- **Estrategia para la prevención y respuesta de la explotación y el abuso de niños en línea 2021-2027.** Plantea como objetivos específicos en el marco estratégico de ejecución:

  i. construir entornos digitales seguros, en coordinación con la institucionalidad pública, la empresa privada y la sociedad civil.
  ii. implementar medidas integrales para la prevención y respuesta a delitos asociados a EASNNAL, siguiendo el Modelo “WePROTECT”
  iii. reducir los riesgos que puedan derivarse del desconocimiento, incomprensión o uso inadecuado de las tecnologías digitales, por parte de las poblaciones meta.

  El desarrollo de este marco estratégico se realiza, a su vez, por medio de los siguientes ejes: políticas públicas y gobernanza; justicia penal; víctimas; sociedad civil; industria; comunicación y medios.

- **Norma N°8934 relativa a la protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos:** El artículo 2 estipula la obligación de la instalación de filtros en las computadoras de espacios públicos destinadas a personas menores de edad, con el fin de bloquear el acceso a sitios y comunicaciones cuyo contenido promueva:

a) pornografía en general, e infantil en particular.
b) lenguaje obsceno.
c) agresión y violencia física, sexual y emocional.
d) construcción de armas, explosivos
e) uso de drogas no autorizadas.
f) actividades bélicas.
g) racismo, xenofobia o cualquier forma de discriminación

Asimismo, el artículo 7 indica que: "todo proveedor de servicios de acceso a Internet (…) deberá incluir, dentro de su oferta de servicios, la opción de adquirir los filtros y demás programas especiales para bloquear el acceso a sitios con los contenidos indicados en el artículo 2"

Además, en el artículo 8 sobre Educación se decreta que el Patronato Nacional de la Infancia, en coordinación con los Ministerios: "desarrollarán campañas de educación para concienciar a los padres, madres, tutores (…) sobre la importancia de velar por la información a la que acceden los infantes, vía Internet o por algún otro medio electrónico de comunicación.

- **Política Nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de la Ciencia, la Tecnología, las Telecomunicaciones y la Innovación 2018-2027:** Política que contiene lineamientos de género con relación a procesos de tecnología del Estado.

4.4. Alineamiento Estratégico con políticas públicas del MICITT, ODS, Plan de Gobierno

No existe transformación digital sin ciberseguridad, es por esta razón que en todos los procesos de política pública en materia TIC la ciberseguridad es un eje transversal.

A continuación, se muestra el alineamiento estratégico con la demás política pública del Ministerio:

1. **Política Nacional de Sociedad y Economía basada en el Conocimiento (PNSEBC) 2022-2050**

   Esta política es una iniciativa del estado costarricense, consensuada con la sociedad civil, el sector privado y la academia para articular los esfuerzos del país en una visión de largo plazo, con respecto al progreso científico, tecnológico y su impacto económico, social y ambiental. El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) propone una redefinición de la sociedad, que acopie el consenso internacional sobre las principales tendencias en la evolución de las sociedades y, la propia conciencia del ser costarricense que persigue un mejor lugar en la orquestación global del progreso humano.

2. **Plan Nacional de Ciencia, Innovación y Tecnología (PNCTI) 2022-2027**

   Se basa en una visión transversal de la ciencia, la tecnología y la innovación, que promueve un enfoque integral con impacto en el desarrollo social, económico y ambiental de la ciudadanía costarricense y su articulación con otros sectores.

   Este Plan refleja las principales tendencias internacionales en la evolución de las sociedades, promueve nuevas prácticas para construir colectivamente soluciones innovadoras frente a los principales retos nacionales y acciones en tecnologías digitales, bioeconomía, investigación en salud y ciencias de la vida, inteligencia artificial y desarrollo aeroespacial.

3. **Estrategia De Transformación Digital (ETD) 2022-2027**

   La Estrategia de Transformación Digital busca llevar adelante importantes transformaciones digitales en las instituciones del sector público con el fin de brindar mejores y más trámites y servicios en medios digitales a disposición de la sociedad, a fin de potenciar el desarrollo socioeconómico del país y asegurar una mejor calidad de vida para todos los habitantes de manera inclusiva, a través de las oportunidades brindadas por la cuarta revolución industrial y las sociedades del conocimiento~~,~~.

4. **Estrategia Nacional de Bioeconomía Costa Rica 2020-2030**

   En el 2020 el país oficializó la Estrategia Nacional de Bioeconomía Costa Rica 2020-2030, como una herramienta alineada a las recomendaciones de acceso de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y las metas plasmadas en el Plan

Nacional de Descarbonización. Esta política pretende establecer una economía ecológica, resistente, descarbonizada, competitiva y sustentada en el conocimiento, a través de la incorporación de la bioeconomía circular y la descarbonización de los procesos de producción y consumo. Con ello, se tiene la aspiración de crear un entorno en el que la producción sea sostenible, genere un alto valor agregado en todas las regiones de país, que se base en el aprovechamiento de la biodiversidad, la circularidad en el uso de la biomasa y el progreso tecnológico

5. Plan Nacional de Desarrollo de Telecomunicaciones (PNDT) 2022-2027

El plan actual ha pretendido transformar el país para convertirlo en una sociedad conectada en la que se promoviera el uso, acceso y apropiación de las TIC de una manera inclusiva. Con base a este objetivo el PNDT establece tres pilares (Inclusión Digital, Gobierno Electrónico y Transparente y Economía Digital), 7 líneas de acción, 29 programas y 40 metas, entre ellas el Programa para impulsar la ciberseguridad como un eje para el desarrollo del Gobierno Electrónico.

6. Estrategia de Prevención y Atención del Abuso y Explotación Sexual de Niños, Niñas y Adolescentes en Línea (2021-2027)

Este instrumento surge como una respuesta a los riesgos y manifestaciones de violencia a las que las personas menores de edad pueden verse expuestas al utilizar las TIC y el Internet, alineada con la Comisión Nacional de Seguridad en Línea (CNSL), la cual fue creada a través del decreto ejecutivo N°36274-MICITT Creación de la Comisión Nacional de Seguridad en Línea, con el propósito de que estuviera a cargo del diseño de políticas públicas para el uso adecuado de las tecnologías y el internet.

7. Clúster de Ciberseguridad

Una alianza público-privada entre empresas, cámaras, la academia e instituciones públicas para mejorar la competitividad en el país. El proyecto cuenta con más de 50 organizaciones y pretende apoyar al sector público y privado para generar un marco común de impulso a la industria, generación de conocimiento y nuevos modelos de negocio, todo esto amparado en el aporte del ecosistema y la cultura digital que caracteriza a este tipo de organizaciones.

5. Visión, misión y metodología

5.1. Visión

Costa Rica maximiza los beneficios económicos, políticos y sociales derivados de las nuevas tecnologías de forma segura promoviendo un ciberespacio abierto, libre e inclusivo que sea capaz de gestionar los riesgos y responder a las amenazas nacionales de ciberseguridad a partir de compromisos pacíficos y proactivos en el ciberespacio para mejorar la prosperidad nacional.

5.2. Misión

Para alcanzar esta visión, el país fortalecerá las capacidades nacionales de ciberseguridad, mejorará el marco de gobernanza, la respuesta frente a incidentes cibernéticos y establecerá medidas para desarrollar confianza en las nuevas tecnologías mediante el uso responsable y seguro del entorno digital.

Publicar una estrategia siempre es un ejercicio inspirador que educa a las partes interesadas y les explica de qué manera se pueden apalancar los avances tecnológicos para mejorar el bienestar económico, político social y de seguridad del país. A partir de la comunicación de los objetivos y las prioridades, la ENC también ayuda a informar a socios estratégicos y a desalentar potenciales adversarios o criminales.

5.3. Metodología

La OEA/CICTE apoyó al Gobierno de Costa Rica con una metodología que fue guía para el desarrollo de la estrategia nacional de ciberseguridad de Costa Rica 2022.

La primera etapa de consultas se llevó a cabo de manera virtual, en los meses de febrero y marzo se trabajó en el desarrollo y validación del documento. En el proceso reunió a los representantes de diferentes sectores para dialogar e identificar las necesidades más urgentes del país en ciberseguridad, se examinaron no sólo las debilidades y amenazas, sino también las fortalezas y oportunidades para mejorar las capacidades de ciberseguridad en el país.

Cada sesión tuvo como objetivo comprender los desafíos actuales que están experimentando las partes interesadas y obtener información sobre las oportunidades que fortalecerán la madurez de Costa Rica en el ciberespacio. Las consultas se centraron en:

- Principales partes interesadas que deben participar
- Experiencias en los distintos sectores relacionados con la ciberseguridad y el ciberespacio
- Desafíos que las partes interesadas están experimentando
- Riesgos involucrados en este proceso
- Posibles soluciones
- Recursos disponibles dentro de su sector

A las sesiones acudieron diferentes sectores representativos como: representantes de Servicios Esenciales, Sector Financiero, Cámaras, Colegios profesionales, Fundaciones, Ministerios y otros representantes de la sociedad civil.

Luego de suspenderse el proceso de elaboración de la Estrategia Nacional debido a los ataques cibernéticos entre abril y mayo 2022, y el cambio de gobierno; las nuevas autoridades del MICITT retoman la labor de finalizar el documento con el nuevo contexto y a partir de una serie de reuniones virtuales de trabajo con múltiples partes interesadas durante los meses de agosto y septiembre y un taller presencial para desarrollar la implementación del plan de trabajo facilitado por la OEA.

6. Enfoque estratégico

Una de las consideraciones clave en el desarrollo de un enfoque estratégico es considerar los riesgos, pero también las fortalezas y oportunidades que existen. Al desarrollar las distintas áreas estratégicas, el Gobierno de Costa Rica participó en amplias consultas nacionales de múltiples partes interesadas, revisó las iniciativas actuales y adelantó las áreas de transformación digital que llevarían a nuestra nación al siguiente nivel. A medida que los costarricenses continúen aprovechando la tecnología digital para mejorar sus vidas, las siguientes áreas buscarán aprovechar nuestros logros y llenar las áreas de mejora.

6.1. Ejes transversales

La ciberseguridad afecta a numerosos aspectos del desarrollo socioeconómico, político y humano, y se ve afectada por diversos factores dentro del contexto nacional. Por esta razón se han identificado una serie de ejes que agrupan distintos ámbitos que corresponden a temas generales que van más allá de los sectores.

Ilustración 3: Ejes transversales

Fuente: Elaboración propia, 2022.

6.1.1. Coordinación Nacional

Con el propósito de garantizar la coordinación política y técnica que permitan implementar las líneas de acción de este plan es necesaria una estructura que posibilite la acción conjunta entre los distintos actores. MICITT, es el ente rector en temas de tecnología.

Se renovará la composición del Comité Consultivo encargado de velar junto con MICITT por el cumplimiento de la estrategia. Este Comité Consultivo estará formado por:

- Representantes del MICITT
- Representante del Poder Judicial
- Representante de la SUTEL
- Representantes de la sociedad civil
- Representantes de la academia
- Representantes del Sector Privado
- Representante de la PRODHAB
- Representante de IFAM
- Representantes del Sector Financiero
- Representantes del Ministerio de Educación Pública, Ministerio de Hacienda, Ministerio de Salud
- Representante de la Caja Costarricense del Seguro Social

El Comité Consultivo, presidido por el MICITT, reforzará relaciones de coordinación, colaboración y cooperación entre los distintos sectores y partes interesadas en la ciberseguridad, incluyendo al Estado, el sector privado, la academia y la sociedad civil.

Además, tendrá la autoridad para monitorear y evaluar la implementación de los objetivos y de las líneas de acción de este Plan Nacional por parte de los distintos actores gubernamentales.

- **Líneas de acción**

1. Coordinación y colaboración:

i. Crear y poner en marcha mecanismos dinámicos de coordinación intergubernamental e intersectorial.

ii. Crear una figura de enlace entre entidades públicas, gobiernos locales y otras organizaciones a nivel operativo.

iii. Crear grupos de trabajo de ciberseguridad a nivel nacional que colaboren con el MICITT.

2. **Búsqueda de recursos:**

    i. Creación de comisiones, comités y grupos consultivos para la obtención de recursos que permitan alcanzar los objetivos de esta estrategia.

    ii. Promover alianzas público-privadas para mejorar la ciberseguridad

3. **Rendición de cuentas:**

    i. Elaborar y aplicar metodología para evaluar y medir el estado de ciberseguridad a nivel nacional.

    ii. Establecer un mecanismo de seguimiento y presentación de informes periódicos con indicadores clave de desempeño de la ciberseguridad y los indicadores clave de riesgo para investigar el estado y las tendencias de la ciberseguridad a nivel nacional.

6.1.2. Fortalecimiento del Ecosistema de Ciberseguridad

El primer paso hacia la instauración de buenas prácticas ciberseguridad, es garantizar que el país cuente con personal capacitado en ciberseguridad en todos sus distintos sectores. Para ello es importante introducir la ciberseguridad en los primeros cursos de enseñanza básica con el objetivo de fomentar el interés profesional de los jóvenes. La educación debe incluir alternativas para realizar estudios especializados en ciberseguridad además de incluir cursos genéricos en la materia para grados no específicos.

Se mejorarán también las capacidades de profesionales y responsables de departamentos de tecnología de organizaciones del sector público y privado y operadores de servicios esenciales a partir de programas de formación.

Esta estrategia pretende también ampliar el uso de las TICs para desarrollar productos y servicios de ciberseguridad innovadores. Para ello se apoyará a la industria a partir de iniciativas gubernamentales y el fomento de los emprendimientos en ciberseguridad con el objetivo de desarrollar productos que sean una referencia no solo nacional, sino internacionalmente.

- **Líneas de acción**

1. **Educación académica:**

    i. Realizar una Encuesta nacional de destrezas y brechas de profesionales para medir las necesidades del país en ciberseguridad.

    ii. Ejecutar un programa de inclusión de la ciberseguridad de manera formal y escalonada en algunas materias optativas en los cursos de computación, tentativamente sobre los riesgos en el ciberespacio y su ámbito legal.

    iii. Desarrollar junto con la academia mallas curriculares en ciberseguridad que cuenten con enfoque de género interseccional e inclusión.

2. **Capacitación de profesionales:**

   i. Elaborar y ejecutar un programa de desarrollo de competencias a profesionales de organizaciones públicas

   ii. Elaborar y ejecutar un programa de desarrollo de competencias a profesionales en organizaciones privadas, haciendo énfasis en PYMES

   iii. Elaborar y ejecutar un programa de desarrollo de competencias a profesionales que ejercen la protección de Servicios Esenciales

   iv. Elaborar y ejecutar un programa de desarrollo de competencias por medio de los colegios profesionales.

3. **Innovación y desarrollo:**

   i. Fomentar la innovación en la industria de la ciberseguridad mediante un plan que apoye a la industria en la investigación de productos innovadores.

   ii. Fomentar la creación de nuevas empresas en alianza con incubadoras y aceleradoras de emprendimiento, para promocionar la colaboración entre la comunidad de expertos en ciberseguridad.

   iii. Fomentar las alianzas público - privadas para el desarrollo del ecosistema de ciberseguridad.

   iv. Desarrollar un programa de alianzas internacionales para el beneficio del ecosistema de ciberseguridad.

6.1.3. Concientización y cultura.

Para asegurar el bienestar socio económico y sostenible del país es necesario sensibilizar a los ciudadanos sobre la importancia del uso seguro y responsable de Internet. Para ello es necesario incorporar de manera progresiva buenas prácticas de ciberseguridad hasta que se interiorice en la ciudadanía, el gobierno y las empresas del país.

Tener una cultura en ciberseguridad significa que el conocimiento de uso, desarrollo, manejo de técnicas y de conceptos de ciberseguridad sirve de orientación para las prácticas de los usuarios finales de la red.

- **Líneas de acción:**

1. **Concientización de personas usuarias finales para que todas las personas conozcan los riesgos y tengan el acceso a las herramientas de protección.:**
    i. Elaboración de campañas de publicidad en alianza con diversos actores y sectores, que den a conocer mejores prácticas en el uso de nuevas tecnologías, con una sección especializada para grupos en condición de vulnerabilidad
    ii. Desarrollo de campañas para promover entre las personas usuarias el uso de internet seguro.
    iii. Planeación de cursos de alfabetización en ciberseguridad con enfoque de género interseccional e inclusión para particulares, en especial en torno a la ingeniería social en escuelas, colegios, municipalidades y colegios profesionales.
    iv. Socializar los avances frente a la lucha contra la cibercriminalidad y nuevas tendencias del ciberdelito.
    v. Elaborar un plan específico para zonas fuera de GAM
2. **Concientización del sector privado:**
    i. Crear y ejecutar campañas para promover la cultura de ciberseguridad a profesionales de organizaciones privadas, haciendo énfasis en PYMES con registros por zona y género.
    ii. Promover reconocimientos nacionales para aquellas empresas e instituciones que incluyan labores de sensibilización en ciberseguridad entre sus empleados.
    iii. Crear campañas de concientización para cambiar la percepción de los costos en las mejoras de ciberseguridad como una inversión y no como un gasto.
3. **Concientización de empleados del Sector público:**
    i. Crear y ejecutar campañas para promover la cultura de ciberseguridad a profesionales de organizaciones públicas.
    ii. Concientización y capacitar a los altos jerarcas de los Poderes de la República sobre ciberseguridad
    iii. Crear una estrategia específica para las municipalidades en alianza con IFAM.
    iv. Fomentar la colaboración horizontal de instituciones expertas con menos acceso a herramientas o personal de TI, para crear espacios donde se compartan buenas prácticas.

6.1.4. Fortalecimiento de la cooperación cibernética internacional

La naturaleza transfronteriza de muchas de las amenazas y ataques cibernéticos hace necesaria la creación de canales de cooperación internacional y la armonización de los marcos legales. Fortalecer la cooperación regional también facilita la participación en las discusiones globales en curso que permiten influir en la toma de decisiones en los foros internacionales.

- **Líneas de acción:**

1. **Fortalecer la cooperación multilateral para hacer frente a los desafíos transfronterizos y participar en las iniciativas regionales y los foros de discusión internacionales.**

   i. Identificar y unirse a los acuerdos de cooperación bilaterales y multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito.

   ii. Evaluar la eventual adhesión a instrumentos internacionales para combatir la cibercriminalidad.

   iii. Promover mecanismos de cooperación, colaboración y asistencia a nivel internacional

   iv. Promover jornadas de intercambio y transferencia del conocimiento

   v. Elaborar informes periódicos de seguimiento a la cooperación internacional

   vi. Fortalecer la participación del CSIRT-CR en la red de centro de respuestas a incidentes cibernéticos CSIRT Américas y otras globales.

   vii. Fomentar la participación de funcionarios del país en los procesos de desarrollo de normativa internacional.

6.1.5. Gestión del riesgo.

Esta estrategia define un mecanismo coherente para la gestión de riesgos que deben aplicar todas las entidades gubernamentales y los operadores de infraestructura esencial identificados en el plano nacional.

- **Líneas de acción:**

1. **Mejorar la resiliencia nacional y organizacional para prepararse, responder y recuperarse de ataques cibernéticos:**

   i. Realizar un estudio de evaluación anual de riesgos que permita al gobierno supervisar los riesgos y las soluciones adoptadas con el fin de gestionarlos, con énfasis a infraestructuras de servicios esenciales

   ii. Expedir un marco de gestión de riesgos de ciberseguridad a nivel nacional.

   iii. Elaborar perfiles de riesgos sectoriales en materia de ciberseguridad asignando valores numéricos a variables relacionadas con diferentes tipos de amenazas y el peligro que representan.

iv. Crear y poner en marcha mecanismos de cooperación e intercambio de información

v. Fomentar el registro centralizado de incidentes junto con sus mecanismos de reporte de incidentes

2. **Fortalecer la respuesta a incidentes cibernéticos:**

i. Crear y ejecutar un plan de fortalecimiento del CSIRT-CR como equipo de respuesta nacional

ii. Crear un SOC gubernamental

iii. Crear y ejecutar una estrategia para crear nuevos equipos de respuesta CSIRT sectoriales y fortalecer los actuales

iv. Desarrollar una guía nacional de clasificación de incidentes

v. Crear mecanismos para que las múltiples partes interesadas denuncien cibercrímenes.

6.1.6. Protección de Servicios Esenciales.

Los servicios esenciales (anteriormente conocido como infraestructuras críticas) son aquellos servicios necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para sus actividades de redes y sistemas de información y cuya interrupción puede tener un impacto grave en la salud, la seguridad, la protección o el bienestar económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o de la economía.

- **Líneas de acción.**

1. **Establecer una definición e inventario de los servicios esenciales del país:**

i. Identificar los servicios esenciales del país de acuerdo con los criterios de esencialidad internacionalmente aceptados.

2. **Establecer protocolos para la protección de los Servicios Esenciales:**

i. Crear y poner en marcha planes de protección y defensa de los servicios esenciales

ii. Identificar tipologías comunes de ataques a servicios esenciales.

iii. Expedir guías con medidas, buenas prácticas y lineamientos para la protección de servicios esenciales.

3. **Crisis y planes de emergencias:**

i. Crear un protocolo nacional de gestión y respuesta a crisis y emergencias cibernéticas

ii. Crear y ejecutar planes de contingencias ante situaciones de crisis y emergencias cibernéticas

iii. Adelantar ciber simulacros nacionales y ejercicios de gestión y manejo de crisis

iv. Crear y ejecutar una estrategia de gestión de la comunicación en crisis y emergencias cibernéticas

6.1.7. Fortalecimiento del marco legal en Ciberseguridad y TIC.

Este fortalecimiento comprende el desarrollo de propuesta de actualización jurídica en materia de ciberdelitos y ciberseguridad para luchar contra la ciberdelincuencia y promover un espacio cibernético seguro que garanticen el bienestar socioeconómico de la ciudadanía.

- **Líneas de acción:**

1. **Fomentar y velar por un marco cibernético regulatorio y legal actualizado:**
   i. Analizar el marco legal y regulatorio relacionadas con el entorno digital en el país, con aliados estratégicos y mesas de trabajo: (comercio electrónico, firma electrónica, transacciones electrónicas, protección al consumidor, protección de datos personales, TICs, protección Infantil en línea, propiedad Intelectual) e identificar necesidades de adecuación, adaptación y/o armonización.
   ii. Elaborar propuestas de adecuación, adaptación y/o armonización del marco legal y regulatorio con grupos descritos
   iii. Tramitar iniciativas legislativas y proyectos regulatorios

6.1.8. Gestión de la comunicación en crisis de ciberseguridad.

Considerando el impacto que un ataque o incidente cibernético puede tener sobre la operatividad de los servicios prestados al público general, los objetivos del Gobierno de Costa Rica y su reputación, es importante desarrollar un plan de comunicación de incidentes cibernéticos.

- **Líneas de acción:**

1. **Minimizar el impacto reputacional de potenciales ataques cibernéticos:**
   i. Crear un comité de comunicación de crisis cibernéticas con responsabilidades específicas de sus representantes, quienes deben representar a las partes responsables del manejo de un incidente cibernético nacional (Ejemplos: CERT nacional, MICITT, etc.)
   ii. Producir una matriz de riesgos cibernéticos y de reputación que puedan escalar a posibles crisis de comunicación, con ponderaciones según factibilidad y plan de acción para cada caso.
   iii. Desarrollar acciones de alerta temprana para la identificación de posibles crisis cibernéticas
   iv. Construir un mapa de audiencias clave y partes interesadas en obtener información en cuanto al desarrollo de un ataque o incidente cibernético.
   v. Elaborar un plan de acción general para el manejo de incidentes o crisis cibernéticas con responsabilidades específicas según los involucrados, designación de voceros principales o secundarios, acciones de mitigación de crisis comunicacional y plan de recuperación.

7. Implementación y Evaluación

La implementación de la estrategia se llevará a cabo a partir de una matriz que relacione:

EJE TRANSVERSAL 1: Coordinación Nacional			
Línea de Acción 1.1: Coordinación y colaboración			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Mecanismos públicos de coordinación para la ciberseguridad	Crear y poner en marcha mecanismos dinámicos de coordinación intergubernamental e intersectorial.	Cantidad de Mecanismos de coordinación creados	Línea base: 1 2023: 2 2024: 3 2025: 4 2026: 5
Enlace interinstitucional	Crear una figura de enlace entre entidades públicas, gobiernos locales y otras organizaciones a nivel operativo.	Cantidad de Personas que son parte de las Figuras de enlace	Línea base: 21 2023: 35 2024: 45 2025: 55 2026: 65
Grupos de trabajo	Crear grupos de trabajo de ciberseguridad a nivel nacional que reporten al MICITT.	Cantidad de Grupos de trabajo	Línea base: 1 2023: 3 2024: 5 2025: 7 2026: 9

Línea de Acción 1.2: Búsqueda de recursos			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Coordinación para la generación de recursos	Creación de comisiones, comités y grupos consultivos para la obtención de recursos que permitan alcanzar los objetivos de esta estrategia.	Cantidad de comisiones, comités, grupos consultivos	Línea base: 1 2023: 3 2024: 5 2025: 7 2026: 9
Alianzas público-privadas	Promover alianzas público-privadas para mejorar la ciberseguridad	Cantidad de Alianzas público-privadas ejecutadas en proyectos	Línea base: 1 (Clúster de ciberseguridad) 2023: 5 2024: 7 2025: 9 2026: 11
Línea de Acción 1.3: Rendición de cuentas			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Evaluación del estado de la ciberseguridad	Elaborar y aplicar metodología para evaluar y medir el estado de ciberseguridad a nivel nacional. Se determina el estado inicial, desde incipiente y hasta avanzado	Porcentaje de entidades que reportan crecimiento en su nivel inicial	2023: 5% 2024: 10% 2025: 15% 2026: 20%

Mecanismo de desempeño	Establecer un mecanismo de seguimiento y presentación de informes periódicos con indicadores clave de desempeño de la ciberseguridad y los indicadores clave de riesgo para investigar el estado y las tendencias de la ciberseguridad a nivel nacional. Determinar los indicadores clave de riesgo cibernético en las instituciones públicas.	Mecanismo de seguimiento: informes presentados (semestrales)	2023: 2 2024: 2 2025: 2 2026: 2
EJE TRANSVERSAL 2: Fortalecimiento del Ecosistema de la Ciberseguridad			
Línea de Acción 2.1: Educación académica:			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Encuesta nacional de brechas profesionales	Realizar una encuesta nacional de destrezas y brechas de profesionales para medir las necesidades del país en ciberseguridad por sectores para construir el plan de capacitación	Encuestas de destrezas por sector profesional	2023: 1 2024: 1 2025: 1 2026: 1
Inclusión de ciberseguridad en etapas tempranas de la enseñanza.	Poner en marcha un programa de inclusión de la ciberseguridad de manera formal y escalonada en algunos contenidos en materias optativas como en los cursos de computación, tentativamente sobre los riesgos en el ciberespacio y su ámbito legal.	Personas estudiantes que participan en programas de inclusión temprana, considerando la zona, región, provincia	2023: 1500 2024: 9000 2025: 10800 2026: 12960
Desarrollo de mallas curriculares	Actualizar junto con el CONESUP y CONARE para las academias, las mallas curriculares en ciberseguridad que cuenten con enfoque de género interseccional e inclusión.	Mallas curriculares actualizadas	2023: 5 2024: 10 2025: 10 2026: 10

Línea de Acción 2.2: Capacitación de profesionales			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Programas de desarrollo de competencias para la función pública	Elaborar y ejecutar un programa de desarrollo de competencias a profesionales de organizaciones públicas.	Cantidad de Personas capacitadas en Programa de competencias	2023: 1.000 2024: 1.200 2025: 1.440 2026: 1.728
Programas de desarrollo de competencias para el sector privado	Elaborar y ejecutar un programa de desarrollo de competencias a profesionales en organizaciones privadas, haciendo énfasis en PYMES	Cantidad de Pymes participantes en el Programa de competencias por región	2023: 40 2024: 80 2025: 120 2026: 150
Programa de desarrollo de competencias para profesionales de Servicios Esenciales	Elaborar y ejecutar un programa de desarrollo de competencias a profesionales que ejercen la protección de Servicios Esenciales	Cantidad de entidades que participan en el Programa de competencias para la protección de servicios esenciales	2023: 20 2024: 30 2025: 40 2026: 50
Programas de desarrollo de competencias para jueces y fiscales	Elaborar y ejecutar un programa de desarrollo de competencias a profesionales de autoridades de aplicación de la ley (jueces y fiscales).	Cantidad de talleres impartidos en Programa de competencias	2023: 4 2024: 4 2025: 4 2026: 4

Línea de Acción 2.3: Innovación y Desarrollo			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Plan de acción industrial para el desarrollo de productos innovadores	Fomentar la innovación en la industria de la ciberseguridad mediante un plan que apoye a la industria en la investigación de productos innovadores.	Cantidad de proyectos que se reciben de los retos de innovación- CyberChallenge - Hackatons o similares	2023: 1 2024: 3 2025: 4 2026: 4
Fomento del emprendimiento	Fomentar la creación de nuevas empresas a partir de la creación de incubadoras y desarrollar las existentes a través aceleradoras de emprendimiento para promocionar la colaboración entre la comunidad de expertos en ciberseguridad.	Cantidad de actividades para fomentar la Creación de empresas	2023: 1 2024: 2 2025: 3 2026: 4
EJE TRANSVERSAL 3: Concientización y Cultura			
Línea de Acción 3.1: Concientización de personas usuarias finales			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Campañas de publicidad	Elaboración de campañas de publicidad que den a conocer mejores prácticas en el uso de nuevas tecnologías, con una sección especializada para grupos en condición de vulnerabilidad	Social Media Engagement de la Campañas de publicidad en redes sociales	2023: 1% 2024: 2% 2025: 3% 2026: 4%

Promoción del uso de internet seguro	Desarrollo de campañas para promover entre los usuarios el uso de internet seguro.	CTR (Click Through Rate) de las Campañas de concientización	2023: 2% 2024: 3% 2025:4% 2026:5%
Cursos de alfabetización	Planeación de cursos de alfabetización en ciberseguridad con enfoque de género interseccional e inclusión para particulares, en especial en torno a la ingeniería social.	Cantidad disponible de Cursos de alfabetización	2023: 6 2024:12 2025:24 2026:36
Cursos de alfabetización	Publicar en un portal web las ofertas académicas con cursos de alfabetización y ciberseguridad del país	Cantidad de publicaciones	2023: 6 2024: 6 2025: 12 2026: 12
Socializar avances frente a la cibercriminalidad	Realizar campañas para socializar los avances frente a la lucha contra la cibercriminalidad y nuevas tendencias del ciberdelito.	Cantidad de Boletines enviados	2023: 6 2024:12 2025:12 2026:12
Socializar avances frente a la cibercriminalidad	Realizar campañas para aumentar la cantidad de denuncias por cibercrimen como lucha contra la cibercriminalidad y nuevas tendencias del ciberdelito.	Porcentaje de aumento de denuncias por intentos o acciones	2023: 5% 2024: 8% 2025: 10% 2026: 15%
Línea de Acción 3.2: Concientización del sector privado			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**

Desarrollo de campañas entre el sector privado	Crear y ejecutar campañas para promover la cultura de ciberseguridad a profesionales de organizaciones privadas, haciendo énfasis en PYMES y empresas fuera de GAM	Números de eventos para la promoción de la cultura de ciberseguridad, webinars, foros, charlas	2023: 6 2024:12 2025: 18 2026: 24
Promover premios a empresas sensibilizadas	Crear un programa para el reconocimiento de entidades empresas e instituciones que incluyan labores de sensibilización en ciberseguridad entre sus empleados.	Reconocimientos nacionales otorgados	2023: 1 2024:1 2025:1 2026:1
Campañas de concientización entre el sector privado	Crear campañas de concientización para cambiar la percepción de los costos en las mejoras de ciberseguridad como una inversión y no como un gasto.	Campañas de concientización	2023: 1 2024:1 2025:1 2026:1
Línea de Acción 3.3: Concientización de empleados del sector público			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Campañas para funcionarios públicos	Crear y ejecutar campañas para promover la cultura de ciberseguridad a profesionales de organizaciones públicas.	Campañas de concientización	2023: 1 2024:1 2025:1 2026:1
Concientización para altos funcionarios	Realizar campañas de concientización a los altos jerarcas de los Poderes de la República sobre ciberseguridad	Campañas de concientización	2023: 1 2024:1 2025:1 2026:1

EJE TRANSVERSAL 4: Fortalecimiento de la cooperación cibernética internacional			
Línea de Acción 4.1: Fortalecer la cooperación multilateral para hacer frente a los desafíos transfronterizos y participar en las iniciativas regionales y los foros de discusión internacionales.			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Identificar acuerdos internacionales relevantes	Unirse a acuerdos de cooperación bilaterales y multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito.	Cantidad de acuerdos suscritos	2023: 1 2024:1 2025:1 2026:1
Promover el intercambio de información de inteligencia	Utilizar herramientas de Threat Intelligence Sharing Platform, como el MISP, para el intercambio de indicadores de compromiso o amenazas	Cantidad de entidades que participan	2023: 1 2024: 2 2025: 3 2026: 3
Fortalecer la participación del CSIRT-CR en redes internacionales	Fortalecer la participación del CSIRT-CR en la red de centro de respuestas a incidentes cibernéticos CSIRT Américas mediante asistencia a capacitaciones e intercambio de información.	Capacitaciones	Línea base: 1 2023: 4 2024: 4 2025: 6 2026: 6
Fomentar participación en procesos de desarrollo de normativa internacional	Fomentar la participación de funcionarios del país en los procesos de desarrollo de normativa internacional.	Cantidad de procesos internacionales	2023: 1 2024:1 2025:1 2026:1
EJE TRANSVERSAL 5: GESTIÓN DEL RIESGO			

Línea de acción 5.1: Mejora de la resiliencia nacional			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Estudio de evaluación de riesgos	Realizar un estudio de evaluación de riesgos que permita al gobierno supervisar los riesgos y las soluciones adoptadas con el fin de gestionarlos, con énfasis a infraestructuras de servicios esenciales	Estudios realizados	2023: 1 2024:0 2025:1 2026:0
Expedir marco de gestión de riesgos	Expedir un marco de gestión de riesgos de ciberseguridad a nivel nacional. Actualización	Marco de gestión elaborado	2023: 1 2024:0 2025:0 2026:1
Elaborar perfiles de riesgos sectoriales	Elaborar perfiles de riesgos sectoriales en materia de ciberseguridad asignando valores numéricos a variables relacionadas con diferentes tipos de amenazas y el peligro que representan.	Perfiles elaborados y asignados	2023: 2 2024:2 2025:2 2026:2
Registro centralizado de incidentes	Crear un registro centralizado de incidentes junto con sus mecanismos de reporte de incidentes	Cantidad de entidades que usan el Registro de incidentes	2023: 0 2024:15 2025: 20 2026: 25
Línea de acción 5.2: Fortalecer la respuesta a incidentes cibernéticos			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**

Desarrollo de programa de certificaciones	Crear un centro de operaciones de seguridad (SOC) gubernamental	cantidad de entidades atendidas por el SOC	2023: 5 2024:7 2025:10 2026:15
Creación de nuevos CSIRT	Crear una estrategia para incentivar la creación nuevos equipos de respuesta CSIRT sectoriales y fortalecer los actuales	Número de CSIRTs sectoriales	2023: 0 2024:0 2025:2 2026:2
Guía de clasificación de incidentes	Implementar una guía nacional de clasificación de incidentes	Número de entidades que utilizan la Guía	2023: 0 2024:15 2025: 20 2026: 25
EJE TRANSVERSAL 6: PROTECCIÓN DE SERVICIOS ESENCIALES			
Línea de Acción 6.1: Establecer una definición e inventario de los servicios esenciales del país.			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Identificación de servicios esenciales	Crear una guía que identifique los Servicios Esenciales del país de acuerdo con los criterios de esencialidad internacionalmente aceptados. Revisión de guía	Cantidad de servicios esenciales con protocolos definidos	2023: 5 2024: 7 2025:12 2026:15
Línea de Acción 6.2: Establecer protocolos para la protección de Servicios Esenciales.			

Intervención Pública	Objetivo	Indicador	Meta
Planes de protección	Crear y poner en marcha planes de protección y defensa de los servicios esenciales	Cantidad de entidades que participan del Plan	2023: 10 2024: 15 2025: 20 2026: 25
Identificación de tipologías comunes	Identificar tipologías comunes de ataques a servicios esenciales en la guía	Reporte de tipologías	2023: 0 2024:1 2025:0 2026:1
Expedición de guías de buenas prácticas	Expedir guías con medidas, buenas prácticas y lineamientos para la protección de servicios esenciales.	Cantidad de Guías publicadas	2023: 4 2024: 6 2025: 12 2026:12
Línea de Acción 6.3: Crisis y planes de emergencia.			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Creación de protocolo nacional	Crear un protocolo nacional de gestión y respuesta a crisis y emergencias cibernéticas	Cantidad de entidades que se integran al protocolo nacional de gestión y de respuesta de crisis publicado	2023:0 2024:16 2025:0 2026:16

Ejecutar planes de contingencia	Crear en conjunto, planes de contingencias ante situaciones de crisis y emergencias cibernéticas	Cantidad de Planes de contingencia desarrollados	2023: 8 2024: 8 2025: 8 2026: 8
Realizar ciber simulacros	Realizar ciber simulacros nacionales y ejercicios de gestión y manejo de crisis	Cantidad de Ciber simulacros realizados	2023: 1 2024:1 2025:1 2026:1
EJE TRANSVERSAL 7: Fortalecimiento del marco legal en Ciberseguridad y TIC.			
Línea de Acción 7.1: Garantizar un marco cibernético regulatorio y legal actualizado:			
Intervención Pública	**Objetivo**	**Indicador**	**Meta**
Elaborar propuestas y Tramitar iniciativas legislativas	Analizar el marco legal y regulatorio relacionadas con el entorno digital en el país: (comercio electrónico, firma electrónica, transacciones electrónicas, protección al consumidor, protección de datos personales, TICs, protección Infantil en línea, propiedad Intelectual) e identificar necesidades de adecuación, adaptación y/o armonización. Elaborar propuestas de adecuación, adaptación y/o armonización del marco legal y regulatorio para tramitar iniciativas legislativas y proyectos regulatorios	Cantidad de Propuestas a la Asamblea Legislativa	2023: 1 2024:1 2025:1 2026:1
EJE TRANSVERSAL 8: Gestión de la comunicación en crisis de ciberseguridad.			
Línea de Acción 8.1: Minimizar el impacto reputacional de potenciales ataques cibernéticos:			

Intervención Pública	Objetivo	Indicador	Meta
Creación de Comités de Comunicación	Crear comités de comunicación de crisis cibernéticas con responsabilidades específicas de sus representantes, quienes deben representar a las partes responsables del manejo de un incidente cibernético nacional	Cantidad de personas de cada entidad que participan en el Comité	2023: 15 2024: 20 2025: 30 2026: 40
Producción de matriz de riesgos reputacionales	Producir una matriz de riesgos cibernéticos y de reputación que puedan escalar a posibles crisis de comunicación, con ponderaciones según factibilidad y plan de acción para cada caso.	Cantidad de entidades que participan construyendo su matriz de riesgos	2023: 15 2024: 20 2025: 30 2026: 40
Acciones de alerta temprana	Desarrollar acciones de alerta temprana para la identificación de posibles crisis cibernéticas	Incremento porcentual de Acciones de alerta temprana	2023: 5% 2024:15% 2025:20% 2026:25%
Mapa de audiencias clave	Construir un mapa de audiencias clave y partes interesadas en obtener información en cuanto al desarrollo de un ataque o incidente cibernético.	Cantidad de entidades que son parte del Mapa de audiencias	2023: 15 2024: 20 2025: 30 2026: 40
Elaboración de plan de acción	Elaborar un protocolo de acción general para el manejo de incidentes o crisis cibernéticas con responsabilidades específicas según los involucrados, designación de voceros principales o secundarios, acciones de mitigación de crisis comunicacional y plan de recuperación.	Cantidad de entidades que participan en las acciones del protocolo de acción	2023: 15 2024: 20 2025: 30 2026:40

OEA Más derechos para más gente

MICITT MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES